DEFENSE INDUSTRY INITIATIVE

DII

ON BUSINESS ETHICS AND CONDUCT

# SMALL BUSINESS TOOLKIT

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

## SMALL BUSINESS TOOLKIT
## RESOURCE 5

# INTRODUCTION

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

# SMALL BUSINESS TOOLKIT

*Updated May 2026 | Created May 2016*

## Table of Contents

## Disclaimer

The Small Business Toolkit (Toolkit) is based on best practices of Defense contractors at the time of publication. Each section of the Toolkit is for reference only and is to be used at the consumer's own risk. The Defense Industry Initiative (DII) disclaims any and all liability for any consequences arising out of your use or deployment of any or all aspects of this Toolkit. DII does not guarantee that any or all aspects of this Toolkit have been updated to reflect any changes or developments in the law. As such, DII is not responsible for any subsequent regulatory or legal changes that may render sections of this Toolkit obsolete.

By posting the Toolkit, DII is not providing legal advice and is not agreeing to enter into an attorney-client relationship. Please consult with legal counsel to verify the completeness, accuracy, and timeliness of the provisions contained within.

## Introduction

The Defense Industry Initiative on Business Ethics and Conduct (DII) has developed this Toolkit to provide guidance to small businesses on how to design, implement, maintain, and augment business ethics and conduct compliance programs. The Toolkit contains four complementary sections.

### 1. Governance & Organization

Guidance as to who within a small business should be responsible for leading a compliance program, different models to use in establishing an ethics and compliance function, and how to implement an effective program, even with a department of one.

### 2. Policies & Procedures

Templates that can be adopted by small businesses with little or no revisions, and that include mandatory policies (e.g. combating human trafficking, drug free workplace, equal employment opportunity) as well as optional policies that would be necessary depending on the type of work a contractor performs (e.g. industrial security for those who handle classified information).

### 3. Training & Engagement

Training presentation and access to videos and other engagement resources on key risk areas and ethics and compliance topics, which small businesses can use to train their employees.

### 4. Auditing, Monitoring & Mentoring

Tools to allow small businesses to self-audit their business ethics and conduct compliance program and determine where gaps may exist.

# The Genesis of the Toolkit

In 2015, following the publication of DII's Model Code of Conduct and Supplier Toolkit, multiple suspension and debarment offices from agencies across the federal Government invited DII to discuss the challenges faced by small businesses in understanding and complying with their obligations as federal contractors. A key concern repeatedly raised by agency officials during these meetings was the lack of existing resources available to small businesses.

Federal procurement policy has included mechanisms intended to increase prime and subcontract awards to small businesses, which are implemented across a number of government agencies. Significantly less time and attention is paid to ensuring that small businesses develop the necessary know-how to implement appropriate internal systems to ensure compliance with the myriad federal statutes, regulations, and contract provisions imposed on small businesses when contracting with the federal Government.

Set within this context, DII committed to provide functional, easily usable, and scalable guidance on how to design, implement, maintain and augment a business ethics and conduct compliance program.

## Guiding Principles Behind DII's Small Business Toolkit

In creating the Small Business Toolkit, DII continues to use FAR 52.203-13, Contractor Code of Business Ethics and Conduct, as the baseline for contractor ethics and compliance expectations. The clause remains the clearest federal contracting source for core program elements: a code, ethics awareness and training, internal controls, timely detection and disclosure, and prompt corrective action.

The Toolkit also reflects the U.S. Sentencing Guidelines for Organizations and DOJ's Evaluation of Corporate Compliance Programs. The Sentencing Guidelines recognize that an effective compliance program can mitigate penalties. DOJ's ECCP, updated in 2024, has become an important enforcement benchmark for assessing whether a program is well designed, adequately resourced and empowered, and working in practice.

Those internal-control concepts became mandatory for covered contracts in 2008, when the FAR was amended to require contractor codes, ethics awareness programs, internal control systems, and disclosure to the Government of credible evidence of specified criminal violations, civil False Claims Act violations, or significant overpayments.

The clause imposes distinct requirements related to codes of conduct, ongoing business ethics awareness and compliance programs, and internal control systems. DII has grouped these requirements into four categories and provides resources on each one:

1. **Governance & Organization**
2. **Policies & Procedures**
3. **Training & Engagement**
4. **Auditing, Monitoring & Mentoring**

# Why Should Small Businesses Implement a Business Ethics and Conduct Compliance Program?

Small businesses may question the need for a business ethics and conduct compliance program. With a limited number of employees and resources, implementing a compliance program may seem unnecessarily complicated and expensive. However, upon closer examination, numerous reasons—ranging from regulatory and contractual requirements to good governance—counsel in favor of all small businesses having some form of a compliance program, as follows:

1. The FAR requires that all government contractors conduct themselves with the highest degree of integrity and honesty. Contractors should have a written code of business ethics and conduct as well as an employee business ethics and compliance training program and an internal control system that promotes compliance with such a code. To that end, this training program and internal control system should:
    a. Be suitable to the size of the company and extent of its involvement in Government contracting;
    b. Facilitate timely discovery and disclosure of improper conduct in connection with Government contracts; and
    c. Ensure corrective measures are promptly instituted and carried out.
2. Although FAR 52.203-13 exempts small businesses from the covered-contract requirement to establish a formal internal control system, adopting policies without any mechanism to promote compliance still presents legal and practical risk. Contractors are assessed under multiple frameworks, including the FAR, responsibility and suspension/debarment rules, the Sentencing Guidelines, and DOJ policy. Even scaled or informal compliance measures can help small businesses prevent and detect misconduct, meet disclosure obligations, and demonstrate responsibility as they perform and grow.
3. Mandatory disclosure is a separate concern. Whether or not FAR 52.203-13 applies, the current FAR and implementing class deviations through acquisition reform efforts continue to recognize suspension or debarment risk when a principal knowingly fails to timely disclose credible evidence of specified criminal violations, civil False Claims Act violations, or significant overpayments in connection with a Government contract or subcontract. DOJ's Corporate Enforcement and Voluntary Self-Disclosure Policy adds another practical incentive for early escalation, disclosure analysis, cooperation, and remediation. For small businesses, the takeaway is the same: potential issues need a reliable path to Legal, leadership, or another responsible reviewer.
4. Responsibility considerations arise not only during contract performance, but also as a threshold matter for award eligibility. Even as acquisition reform efforts emphasize speed, flexibility, and streamlined rules, contracting officers still make affirmative responsibility determinations that consider integrity, business ethics, and eligibility under applicable laws and regulations. When a small business is found nonresponsible, the matter is generally referred to the SBA for a Certificate of Competency determination. Under either process, the existence or absence of a compliance program may affect the review.

5. Other business considerations also support having a business ethics and conduct compliance program. Reputational risk can be a significant concern, and an established compliance program can help distinguish a small business when pursuing future opportunities, including teaming agreements or mentor-protégé relationships with larger primes. For small businesses engaged in exit planning or preparing for a future sale, documented compliance practices can also reduce transaction risk.
6. Establishing a business ethics and conduct compliance program is not a one-size-fits-all exercise. The FAR, the Sentencing Guidelines, and DOJ's ECCP all recognize that programs should be scaled to the organization's size, government-contracting activity, and risk profile. Rather than prescribing a uniform approach, these frameworks allow organizations to design compliance measures appropriate to their circumstances. Factors that may influence the structure and scope of a small business's compliance program include:
    a. Size of the organization. A small business with a limited workforce and resources would not be expected to maintain the same level of formality or dedicated compliance personnel as a larger contractor.
    b. Nature of the organization's business. In commercial item contracting, the Government employs a single, streamlined set of instructions, requires a consolidated list of representations and certifications, and includes terms and conditions that more closely resemble those found in typical commercial contracts. By contrast, small businesses performing work that implicates export controls, counterfeit electronic parts, or security clearance requirements are subject to additional regulatory obligations and potential penalties.
    c. Prior history of misconduct, if any. Past compliance issues—such as inaccurate certifications or reporting failures—may warrant more targeted training, monitoring, or auditing.
    d. Experience in the federal marketplace. A small business with an established history of government contracting would generally be expected to maintain more developed compliance practices than a company performing its first government contract.
    e. Risk profile associated with government contracts. The type, complexity, and regulatory sensitivity of a contractor's work directly affect the level of compliance risk and, accordingly, the design of its compliance program.

None of these factors is static. As FAR clauses, class deviations, acquisition policy, and DOJ enforcement policy continue to evolve, small businesses should periodically reassess their risks and adjust their compliance systems accordingly.

The resources in the Toolkit are scalable and purposefully designed to be adapted to the particular needs of a small business. As part of the Toolkit, DII provides guidance on how a small business can implement each section of the Toolkit – both for small businesses that are establishing a compliance program for the first time and for small businesses that are seeking to augment an existing compliance program.

DEFENSE INDUSTRY INITIATIVE

DII

ON BUSINESS ETHICS AND CONDUCT

## SMALL BUSINESS TOOLKIT

# GOVERNANCE & ORGANIZATION

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 1: GOVERNANCE AND ORGANIZATION

**Governance structures are evaluated by prosecutors, suspension and debarment officials, regulators, and prime contractors. An effective ethics and compliance program is evaluated not solely by the absence of misconduct, but by whether the organization took reasonable, good-faith, and proactive steps to prevent, detect, and respond to misconduct. Enforcement authorities assess governance structures as a threshold indicator of whether a program can function in practice, with expectations scaled to the company's size, resources, and risk profile.**

## When designing an ethics and compliance program for a small business, consider:

1. ***The size of the company***
2. ***The industry and the extent to which it is regulated***
3. ***Distribution of your workforce***
4. ***The number of countries in which you operate***
5. ***Personnel competence***
6. ***Ethics and compliance function funding***
7. ***Placement of the ethics and compliance function within the organization, including leadership designation and reporting structure***
8. ***Determination of ethics and compliance function lead***
9. ***Structures/systems available to support this function***

For some organizations, the establishment of an ethics and compliance program is a proactive measure to ensure the company operates on a strong foundation; for others, regulatory requirements mandate certain program elements. In either case, a robust ethics and compliance program can create a positive work environment, elevate the company's reputation, and serve as a competitive advantage.

## Who should lead the ethics and compliance function?

Identifying the right leader is essential to the success of the program. Government authorities emphasize meaningful oversight rather than symbolic assignments. The individual should have demonstrated leadership skills, a solid reputation, and serve as a role model for character, integrity, and professionalism. The individual should be knowledgeable about the business and its operations, approachable, fair, trustworthy, and perceived as someone who will safeguard the confidentiality of those who contact the Ethics Office.

In addition to integrity and credibility, the individual leading the ethics and compliance function must be vested with sufficient authority, independence, and resources to carry out the program effectively. This includes the ability to raise concerns without obstruction, recommend corrective actions, and operate free from improper business pressure or retaliation.

Ideally, the leader of the ethics and compliance function should report directly to the Board of Directors or Chief Executive Officer; however, for many companies this may not be feasible. Some potential departments that can lead these efforts are the Law Department, Human Resources, Internal Audit, Corporate Responsibility, Finance, or Operations. In such cases, the ethics and compliance leader should have documented, recurring access to the Board, governing authority, or a designated senior leader acting in that capacity. This access should include the ability to escalate significant compliance issues, trends, and risks, and should not be limited to extraordinary circumstances. Any reporting relationship and escalation pathway should be documented in the policy establishing the ethics and compliance program.

The person selected must have the time and resources to dedicate to developing, implementing, and maintaining the program. They should have a solid foundation in legal and regulatory compliance, investigations and issue resolution, and training and communication.

## What could the department look like?

If you are fortunate to have a department, there are several options for organizing the compliance function.

- **De-centralized model** — Organizations with multiple business units may use a de-centralized model. A de-centralized model includes the program leader at the corporate office setting overall program requirements and standards, with each business unit having an ethics and compliance leader who develops and implements the program to meet those program requirements. Typically, overarching documents, like the code of conduct, are developed for the enterprise; however, policies, procedures, helpline administration, training and communication are all developed and implemented at the business unit level.

  This model enables the business units to take full ownership of their ethics and compliance program and have it customized to meet the needs of their employees. However, this model can create program inconsistencies and increased risk, which could be mitigated through program controls and audits.

- **Centralized model** — A centralized model has a team at the corporate level developing all aspects of the program including the code of conduct, policies and procedures, training and communication, helpline administration and monitoring and auditing.

This model is consistent across the enterprise and avoids duplication of effort. However, a centralized model could be further from the pulse of the organization as it is not necessarily integrated with leadership at the business unit level. Additionally, additional effort may be required to ensure the program elements meet the needs of the entire organization.

- **Hybrid model** — If you combine the two models, you get a centralized function that develops all of the key program elements, like the code of conduct, policies and procedures, helpline administration and training and communications, plus ethics and compliance leaders that are integrated into the business units to customize and deploy the program elements within their groups.

  This model enables a consistent program and still elicits leadership ownership of the program at the business unit level.

Whichever model is adopted, the scope, roles, responsibilities, and reporting relationships of all participants in the ethics and compliance program should be documented in policy. The choice of governance structure should be informed by the organization's risk profile, including the nature of its government contracts, regulatory exposure, geographic footprint, and supply-chain complexity, and should be periodically reassessed as risks and operations evolve.

## What if it is a department of one?

Realistically, most ethics and compliance departments in small businesses may consist of a department of one. What is critical to successfully implementing an ethics and compliance program is that you have support from leadership and you develop close partnerships with key stakeholders to accomplish your goals. No matter the size of your department, consider establishing the following forums to aid in the development, implementation, and assessment of your program and its initiatives. The scope, composition, roles, responsibilities, and meeting cadence of these forums should be documented, and outcomes should be tracked to support program oversight and continuous improvement.

- **Ethics and Compliance Committee** — An ethics and compliance committee can provide leadership and oversight to your program. They can help resolve major issues, identify risks and potential mitigation strategies. Additionally, they can help identify training and communications needs.

  The Ethics and Compliance Committee can be made up of senior leaders from the Law Department, Human Resources, Internal Audit, Business Management, Operations, Communications, Security, Information Technology and any other organization with which you may partner.

- **Working Group** — While an ethics committee can identify issues and actions, many companies also have working groups to help implement the program. The working group can be made up of the same organizations that constitute the Ethics and Compliance Committee, but with select individuals who can partner with the ethics program in developing and implementing the program. The working group should enable greater harmony and integration of effort across organizations within the company that share responsibility for ensuring compliance with laws, regulations, and internal policies.

- **Ethics Liaisons** — An Ethics Liaison program is an excellent way to acquire visibility for your program when you have limited resources and budget. Ethics Liaisons are full-time employees in other roles; however, they are tasked with being the ethics point of contact for their location or business group. Ethics Liaisons can serve as a contact for employees who have questions on policies and procedures or

would like to bring forward an ethics issue. Additionally, they can help implement program initiatives and communicate the ethics program within their group. Since the Ethics Liaisons have full-time jobs, they typically do not have time to develop program elements, and should not be called upon to conduct investigations because they lack the requisite knowledge and skills. However, they can implement program initiatives, serve as a touch point for employees on ethics and compliance concerns, and promote ownership of the program and its initiatives within their organization and at their site(s).

Once again, to ensure continuity and program maturity, your program policy should identify the forums you rely upon to help execute program elements. At a minimum, the forums' composition, scope, roles and responsibilities, and meeting frequency should be documented.

## What is the role of the Board of Directors or governing authority?

The Board of Directors or equivalent governing authority plays a critical oversight role in an effective ethics and compliance program. Oversight responsibilities may include receiving periodic updates on program performance, understanding key risk areas, supporting the independence and authority of the compliance function, and ensuring that significant compliance issues are addressed appropriately.

For small businesses without a formal board structure, these responsibilities may be exercised by the owner, managing partner, or designated senior leader, provided the oversight role is documented and actively performed.

## What other resources are available to supplement internal governance tools?

There are many resources available to assist you with the design of an ethics and compliance program appropriate for your business, in addition to this toolkit. A solid but non-comprehensive list can be found in Resource 4.

DEFENSE INDUSTRY INITIATIVE

DII

ON BUSINESS ETHICS AND CONDUCT

## SMALL BUSINESS TOOLKIT

# TRAINING & ENGAGEMENT

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 2: SAMPLE COMPLIANCE TRAINING

## Welcome & Purpose

This training provides an overview of key compliance obligations applicable to U.S. government defense contractors. It is intended for awareness and training purposes only. Employees should always consult current law, regulations, contract clauses, and company policies for specific requirements. This training reinforces the Company Code of Conduct — see the Code of Conduct for the full statement of expectations.

- Defense industry regulations are complex
- All providers are expected to be aware of and comply with the applicable rules. These expectations apply regardless of company size, contract value, or position in the supply chain
- Delivering quality services or goods includes being aware of and managing compliance risks. Compliance is an integral part of contract performance and quality delivery, not a separate administrative activity
- Laws and standards in countries outside the United States may vary; nevertheless, general awareness remains essential. Certain U.S. laws and contract requirements may continue to apply to overseas activities
- This training is intended to support awareness and risk recognition; specific obligations depend on contract terms and applicable law

## Government Contracting Basics: Accuracy and Integrity

### Be Accurate

- Perform due diligence before supplying information to anyone involved in government contracting. Employees involved in government contracting must ensure that information provided to the U.S. Government or prime contractors is accurate, complete, and not misleading, including:

**Proposals, certifications, and representations**

**Cost or pricing data**

**Timekeeping and labor charging**

**Technical and performance data**

- Explain clearly what the information does and does not include
- Estimates, projections and approximations must be presented as such

## Comply with Policies & Procedures

- Company policies and procedures help employees meet contract requirements and protect from enforcement risk
- Following policies and procedures is an important aspect of performing US Government contracts correctly, as many requirements fall outside of the contract itself (i.e. FAR and DFARS clauses, statutes and regulations)

## Abide by the Contract

- Includes all specifications, statements of work, and referenced documents
- Includes all contract clauses, including those incorporated by reference
- Fully explain and obtain customer concurrence for any contract requirements at risk of not being met before proceeding

## Report Concerns

- Encourage employees to speak up
- Follow mandatory disclosure requirements

## Mandatory Disclosures

- As a federal contractor, we have an obligation to make timely disclosures of certain misconduct
- Mandatory disclosures include violations of federal criminal law involving fraud, conflicts of interest, bribery, or gratuities under Title 18 of the United States Code; violations of the Civil False Claims Act related to the award, performance, or closeout of contracts or subcontracts; and significant overpayments received on a federal contract (other than contract financing payments)
- Certain conduct — such as inaccurate or improper time charging — may give rise to mandatory disclosure obligations when it involves fraud, false claims, false records, or knowing misrepresentations to the government
- Failure to make timely mandatory disclosure may lead to suspension or debarment
- Some agencies or contracts may impose broader or more specific disclosure requirements than the FAR baseline, based on mission needs or contractual terms

## Procurement Integrity

The Procurement Integrity Act (PIA) and related rules protect the integrity of the federal competitive process by restricting access to procurement-sensitive information and regulating post-government employment activities.

- Do not seek or accept procurement-sensitive information about competitors, such as source selection information or contractor bid or proposal information, unless you are explicitly authorized and it legitimately relates to performance of your contract obligations.
- Be cautious in contacts with current and former government personnel. Certain information received directly from government acquisition officials may be procurement sensitive and restricted from broader distribution. If you inadvertently receive non-public procurement information (electronically, in conversation, or attached to a public document), stop reviewing it immediately and report it in accordance with company policy.
- Be mindful of cooling-off periods for former government employees the company hires. These individuals may be temporarily barred from representing the company before the government or from involvement in certain projects related to their former government roles.

### Civil False Claims Act

The False Claims Act (FCA), also known as "Lincoln's Law," was enacted in 1863 to address rampant fraud during the Civil War. The FCA imposes treble damages and penalties on each count for knowingly submitting a false claim; causing a false claim (for example, falsifying a timecard even if you don't send the invoice yourself); making a false statement or record material to a false claim; or concealing — or knowingly and improperly avoiding or decreasing — an obligation to pay money or property to the Government.

Knowledge in FCA cases includes reckless disregard and deliberate ignorance. The Department of Justice recovers billions of dollars under the FCA each year and publishes recovery statistics annually.

FCA liability does not require that an individual know an action violates the FCA, or have specific intent to submit a false claim to the government.

Recent FCA developments reflect an increased emphasis on compliance clauses that are material to contract performance or payment, where noncompliance may give rise to FCA liability

FCA cases may be brought by the government itself or, uniquely, by private whistleblowers known as qui tam relators

## Human Rights and Workplace Obligations

### Harassment-Free Workplace and Non-Discrimination

Harassment and discrimination undermine a professional work environment. Certain forms are prohibited by law.

Even conduct that may not be unlawful can be demeaning, disruptive, and damaging to workplace productivity.

All employees should conduct themselves professionally and respectfully. Conduct that is discriminatory, harassing, or otherwise inappropriate in the workplace is not acceptable.

Legal requirements may vary by jurisdiction. Concerns should be raised promptly through appropriate reporting channels so they can be reviewed and addressed.

Threats, intimidation, or violence in the workplace are not acceptable. Promptly report any threats, suspicious behavior, or violent incidents through company channels.

Working under the influence of alcohol, illegal drugs, or any substance that impairs job performance is prohibited. Misuse of legal medications in a way that affects work also raises safety concerns and should be addressed through appropriate channels.

### Combating Human Trafficking

As a federal contractor, you may have an obligation to comply with FAR 52.222-50, Combating Trafficking in Persons, which implements federal anti-trafficking laws and policy through the government contracting process. Compliance plan thresholds and related requirements may vary based on contract terms and agency-specific deviations.

If this requirement applies to your business, it may include:

- Maintaining a compliance plan that includes an employee awareness program
- Informing employees about the U.S. Government's policy prohibiting trafficking-related activities, the conduct that is prohibited, and the actions that may be taken for violations
- Implementing reporting and response processes consistent with contract requirements

FAR 52.222-50 references the Department of State Office to Monitor and Combat Trafficking in Persons as a source of information and examples of awareness programs.

### Environmental Safety & Health

Providing a safe and healthy work environment is a shared responsibility and an important part of contract performance.

General expectations include:

- Maintaining a safe work environment for employees and applicable third parties
- Posting required safety warnings and notices
- Promptly reporting accidents, injuries, and environmental, safety, or health concerns
- Complying with applicable environmental, health, and safety standards, which may vary by country, location, and contract

Environmental responsibilities may also include managing materials appropriately and following requirements related to their storage, use, handling, and disposal.

Employees are expected to support responsible practices, including efforts to reduce waste and conserve energy, water, and raw materials.

## International Trade Compliance

Export and import control laws are designed to protect national and economic security and foreign policy objectives.

### What constitutes an export?

- Taking or sending an item or sensitive data out of the country
- Disclosing sensitive information (including oral or visual) to a foreign person — be mindful of electronic transmission

Penalties for export-control violations can be significant — to both the company and individual employees. When in doubt, contact your Trade Compliance or Legal function before sharing technical data, hosting foreign visitors, traveling internationally with sensitive items, or working with non-US suppliers. Obtain US government approval before sharing export controlled information with any non-US person in the US or abroad.

## Responsibilities: To Business Partners

### Quality

Strict compliance with all contract requirements — including conformance with specifications and quality requirements — is essential. FAR 52.246-2 imposes the following obligations on the contractor:

- Provide and maintain an inspection system acceptable to the Government
- Present for acceptance only supplies that have been inspected in accordance with that system and meet contract requirements
- Prepare records evidencing all inspections; those records must be complete and available to the Government during contract performance and for as long afterward as the contract requires

Any change to a contract requirement must be communicated to the customer in advance and approved before implementation.

## Counterfeit Parts

Your counterfeit electronic part detection and avoidance system must meet specific criteria. Contract clause (DFARS 252.246-7007) requires the contractor to address the following areas:

**Training of personnel**

**Electronic part traceability back to the original manufacturer**

**Reporting and quarantining of suspect parts**

**Due diligence of sources**

Be sure your detection and avoidance system meets ALL the specific elements outlined in the clause.

## Small Business Programs & Audit / Records Access

Small businesses, as well as primes who do business with SBA-certified small businesses under 8(a) and other programs, must understand unique compliance implications.

### *Small Business Program Compliance*

When performing under a small business contract or joint venture:

- Work must be performed consistent with the representations made to the Government regarding size status, ownership, and control
- Limitations on subcontracting requirements may apply, restricting how much work can be subcontracted to other entities
- In a joint venture or mentor-protégé arrangement, employees should understand which entity is performing the work, how labor should be charged, and which company's systems and controls apply
- Reporting to the Government (e.g., subcontracting reports or program status reports) must be accurate and supported by underlying documentation

Misrepresentation of small business status or failure to comply with performance requirements can result in contract termination, False Claims Act exposure, or suspension and debarment.

### *Audits & Records Access*

Government contracts often include audit and records access clauses. Agencies such as DCAA, DCMA, or Inspectors General may review:

- Timekeeping and labor charging
- Cost accounting and billing practices
- Subcontracting performance
- Compliance with small business program requirements

Employees are expected to:

- Maintain accurate, complete, and contemporaneous records
- Ensure time and costs are recorded correctly and supported
- Cooperate professionally with authorized auditors through proper company channels
- Never alter, conceal, or destroy records in anticipation of an audit

Records supporting contract performance must be retained in accordance with applicable contract clauses and regulatory requirements.

## Cost Principles & Pricing Integrity

Not all government contracts are subject to the same cost accounting rules. Some contractors and contracts are subject to the Cost Accounting Standards (CAS), while others, particularly certain small businesses or commercial item contracts, may not be. Cost-reimbursable, negotiated contracts may be subject to specific pricing rules.

### *Allowable vs. Unallowable Costs*

The Federal Acquisition Regulation (FAR Part 31) identifies which costs may be charged to the Government.

**Common unallowable costs include:**

**Alcohol and entertainment**

**Certain advertising or promotional expenses**

**Fines and penalties**

**Costs not allocable to contract performance**

Employees should ensure that only costs properly related to contract performance are charged to the appropriate project and that personal or unrelated expenses are never billed to the Government.

### *Truthful Cost or Pricing Data & Proposal Integrity*

For certain negotiated contracts, the company may be required to certify that cost or pricing data submitted to the Government is accurate, complete, and current. While employees may not sign these certifications, their work often supports the data submitted.

**Examples of information that may be included in proposals or negotiations:**

**Labor rates and historical time data**

**Vendor quotes or subcontractor pricing**

**Bills of materials**

**Cost estimates and projections**

Providing materially incomplete or misleading data, intentionally or through reckless disregard, can lead to defective pricing claims, contract price reductions, or enforcement action.

# Responsibilities: To Corporate Citizens

## Antitrust Laws

- Antitrust laws promote open and fair competition and protect against unlawful restraints, monopolies, and unfair business practices
- Antitrust laws, sometimes referred to as competition laws, prohibit conduct that undermines fair competition, including price fixing, bid rigging, market allocation, price discrimination, and other improper coordination or unfair trade practices
- Anticompetitive conduct can undermine the integrity of the procurement process and may result in investigations, significant civil or criminal penalties, contract remedies, and suspension or debarment
- Employees must avoid engaging in or discussing activities that may violate antitrust laws or create the appearance of improper coordination, such as:
  - Discussing pricing, bid strategies, or terms with competitors
  - Sharing non-public or competitively sensitive information

- Agreeing informally to divide customers, contracts, or markets
- Coordinating who will bid, how bids will be structured, or whether a company will bid at all

## Anti-Boycott Laws

US anti-boycott laws prohibit and penalize participating in or cooperating with, or agreeing to participate in or cooperate with, any boycott not sanctioned by the US government — most notably the Arab boycott of Israel.

- The United States government has identified Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and Yemen as boycotting countries
- Other countries not listed by the US government, such as Oman, Pakistan, Bangladesh, and Indonesia also may impose boycott requirements — the Department of the Treasury maintains a list that is updated periodically
- Boycott-related requests may be reportable and prohibited or penalized under US law

Don't make any boycott-related agreement or provide any suspected boycott-related information. Report any suspected boycott-related requests.

## Anti-Corruption Laws

- Anti-corruption laws prohibit offering or providing money or anything of value to government officials or others to win new business, retain existing business, or obtain an improper business advantage
- Corruption can take many forms, including bribery, kickbacks, conflicts of interest, falsification of records, or misuse of government information, and may involve interactions with government officials, customers, subcontractors, suppliers, or other third parties
- Employees must comply with applicable anti-corruption laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and the U.K. Bribery Act
- Violations of anti-corruption laws can result in serious consequences, including investigations, suspension or debarment, loss of export privileges, and significant civil or criminal penalties, including imprisonment

Look for "red flags" and conduct due diligence before engaging the services of international sales representatives, consultants, distributors or other third parties.

## Kickbacks

- A kickback is any money, fee, commission, credit, gift, gratuity, thing of value, loan, entertainment, service, or other compensation provided, directly or indirectly, to a prime contractor, prime contractor employee, subcontractor, or subcontractor employee for the purpose of improperly obtaining or rewarding favorable treatment
- Kickbacks may involve prime contractors, subcontractors, employees, or agents at any tier
- Kickbacks are prohibited and may constitute criminal offenses under U.S. law and the laws of other countries

Do not offer, give, solicit or receive any form of bribe or kickback.

## Conflicts of Interest

A conflict of interest generally exists when you have divided loyalties — meaning personal, financial, or other interests interfere, or appear to interfere, with your ability to act objectively and in the best interests of the company.

A conflict of interest may arise when you have a direct or indirect personal interest that could:

- Influence, or reasonably appear to influence, your actions or judgment on behalf of the company
- Cause you to place personal or family interests ahead of the company's business interests

Conflicts of interest may arise in a variety of situations, including:

- Relationships with customers, competitors, suppliers, or business partners
- Relationships with current or prospective employees
- The acquisition or use of company assets, information, or opportunities for personal gain
- Outside employment, consulting, or other business activities

> ***General Guidelines***
> - Avoid actual conflicts of interest as well as situations that may create the appearance of a conflict
> - Do not pursue personal or family interests that conflict, or appear to conflict, with company business interests
> - Do not use your position, authority, or business relationships to advance personal or outside interests
> - Do not use company property, information, or opportunities for personal benefit
> - Be fair and impartial in all business dealings and disclose actual or potential conflicts of interest

## Gifts, Business Courtesies

- Avoid the perception that favorable treatment is being sought, received, or given in exchange for gifts or business courtesies
- Ensure that any gift or business courtesy offered or received is permitted by law and consistent with reasonable marketplace customs
- Confirm that a gift or business courtesy does not violate the rules, policies, or standards of conduct applicable to the recipient or the recipient's organization

> ***US Government Officials***
> Specific guidance located at the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635) imposes stricter limitations on the giving or offering of business courtesies to certain US government political appointees.
>
> **US Executive Branch (including military personnel)**
> - $20 USD or less on a single occasion, and collectively no more than $50 USD in a calendar year from your entire company
> - The $20 USD / $50 USD limit cannot be adjusted by allowing that individual to pay the dollar amount that exceeds either threshold
> - Modest refreshments at a business meeting are allowed, but generally the contractor cannot pay for government employees' meals absent specific, narrow exceptions (i.e. widely attended gathering)
>
> **US Legislative Branch Employees (Congressional Representatives and Senators and their staffs)**
> - The default is no gifts, with narrow, fact-specific exceptions including widely attended gatherings and commemorative items
> - Modest value food and refreshments may be acceptable, provided they are offered to a broad group and not targeted to influence a specific individual
> - Dollar thresholds and exceptions vary based on the source, the nature of the event, and applicable ethics rules; employees should not assume permissibility based on value alone

**US Judiciary (US Supreme Court, US Courts of Appeals, and US District Courts)**

- Strict rules and generally prohibited

***Foreign Officials***

- Do not provide hospitality to foreign officials, except as authorized by local hospitality policies and hospitality rules for foreign officials for each country where you do business
- Subject to the requirements of local law, certain expenses incurred by foreign government officials in order to explain, demonstrate or promote company business are acceptable if they are reasonable and bona fide
- Facilitating or "grease" payments are generally prohibited
- Seek legal guidance to distinguish between dealing with foreign officials covered under the Foreign Corrupt Practices Act and commercial partners (private or state-owned) governed by other laws and policies

# Responsibilities: To Shareholders and Other External Stakeholders

## Accurate Business Records

We are responsible for creating and maintaining accurate and complete business records, including reports filed with the Securities and Exchange Commission or other regulatory authorities, as well as information used for internal decision-making, contract performance, and billing.

Ensuring accurate business records includes:

- Understanding and following applicable timekeeping and labor-charging policies at your work location
- Properly recording and accounting for all costs, including labor, travel, materials, and other expenses
- Ensuring that statements, communications, and representations to customers, suppliers, and partners are accurate and not misleading
- Never misrepresenting facts, omitting material information, or falsifying records

## Information Protection

We are entrusted with sensitive information belonging to our company, customers, suppliers, and other partners.

Mishandling sensitive information can harm national security, damage our reputation and relationships, and expose both individuals and the company to legal risk, including fines and penalties.

When conducting business internationally, additional requirements may apply, such as export controls, privacy laws, and specific information handling and safeguarding obligations.

Handle, store, and protect sensitive information in accordance with applicable laws, contracts, and company policies:

- Obtain proper authorization before disclosing or receiving such information, internally or through a third party (like a supplier, customer or competitor)
- Only access personal information or personal data for legitimate business purposes
- Safeguard the confidentiality of employee records and information
- Prior to disclosing classified or other controlled information, ensure that recipients are properly authorized, have a valid need to know, and that the information is shared only through approved systems and methods
- Controlled Unclassified Information has become a heightened area of risk because it is less obvious than classified information and can span many aspects of contract performance, including technical data

- Use caution when communicating or posting on social media to avoid disclosing sensitive or proprietary information

### Artificial Intelligence (AI)

AI tools can support productivity, but introduce new compliance risks when used carelessly.

- Do not enter confidential, personal, export-controlled, or other sensitive information into public AI tools (such as consumer chatbots)
- Treat AI outputs as drafts to review and verify — AI can produce inaccurate or biased information
- Follow Company AI policy and any function-specific restrictions on AI use

### Cybersecurity Hygiene

Day-to-day security habits protect Company, customer, and contract information.

- Use strong passwords and multi-factor authentication on company accounts
- Recognize and report phishing or suspicious messages—do not click unknown links or open unexpected attachments
- Use removable media (USB drives, external storage) only as authorized by Company policy
- Report suspected cyber incidents promptly through company channels

Treat cybersecurity as part of contract performance — small lapses can have significant consequences.

### Insider Trading

- Insider trading laws prohibit buying or selling securities while in possession of material, nonpublic information
- "Securities" include stocks, stock options, bonds, notes, debentures, put or call options
- "Trading" means buying or selling a security — for example, trading in the open market, or in company plans, like employee stock options or retirement savings plans
- Information, both positive and negative, is "material" if there is a substantial likelihood that a reasonable investor would consider it important in deciding whether to trade a security
- Information may be material even if it relates to events that are expected or merely possible
- Information is considered "nonpublic" until it has been widely disseminated, such as through the news or an official announcement, and enough time has passed for the information to be assimilated by the general public, typically one business day
- Do not buy or sell securities while you are in possession of material, nonpublic information

## Responsibilities: Doing the Right Thing

### Suspension and Debarment

Suspension and debarment are administrative actions used to protect the Government from contractors that lack present responsibility.

- Suspension is a temporary exclusion from new Government contracts while an investigation or legal proceeding is pending
- Debarment is an exclusion from Government contracting for a specified period, often three to five years, based on a determination of lack of business integrity or responsibility

Causes for suspension or debarment may include:

- Criminal convictions or civil judgments involving fraud or false claims
- False statements or falsification of records
- Other conduct indicating a lack of business honesty or integrity

A contractor may be suspended or debarred for misconduct even if it does not arise directly from Government contract performance, such as export control violations, environmental noncompliance, tax offenses, or false records.

Evidence of a strong ethics and compliance program helps mitigate the risk of misconduct and potential suspension or debarment if misconduct does occur.

### Whistleblower Protection Act

Whistleblower protection laws prohibit retaliation against employees or applicants who raise concerns or report suspected misconduct.

Protected disclosures may include reports of:

- Violations of law, rule, or regulation
- Gross waste of funds or gross mismanagement
- Abuse of authority
- Substantial and specific dangers to public health or safety

Retaliation or threats of retaliation are prohibited. Employees are encouraged to raise concerns in good faith and in accordance with company policy.

Applicable poster and notice requirements, including Department of Defense hotline postings, must be followed.

## Conclusion

**Government contracting rules, regulations and procedures prescribe how you do business with the government and...**

**The rules for supporting US Government contracts are complex.**
**The penalties for non-compliance can be severe.**

**Establishing and promoting a strong ethics and compliance program is a proven approach.**

**The Defense Industry Initiative toolkit can help.**

*Disclaimer: This document is for reference only and to be used at the consumer's own risk. The Defense Industry Initiative (DII) disclaims any and all liability for any consequences arising out of your use of this document. DII does not guarantee that any or all aspect of this document has been updated to reflect any changes or developments in the law. As such, DII is not responsible for any subsequent regulatory or legal changes that may render this document obsolete. By posting this document, DII is not providing legal advice and is not agreeing to enter into Conclusionionship. Please consult with legal counsel to advise you on establishing, maintaining, and auditing your compliance program.*

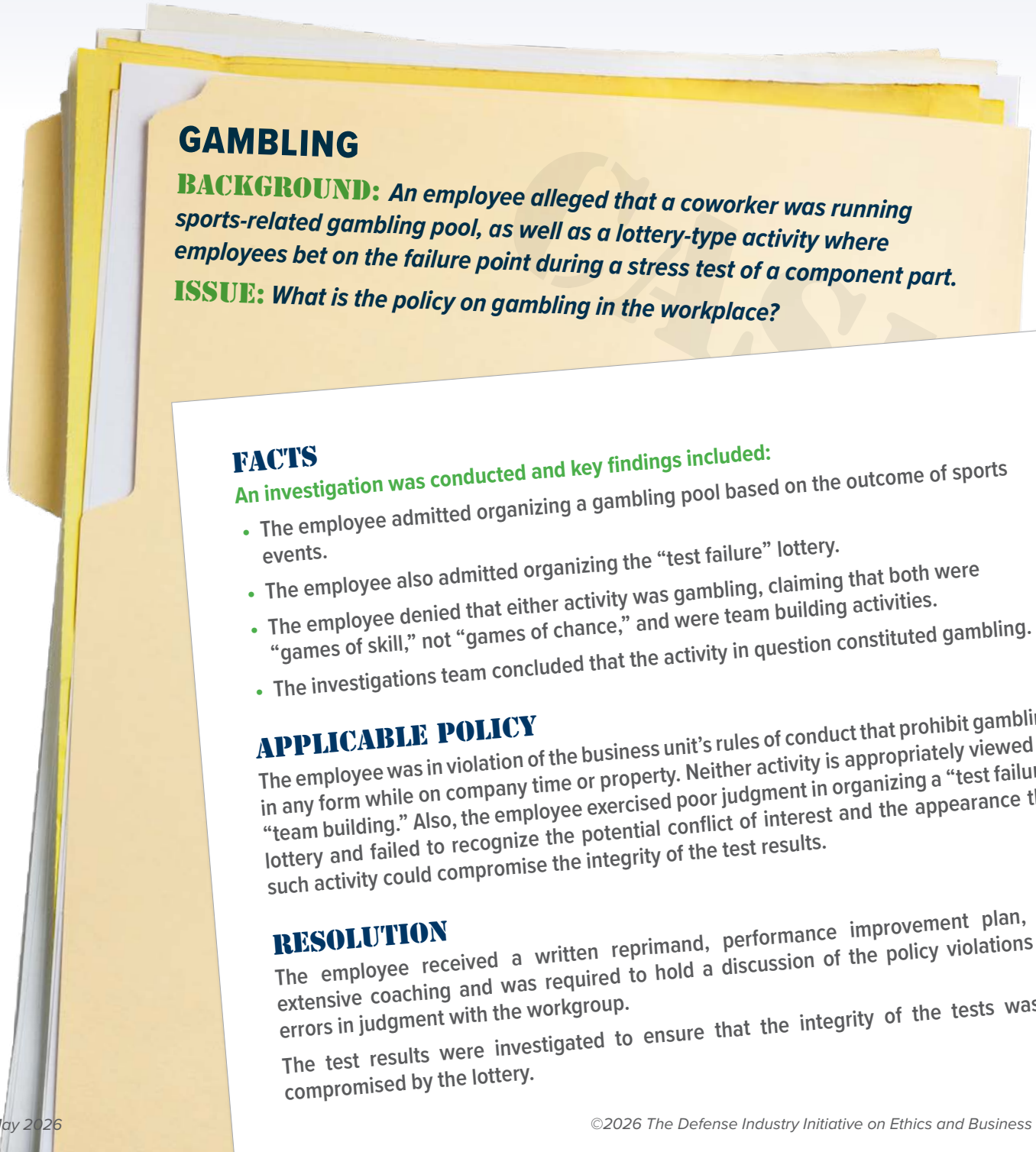
DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 3: ETHICS CASE FILES

**Sharing information about your investigations is a potential way to engage employees and provide a supplemental training method. Here is an example of an article format you may want to consider.**

**The following case files are example scenarios drawn from common ethics issues that can arise in the defense contracting space, along with how a company might investigate and resolve them. They are designed as a supplemental training tool, and can also serve as a model for the format you might use to share your own investigation outcomes with employees.**



## GAMBLING

**BACKGROUND:** ***An employee alleged that a coworker was running sports-related gambling pool, as well as a lottery-type activity where employees bet on the failure point during a stress test of a component part.***

**ISSUE:** ***What is the policy on gambling in the workplace?***

### FACTS

**An investigation was conducted and key findings included:**

- The employee admitted organizing a gambling pool based on the outcome of sports events.
- The employee also admitted organizing the "test failure" lottery.
- The employee denied that either activity was gambling, claiming that both were "games of skill," not "games of chance," and were team building activities.
- The investigations team concluded that the activity in question constituted gambling.

### APPLICABLE POLICY

The employee was in violation of the business unit's rules of conduct that prohibit gambling in any form while on company time or property. Neither activity is appropriately viewed as "team building." Also, the employee exercised poor judgment in organizing a "test failure" lottery and failed to recognize the potential conflict of interest and the appearance that such activity could compromise the integrity of the test results.

### RESOLUTION

The employee received a written reprimand, performance improvement plan, and extensive coaching and was required to hold a discussion of the policy violations and errors in judgment with the workgroup.

The test results were investigated to ensure that the integrity of the tests was not compromised by the lottery.

# FALSIFICATION OF RECORDS (NON-FINANCIAL)

**BACKGROUND:** *An employee was suspected to have forged several documents in connection with a medical leave of absence.*

**ISSUE:** *What constitutes falsification of records?*

## FACTS

**An investigation was conducted and key findings included:**

- The employee had a long history of absences from work for a variety of reasons.
- Over several months, the employee submitted documents requesting paid medical leave.
- The documents contained signatures, purportedly of the employee's attending physician.
- The signatures on the documents did not match known examples of the physician's signature.
- The medical department noted that forging a physician's name on medical forms is a criminal offense and that the doctor's office had notified the police.
- The employee admitted signing the physician's name on the medical leave documents, claiming to be under stress from work and stating, "I know what I did was wrong."
- The investigations team concluded that the activity in question constituted gambling.

## APPLICABLE POLICY

The employee violated our Code of Conduct and corporate policies, which state that we will conduct business with honesty and integrity, and in compliance with the laws of the United States and of each country which the Corporation operates.

## RESOLUTION

The employee was discharged from employment.

# COMPUTER MISUSE

**BACKGROUND:** *An employee was suspected of sending vulgar electronic messages over company messaging platforms to an individual outside of the company.*

**ISSUE:** *What constitutes harassment and inappropriate use of company communications tools?*

## FACTS

**An investigation was conducted and key findings included:**

- Several instant messages had been sent from the employee's workstation to a person outside of the company.
- The messages included the use of vulgar sexual language that was demeaning and disrespectful of women.
- The employee admitted to sending the messages, apologized and stated, "It will never happen again."

## APPLICABLE POLICY

The conduct violated the Company's Non-Harassment Policy, which prohibits verbal, written, or visual conduct of a sexual nature that is unwelcome or that creates a hostile work environment, whether delivered in person or through electronic communications.

## RESOLUTION

The employee was suspended without pay, required to complete harassment-prevention training before returning to work, and placed under a 12-month performance review tied to conduct expectations. The matter was also referred to Human Resources for separate review under the Non-Harassment Policy.

# TIME SHEET MISUSE

**BACKGROUND:** *An employee was suspected of charging time to a contract on a day for which he was not in the office.*

**ISSUE:** *Did the employee mischarge his time?*

## FACTS

**An investigation was conducted and key findings included:**

- A review of the timesheets noted that the employee had charged time to the contract on the days in question.
- Interviews of the employee's office mates confirmed that the employee was not seen in the office on those same days.
- The employee had posted photos of himself on Facebook that showed he was out-of-state during the days in question.
- During his interview, the employee admitted to not have been in the office on the days for which he had charged the contract. When asked why he had done that, the employee explained that he had traveled out-of-state to attend a wedding via non-refundable plane tickets and had no time left in his leave bank.

## APPLICABLE POLICY

The employee violated Company policy 5k, Time Charging, which prohibits charging time to a contract for which work had not been performed. In addition, the conduct may have and triggered Company's evaluation under FAR 52.203-13 for potential mandatory disclosure to the cognizant agency Inspector General and Contracting Officer.

## RESOLUTION

The employee was terminated.

# UNAUTHORIZED DISCLOSURE OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)

**BACKGROUND:** *An engineer working under a tight deadline emailed technical drawings to a subcontractor to expedite performance.*

**ISSUE:** *Was CUI handled appropriately?*

## FACTS

**An investigation was conducted and key findings included:**

- The drawings were clearly marked as Controlled Unclassified Information.
- The subcontractor had not yet completed required cybersecurity onboarding and had not been authorized to receive controlled data.
- The employee was aware of the onboarding delay.
- Rather than wait for approval, the employee sent the drawings through standard company email without encryption in order to "keep the schedule moving."
- During the interview, the employee acknowledged knowing the subcontractor was not yet cleared to receive CUI but stated, "It would have taken weeks, and we needed them to start now."
- There was no evidence of external compromise.

## APPLICABLE POLICY

Company policy and contract requirements mandate safeguarding CUI and prohibit sharing controlled information with third parties that have not completed required security onboarding.

## RESOLUTION

The employee was suspended without pay for intentionally bypassing established security controls. The employee was required to complete additional training on information handling requirements prior to returning to work. The company reinforced expectations regarding schedule pressure and security compliance and reviewed onboarding timelines to identify process improvements.

# FAILURE TO VALIDATE AI-GENERATED TECHNICAL CONTENT

**BACKGROUND:** *An engineer supporting a competitive proposal used an AI tool to help draft portions of the technical volume and compliance matrix.*

**ISSUE:** *Were representations to the government adequately reviewed and verified before submission?*

## FACTS

**An investigation was conducted and key findings included:**

- The engineer used an AI tool to generate draft responses describing the system's compliance with certain performance specifications.
- Portions of the AI-generated language overstated system capabilities and suggested testing had been completed when it had not.
- The engineer copied the language into the proposal without independently verifying each technical claim.
- The proposal was submitted to the government with the inaccurate statements included.
- The discrepancies were identified during post-award technical discussions.

## APPLICABLE POLICY

Company policy requires that all technical, cost, and performance representations submitted to the government be accurate and verified. Use of automated tools does not relieve employees of their obligation to ensure submissions are complete and correct.

## RESOLUTION

Following review, the employee's employment was terminated for failure to exercise due diligence and for submitting inaccurate representations to the government. The company conducted a root cause review, strengthened proposal review controls, and issued updated guidance clarifying that AI-generated content must be independently validated prior to submission.

# ORGANIZATIONAL CONFLICT OF INTEREST (UNEQUAL ACCESS TO INFORMATION)

**BACKGROUND:** *A business unit provided advisory support to a government office developing technical requirements for a future procurement.*

**ISSUE:** *Did the company create a potential OCI by bidding on the resulting contract?*

## FACTS

**An investigation was conducted and key findings included:**

- The advisory team had access to draft acquisition planning documents.
- A separate internal team prepared a proposal for the follow-on effort.
- While there was no evidence of improper data sharing, no formal firewall documentation had been implemented.
- The proposal did not disclose the prior advisory role.

## APPLICABLE POLICY

Company policy requires early identification and mitigation of potential organizational conflicts of interest and accurate disclosures in proposals.

## RESOLUTION

The company submitted an updated OCI disclosure and mitigation plan. Internal procedures were strengthened to require documented firewalls and early legal review when supporting acquisition planning efforts.

# BUSINESS MEALS WITH GOVERNMENT PERSONNEL

**BACKGROUND:** *An employee met with a government counterpart while traveling for a program review.*

**ISSUE:** *Was the meal consistent with gift and gratuity rules?*

## FACTS

**An investigation was conducted and key findings included:**

- The employee paid for lunch for both parties at a modest restaurant.
- The total cost per person was below the federal gift threshold.
- The employee did not seek prior guidance or document the meal.
- The discussion included both personal catching up and ongoing contract performance issues.

## APPLICABLE POLICY

Company policy requires compliance with federal gift and ethics rules and encourages seeking guidance when interacting with government personnel. Federal employee gift rules under 5 C.F.R. § 2635 set per-event and aggregate annual limits, but cost alone does not resolve the analysis: paying for a meal while discussing active contract performance can create an appearance of seeking to influence an official act, even where the value is within limits. Employees should obtain advance guidance from the Ethics Office, contemporaneously document the business purpose, and avoid substantive contract discussions in any setting where a Company-paid courtesy is being extended.

## RESOLUTION

The employee was counseled on documenting interactions with government officials and seeking advance guidance when appropriate.

# IMPROPER COMMUNICATIONS DURING SOURCE SELECTION

**BACKGROUND:** *An employee serving as a capture lead maintained a longstanding professional relationship with a government program manager overseeing an active procurement.*

**ISSUE:** *Did the employee engage in improper communications during an active source selection?*

## FACTS

**An investigation was conducted and key findings included:**

- During the active source selection period, the employee exchanged multiple text messages and phone calls with the program manager.
- In those communications, the employee discussed aspects of the company's staffing plan and asked whether "greater emphasis on incumbent retention" would be viewed favorably.
- The employee also shared general observations about competitor strengths and weaknesses.
- The employee was under significant internal pressure to secure the contract due to projected revenue shortfalls in the business unit.

## APPLICABLE POLICY

Company policy and federal procurement integrity requirements prohibit unauthorized communications with government personnel during an active source selection and restrict discussion of proposal-related information outside approved channels.

## RESOLUTION

The employee's employment was terminated for knowingly engaging in prohibited communications during an active procurement. The company conducted a broader review of capture procedures and reinforced training on source selection communication restrictions across all business units.

# SUBCONTRACTOR WITH RESTRICTED ENTITY CONCERNS

**BACKGROUND:** *A supply chain employee recommended a new overseas vendor to reduce lead times.*

**ISSUE:** *Was appropriate due diligence conducted?*

## FACTS

**An investigation was conducted and key findings included:**

- Initial screening identified a corporate affiliate operating in a sanctioned jurisdiction.
- The recommending employee stated they were unaware of the affiliation.
- Procurement due diligence documentation was incomplete.

## APPLICABLE POLICY

Company policy requires screening third parties against restricted party lists and documenting due diligence.

## RESOLUTION

The vendor onboarding was paused pending review. Procurement procedures were updated to require documented compliance clearance before vendor approval.

# USE OF GENERATIVE AI IN PROPOSAL DEVELOPMENT

**BACKGROUND:** *A proposal writer used a publicly available AI tool to draft portions of a technical narrative.*

**ISSUE:** *Was sensitive information improperly shared?*

## FACTS

**An investigation was conducted and key findings included:**

- The employee entered non-public program details into the AI platform to generate draft language.
- The platform's terms of service permitted data retention.
- The employee believed the tool improved efficiency and did not consider data security implications.

## APPLICABLE POLICY

Company policy restricts uploading non-public or controlled information into unapproved third-party systems.

## RESOLUTION

The draft was reviewed for data exposure risk. Additional guidance was issued clarifying acceptable AI tool usage.

# UPLOADING GOVERNMENT DATA TO UNAPPROVED CLOUD PLATFORM

**BACKGROUND:** *A project team used a commercial file-sharing service to collaborate with a government customer.*

**ISSUE:** *Was the platform authorized under contract requirements?*

## FACTS

**An investigation was conducted and key findings included:**

- The platform had not been approved for handling sensitive government data.
- The files contained performance metrics designated as sensitive but unclassified.
- The team believed the tool was acceptable because it was widely used in industry.

## APPLICABLE POLICY

Contract clauses and company cybersecurity policies require use of approved systems for storing government data.

## RESOLUTION

Files were migrated to an approved environment. IT controls were updated to restrict unauthorized file-sharing platforms.

# MANAGER DISCOURAGING REPORTING

**BACKGROUND:** *An employee raised concerns about potential mischarging practices.*

**ISSUE:** *Was the employee's concern appropriately handled?*

## FACTS

**An investigation was conducted and key findings included:**

- The employee informed a supervisor of possible timekeeping inconsistencies.
- The supervisor responded that the issue was "minor" and suggested not escalating it.
- The employee later reported the matter through the ethics hotline.

## APPLICABLE POLICY

Company policy prohibits retaliation and requires that concerns be elevated through appropriate channels.

## RESOLUTION

The supervisor was issued a final written warning and suspended without pay for failing to elevate a reported concern and for discouraging use of established reporting channels. The supervisor was required to complete additional training on non-retaliation and escalation obligations. Leadership conducted follow-up discussions with the workgroup to reinforce the company's commitment to a speak-up culture and the expectation that all concerns be taken seriously and reported through appropriate channels.

# INTERNAL INVESTIGATION LACKED INDEPENDENCE

**BACKGROUND:** *A business unit conducted an internal review of alleged policy violations involving a senior manager.*

**ISSUE:** *Was the investigation sufficiently independent?*

## FACTS

**An investigation was conducted and key findings included:**

- The review was led by an HR manager who reported to the accused individual.
- No legal or compliance oversight was involved.
- The review concluded without documented witness interviews.

## APPLICABLE POLICY

Company policy requires impartial and appropriately overseen investigations into alleged misconduct.

## RESOLUTION

The matter was reopened under compliance leadership. Investigation protocols were clarified to ensure independence and documentation standards.

# UNDISCLOSED PERSONAL CONFLICT OF INTEREST

**BACKGROUND:** *An employee serving as the technical lead on a sustainment program participated in vendor selection for a new instrumentation subcontract. The employee's spouse was a senior account manager at one of the bidding firms.*

**ISSUE:** *Did the employee have a personal conflict of interest that required disclosure and recusal?*

## FACTS

**An investigation was conducted and key findings included:**

- The employee participated in source list development, technical scoring, and award recommendation discussions.
- The relationship was not disclosed on the employee's annual Conflict of Interest certification or to the contracting team.
- The spouse received variable compensation tied to the bidding firm's award activity.
- The bidding firm was awarded the subcontract; performance issues subsequently triggered an internal review that surfaced the relationship.
- The employee stated the relationship had been disclosed verbally to a manager years earlier and had been forgotten.

## APPLICABLE POLICY

Company policy and FAR 52.203-16 require employees in covered positions to identify and disclose any personal, financial, or family interest that could reasonably appear to influence the employee's judgment in the performance of Company work, and to recuse from related decisions until the conflict is mitigated. Annual COI certifications must be complete and accurate, and reaffirmed when circumstances change.

## RESOLUTION

The employee was removed from the program and issued a final written warning. The subcontract award was reviewed for procurement integrity; no evidence of improper influence on scoring was found, but the affected procurement documentation was annotated. Annual COI certification language was strengthened to include immediate-family employment, and managers received refresher training on recognizing and escalating disclosed conflicts.

# IMPROPER BUSINESS COURTESY TO A FOREIGN GOVERNMENT OFFICIAL

**BACKGROUND:** *A logistics coordinator supporting an overseas program was responsible for clearing test equipment through the host-country customs authority before a scheduled demonstration.*

**ISSUE:** *Was a payment offered to a foreign government official permissible under Company policy and applicable anti-corruption laws?*

## FACTS

**An investigation was conducted and key findings included:**

- The shipment was held at customs and the demonstration date was at risk.
- A customs official suggested that a cash payment of approximately $200 would result in the shipment being released the same day.
- The coordinator approved the payment from a petty cash account and recorded it as a "miscellaneous clearance fee."
- The payment was not reviewed by the Ethics Office, the Trade Compliance team, or Legal in advance.
- The coordinator stated the payment was "just a facilitating payment" and a routine cost of doing business in the region.

## APPLICABLE POLICY

Company policy and the Foreign Corrupt Practices Act prohibit offering, promising, or giving anything of value to a foreign official to obtain or retain business or any improper advantage. Company policy also prohibits facilitating or "grease" payments, even where local practice tolerates them. All interactions with foreign officials must be transparent, accurately recorded in the books and records, and pre-cleared through Ethics, Trade Compliance, or Legal.

## RESOLUTION

The employee's employment was terminated. The payment was disclosed internally, reviewed by Legal, and reported through Company's voluntary disclosure channels.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 4: OTHER ETHICS & COMPLIANCE RESOURCES

**This resource provides a curated list of ethics and compliance resources for federal defense contractors. It is not intended to collect every available article or training tool. Instead, it highlights foundational laws, regulations, government guidance, benchmarking resources, and select external materials that are likely to remain useful over time.**

## Laws, Regulations, and Government Guidance

### FAR 52.203-13 — Contractor Code of Business Ethics and Conduct

> This contract clause is one of the most important compliance clauses for federal contractors. It requires covered contractors to maintain a written code of business ethics and conduct, promote an ethical culture, exercise due diligence to prevent and detect criminal conduct, and make timely written disclosures when the contractor has credible evidence of certain criminal violations or civil False Claims Act violations. It also addresses internal controls, anonymous or confidential reporting mechanisms, discipline, corrective action, and cooperation with government audits and investigations.
>
> *https://www.acquisition.gov/far/52.203-13*

### U.S. Sentencing Guidelines, Chapter 8 — Sentencing of Organizations

> Section 8B2.1 describes the elements of an effective compliance and ethics program, including standards and procedures, high-level oversight, due diligence in delegation of authority, training and communication, monitoring and auditing, reporting mechanisms, discipline, and appropriate response and remediation.
>
> *https://www.ussc.gov/guidelines*

### DOJ Evaluation of Corporate Compliance Programs

> The DOJ Evaluation of Corporate Compliance Programs is one of the most important government guidance documents for assessing whether a compliance program is well designed, adequately resourced and empowered, and working in practice. It is useful for benchmarking codes of conduct, reporting mechanisms, investigations, discipline, third-party management, training, risk assessments, and compliance program testing.
>
> *https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl*

### DOJ Corporate Enforcement and Voluntary Self-Disclosure Policy

> This new DOJ policy explains how the Department evaluates voluntary self-disclosure, cooperation, remediation, and aggravating circumstances in corporate criminal matters. Contractors should track it because disclosure decisions, cooperation posture, remediation, and documentation can affect enforcement outcomes if misconduct arises.
>
> *https://www.justice.gov/dag/media/1430731/dl?inline*

### U.S. Office of Government Ethics

The U.S. Office of Government Ethics provides ethics rules, guidance, advisories, training materials, and resources for federal executive branch employees. While OGE rules apply to government personnel rather than contractors, contractors should understand them because many procurement integrity, gifts, conflicts, source selection, and post-government employment issues involve interactions with federal employees.

*https://oge.gov/*

### DoD OIG Contractor Disclosure Program

The DoD OIG Contractor Disclosure Program provides information for contractors making disclosures to the Department of Defense. It is directly relevant to contractors subject to FAR 52.203-13 and to companies evaluating how to make mandatory disclosures involving credible evidence of covered criminal violations or civil False Claims Act violations.

*https://www.dodig.mil/Programs/Contractor-Disclosure-Program/*

### DoD OIG Contractor Disclosure Program Brochure

This DoD OIG brochure provides a practical overview of the Contractor Disclosure Program and how contractors may submit disclosures to the DoD OIG. It is useful as a practical companion to FAR 52.203-13 and internal mandatory disclosure procedures.

*https://www.dodig.mil/Portals/48/10082025-DoW-OIG-Contractor-Disclosure-Program-Brochure-05%20%28DoW%29.pdf*

## Industry Associations and Benchmarking

### Ethisphere

Ethisphere provides ethics and compliance benchmarking, culture assessment tools, program assessments, events, and resources, including materials connected to its "World's Most Ethical Companies" recognition and Business Ethics Leadership Alliance. Some resources are public, but many benchmarking tools, assessments, and member resources require payment or membership.

*https://ethisphere.com*

### Society of Corporate Compliance and Ethics (SCCE)

SCCE is a major professional association for compliance and ethics professionals. It offers conferences, certifications, training, publications, webinars, and practical resources on compliance program design, investigations, reporting systems, risk assessment, auditing, monitoring, and compliance leadership. Many resources require membership, registration, or payment.

*https://www.corporatecompliance.org/*

### Ethics & Compliance Initiative (ECI)

ECI provides ethics and compliance research, benchmarking, surveys, working groups, and best-practice resources. Its materials are useful for companies assessing ethical culture, reporting trends, retaliation risk, program maturity, and employee perceptions of compliance programs. Some resources are public, while others require membership or payment.

*https://eci-insights.com/*

## Other

### V2X Ethics and Compliance Materials (Attached)

V2X public ethics and compliance materials may be useful as a contractor-facing example of how a defense contractor explains ethics responsibilities, reporting channels, investigations, and compliance expectations. These materials may be particularly useful for practical examples involving "who is ethics," case examples, compliance metrics, and the investigation lifecycle.

### Lockheed Martin Ethics and Business Conduct Resources

Lockheed Martin's public ethics materials are useful as a reference point for how a major defense contractor communicates ethics expectations, reporting channels, leadership accountability, and employee responsibilities. These materials should be used as examples rather than copied as templates.

*https://www.lockheedmartin.com/en-us/who-we-are/ethics.html*

### NAVEX Benchmarking Reports

NAVEX publishes benchmarking and risk/compliance reports, including whistleblowing and incident management benchmarks, risk and compliance statistics, regional whistleblowing data, state of risk and compliance reports, and small-to-medium-sized business compliance data. These reports can help companies compare hotline use, reporting volume, substantiation rates, case closure timing, reporting channels, and program maturity against broader industry data. Some reports may require registration.

*https://www.navex.com/en-us/resources/reports/*

# 2025 ETHICS & COMPLIANCE IN ACTION ANNUAL REPORT

In support of our customers, partners, and missions, V2X operates with integrity at every level. This year-end report highlights how ethics and compliance guide decisions, strengthen accountability, and reinforce trust across the organization.



2100 Reston Parkway
Suite 300
Reston, VA 20191
USA

+1 571.481.2000
www.gov2x.com

# TABLE OF **CONTENTS**




**"Acting with integrity, honoring our values, and maintaining a strong culture of ethics and compliance are essential to who we are and how we succeed together."**

"At V2X, we believe that doing what's right is not just a standard it's a responsibility we all share. Acting with integrity, honoring our values, and maintaining a strong culture of ethics and compliance are essential to who we are and how we succeed together.

Each of us plays a role in creating a workplace where concerns can be raised openly and respectfully. When something doesn't feel right, speaking up helps us address issues early, learn from them, and strengthen the trust that employees, customers, and partners place in us. Your voice helps shape a better, safer, and more accountable organization.

As you review the Ethics and Compliance in Action: Annual Report 2025, I encourage you to reflect on the importance of our collective commitment. Thank you for the integrity you bring to your work every day. Together, we continue to grow, improve, and uphold the values that define our organization."

**Jeremy C. Wensinger**
President and Chief Executive Officer





# ETHICS AND COMPLIANCE IN ACTION: **ANNUAL REPORT 2025**

At our organization, Ethics and Compliance remain central to who we are and how we work. Our values guide every decision we make, shaping not only what we accomplish but the way we treat one another along the way. Upholding these principles is a shared responsibility—one that reflects our commitment to operating with integrity and earning trust at every level of the company.

Our Ethics and Compliance resources exist to support a culture where concerns can be raised openly, respectfully, and without fear of retaliation. When employees share their questions, observations, or concerns, they play a direct role in strengthening our ethical foundation. Speaking up helps us identify potential risks early, respond thoughtfully, and maintain a workplace where transparency is expected and supported.

This annual report provides a look back at our 2025 activity, offering insights into the trends, data, and themes that shaped our Ethics and Compliance efforts over the past year. It highlights how our processes function, how concerns are managed, and how our collective actions contribute to a strong, resilient culture.

As we move forward, we encourage every employee to continue engaging in these conversations. If something doesn't seem right, your voice matters. Together, we reinforce the standards that define us and continue building an environment where doing what's right is at the heart of everything we do.



# FREQUENTLY ASKED **QUESTIONS**

These frequently asked questions are intended to provide a clearer understanding of Ethics and Compliance, how concerns are reviewed, and when employees should seek guidance or raise a concern. Together, they help reinforce transparency, accountability, and a culture where doing the right thing remains part of how we work every day.

**Who is Ethics and Compliance?**
Ethics and Compliance is the team that helps ensure our organization does business the right way. We provide guidance on ethical decision making, promote our Code of Conduct, support compliance with laws and company policies, and offer a safe place to ask questions or raise concerns.

**What is the Investigation Process?**
Investigations are necessary for a fair and impartial review. We look to ensure that every allegation is explored in a fair and unbiased way. All investigations are treated confidentially, and we recognize confidentiality is paramount to each investigation.

- We listen when a concern is raised and document the information shared.
- The concern is thoughtfully reviewed to determine the appropriate next steps and who should handle it.
- If needed, an investigation is conducted respectfully, objectively, and as confidentially as possible.
- The information gathered is carefully reviewed to ensure outcomes are fair and consistent.
- Once the process is complete, appropriate actions are taken and relevant parties are informed, as appropriate.

We do not tolerate retaliation against anyone for raising a concern or participating in an investigation in good faith.

**What matters should I report to Ethics and Compliance?**

- Financial or accounting matters (misuse of V2X funds, embezzlement, revenue recognition)
- Misuse/abuse of IT resources (downloading movies, pornography, or similar)
- Harassment or discrimination
- Insider Trading (unauthorized disclosure of material info)
- Privacy (confidentiality and protection of personally identifiable info)
- Labor/Time charging
- Retaliation
- Wrongful termination of employee
- Corruption (bribery, providing gifts to government officials, kick-backs, facilitation payments)
- Anti-Trust (unfair competition, price fixing)
- Hostile Work Environment
- Trade Compliance (import/export)



**2025 COMPLETED INVESTIGATIONS**

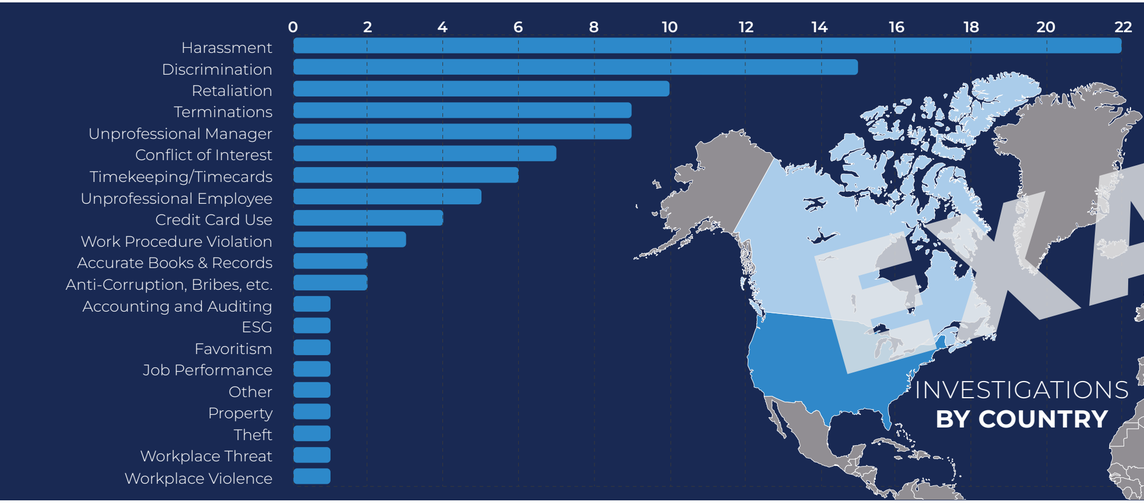
Of 103 completed investigations, **22% were reported anonymously** and **25% were substantiated**. Compared with benchmark data, V2X had a lower anonymous reporting rate (**22% vs. 52% benchmark**) and a lower substantiation rate (**25% vs. 45% benchmark**).

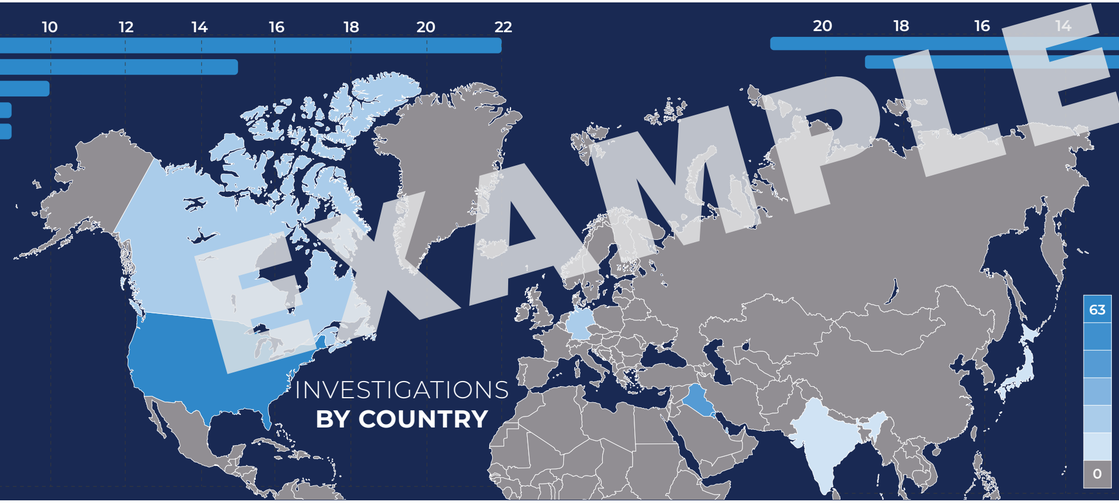
| REPORTS 2025 | Q1 | Q2 | Q3 | Q4 | TOTALS |
|---|---|---|---|---|---|
| | | | | | **426** |
| Investigations | 26 | 17 | 29 | 31 | 103 |
| *Days-to-Close | 30 | 42 | 41 | 56 | Avg=42 |

** Industry benchmark is 50 days-to-close*

# INVESTIGATIONS **BY ALLEGATION**

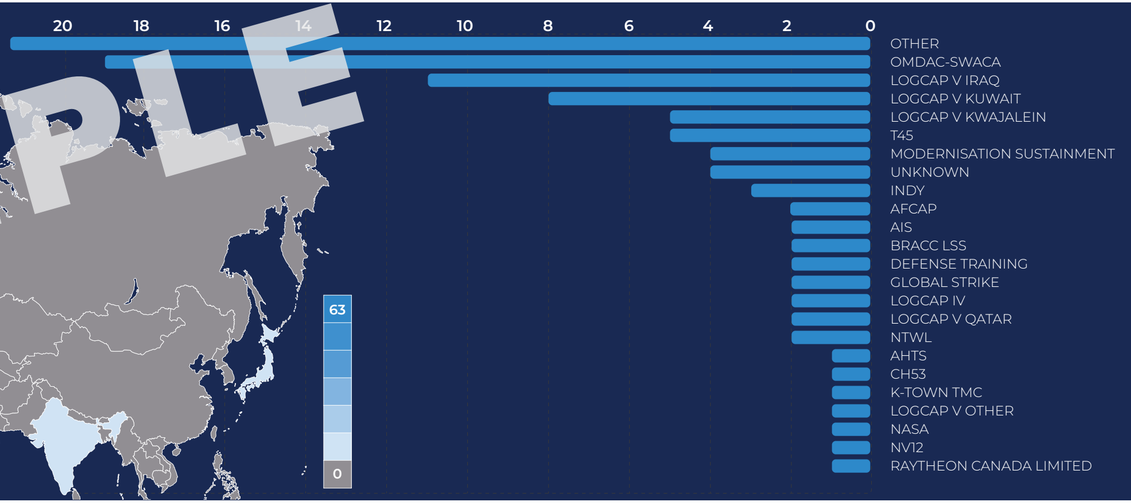
The following data reflects the types of allegations most frequently reported during 2025 and provides insight into the issues that prompted review across the organization. By tracking allegation trends over time, Ethics and Compliance can better identify areas of risk, strengthen awareness efforts, and support a workplace culture grounded in accountability, respect, and responsible conduct.




This data highlights where completed investigations were reported across programs in 2025, offering a view into how concerns were distributed throughout the organization. Reviewing activity by program helps Ethics and Compliance better understand patterns, focus engagement where needed, and ensure resources and support remain aligned with the areas of greatest activity.

# INVESTIGATIONS **BY PROGRAM**



# SPEAKING **UP**

Why it's important to report your concerns

Speaking up is an important way we live our V2X values. Raising concerns supports integrity by helping ensure we do the right thing, even when it's difficult. It demonstrates respect for our colleagues by helping maintain a workplace where everyone feels safe and treated fairly. Reporting concerns reflects responsibility to our company, our customers, and the missions we support by addressing issues early and thoughtfully. And it reinforces professionalism by holding ourselves and one another to high standards of conduct. When you speak up in good faith, you help protect our culture and strengthen V2X as a trusted partner.







## CONCERN RESOLUTION **PROCESS**

*The recommended sequence of steps for resolving employee issues is shown here.*

***This chain of command approach will greatly improve the response time to address your concerns.***

**Start by contacting your direct supervisor or their supervisor. If your concern involves either of them, move to the next action.**

**ACTION 1**

***IF YOU DO NOT FEEL COMFORTABLE WITH A PARTICULAR ACTION, SKIP TO THE NEXT ACTION.***

Contact your local HR, Site, Country, or Program Manager

**ACTION 2**

Contact Corporate Ethics at ethics@gov2x.com

**ACTION 3**

Contact the EthicsPoint Website*

or call 866.294.8691 or 503.748.0662

*(collect calls are accepted)*

**ACTION 4**

**Your complaint can be submitted anonymously using this action.*

# ANNOUNCING THE ETHICS **ADVISOR PROGRAM!**

At V2X, we believe that a strong ethical culture starts at every level of our organization. To further support our commitment to integrity, transparency, and open communication, we are excited to announce the launch of our new Ethics Advisor program!

Our Ethics Advisors will serve as trusted resources within their sites, helping to promote our core values, provide insight on the Ethics program and process, and foster an environment where everyone feels comfortable speaking up. This is a volunteer opportunity for employees who are passionate about upholding our standards and supporting their colleagues.

More information about the program including eligibility, responsibilities, and how you can become an Ethics Advisor for your site, will be shared in the coming months. Be on the lookout for further communications with details on how to express your interest!

We look forward to your involvement as we take this important step to strengthen our culture of ethics and compliance!

## Ethics Advisor Program

The V2X Ethics Advisor Program is designed to strengthen our culture of integrity by creating a trusted network of employees who can help support ethics awareness, encourage open dialogue, and serve as local resources across our sites.

## DOING THE RIGHT THING:
## **A COMMITMENT TO INTEGRITY**

At V2X, we are committed to upholding the highest standards of ethical conduct in all our business activities. Recently, a member of our team demonstrated exemplary integrity by reporting an inappropriate offer received from an external business partner.

As a result of this individual's willingness to speak up, our company was able to conduct a thorough investigation and take swift action, including discontinuing our relationship with the third party involved. In recognition of their courage and commitment to our core values, the employee received a SPOT award.

This serves as a reminder of the critical role each of us plays in reinforcing V2X's culture of transparency and accountability. By voicing concerns and acting with integrity, we help ensure V2X remains a company we are all proud to represent.

Thank you for doing the right thing, every time.



## REINFORCING OUR
## **COMMITMENT TO INTEGRITY**

At V2X, integrity is at the core of everything we do, and we rely on every member of our team to uphold our ethical standards, both directly and indirectly.

Recently, Ethics and Compliance was alerted to a matter in which an individual may have accepted a bribe indirectly through a non-V2X spouse from an external third party. Upon learning of this situation, a thorough investigation was conducted to assess the facts and impact. Following the investigation, the individual involved was separated from V2X, and our company has also discontinued our business relationship with the third party.

This situation serves as an important reminder that ethical behavior extends beyond direct personal actions, it also includes avoiding situations where conflicts of interest or the appearance of impropriety may arise. Our commitment to ethical conduct protects both our company and our values, and it ensures the continued trust of our customers, partners, and teammates.

If you ever encounter a situation where you are unsure of the right thing to do, or if you become aware of conduct that doesn't align with our Code of Conduct, please speak up. There are resources available, and your voice is critical in fostering a culture where integrity is paramount.

Thank you for continuing to uphold the standards that define V2X

# CONTACT US


**2100 Reston Parkway Suite 300**

**Reston, VA 20191 USA**

**+1 571.481.2000**

**www.goV2X.com**

**Facebook.com/goV2X**

**X.com/goV2X**

**linkedin.com/goV2X**


V2X transforms operations and sustainment for government and commercial clients worldwide through operational support services, training, and converged environments that integrate physical and digital infrastructures

Our people deliver performance excellence through client-centric, high-quality services and solutions, with an uncompromising focus on mission success.

DEFENSE INDUSTRY INITIATIVE

DII

ON BUSINESS ETHICS AND CONDUCT

## SMALL BUSINESS TOOLKIT

# POLICIES & PROCEDURES

# RESOURCE 5A: TEMPLATE CODE OF CONDUCT

## Template

## Code of Conduct

*[Cover: shall include "Company Code of Conduct" along with picture representative of company]*

*[Insider cover: shall include Company vision/mission statement and corporate values]*

## Company

*[Vision/Mission statement(s)]*

### Our Values

**Value 1**

*[Value 1 Definition]*

**Value 2**

*[Value 2 Definition]*

**Value 3**

*[Value 3 Definition]*

## CEO Message

Our Code of Conduct serves as a compass, guiding us to a common destination. Our company values of Value 1, Value 2, and Value 3 establish high standards of expected ethical behavior that serve as an essential part of our company's foundation. By embodying these values into our organization, we are helping ensure our future success.

It is important to know that this Code applies to every *[Company]* employee, no matter what part of the business, level, or area. Its scope also extends beyond employees and embraces our interactions and obligations to others, such as our customers, shareholders, and partners. When we live these values and hold each other accountable to them, we strengthen our corporate culture and solidify our reputation.

The importance of individual accountability to our Code standards is paramount. While it may sometimes be easier to look the other way and ignore something that appears inconsistent with our Code, this is never acceptable. It is expected that employees will always do the right thing and have the moral courage to speak up and raise concerns. This is especially true in times of increased performance pressures. We must not let the challenges we face lead us to neglect our compliance and values commitments.

I invite you to join me in living our values of Value 1, Value 2, and Value 3 and adhering to the *[Company]* Code of Conduct. Together we can foster an ethical workplace culture, and continue our history as a strong and trustworthy company to our employees, shareholders, and customers.

*[CEO Name]*

Chief Executive Officer and President

# Table of Contents

## Responsibilities: Doing the Right Thing

Our values of Value 1, Value 2, and Value 3 are the foundation for the way we do business and our success depends upon our unwavering commitment to conducting business ethically and in compliance with the laws and regulations where we operate. As part of this commitment, we are expected to comply with this Code of Conduct ("Code").

*[Company]* maintains an ethics and compliance program designed to prevent and detect misconduct, to encourage ethical conduct, and to ensure compliance with the laws and regulations that apply to our business. This Code is the foundation of that program. It is supported by more detailed policies and procedures that describe how we implement the standards set out here.

### Scope and Application

This Code, and the standards of business conduct and ethics incorporated in the Code, apply to all employees, officers, and directors of *[Company]*. Certain business partners and third parties, such as suppliers, agents, representatives, contractors, subcontractors, and consultants serve as an extension of *[Company]* and as such, are expected to conduct themselves according to our values and standards of ethics when working on behalf of *[Company]*.

We communicate this expectation to third parties through our Supplier Code of Conduct and through tailored provisions in our contracts. For U.S. government contracts and subcontracts above applicable thresholds, we flow down the requirements of FAR 52.203-13 (Contractor Code of Business Ethics and Conduct) to our subcontractors as required.

Any waivers to this Code may only be granted by the Board of Directors and will be publicly disclosed as required by law or regulation.

### Employee Responsibilities

Each of us must take personal responsibility for acting according to our company values and this Code, even when this means making difficult choices. We must be committed to living our values and using our Code as a guide for interactions with our stakeholders, including fellow employees, customers, business partners, shareholders, suppliers, third parties, government agencies, and communities. Accordingly, we have the responsibility to:

- Live our company values and abide by the Code, company policies, and the laws and regulations that pertain to our job responsibilities.
- Report concerns about possible violations of the Code, company policy, or laws and regulations.
- Complete all required employee training in a timely manner and keep up-to-date on current standards and expectations.
- Cooperate fully with internal and government audits, investigations, and inquiries.

Violations of the Code, company policies, or laws and regulations may result in disciplinary action up to and including termination, or legal proceedings and penalties including, in some circumstances, civil or criminal prosecution for both the individual involved and *[Company.]*

## Supervisor and Manager Responsibilities

Leaders, supervisors, and managers have the following additional responsibilities:

- Lead by example and model the highest standards of ethical business conduct and our company values.
- Take the time to ensure your employees know how to use the Code and how to seek additional help.
- Help create a work environment that focuses on building relationships, recognizes effort, and values mutual respect and open communication.
- Be proactive. Look for opportunities to discuss and address ethics and challenging situations with others.
- Create an environment where everyone feels comfortable asking questions and reporting known or potential violations of the Code, policies, or the law.
- Strictly avoid acts of retaliation or behavior that may be perceived by others as retaliation against those who report concerns.
- Respond in a timely and effective manner to concerns which are brought to your attention, but do not feel you must give an immediate response. Reflect, seek advice, and respond later if needed.
- Never ask or pressure anyone to do something that you would be prohibited from doing yourself.
- Hold employees accountable for completing all training requirements.
- Escalate concerns you cannot resolve at your level.

## Compliance with Laws and Regulations

As a *[Company]* employee, regardless of nationality or country location, you are responsible for being aware of relevant laws and regulations that apply to your work. You must be vigilant in compliance and alert to changes in the law or new requirements that may affect your responsibilities.

Working globally can raise additional ethics and compliance issues because local business and cultural practices may vary. While we respect the norms of our customers and colleagues throughout the world, we must comply with applicable laws and regulations. Where U.S. law and local law differ, we follow the higher standard. If you have questions, or if a conflict appears to exist between requirements, stop what you are doing and seek guidance from your supervisor or others listed in this Code.

## Making Ethical Decisions

We all take pride in our work and in the choices we make on behalf of *[Company.]* These choices may be more difficult to make when we encounter ethical challenges.

When faced with a difficult ethical decision, ask yourself the following questions to determine whether the action you are considering is appropriate:

- Am I adhering to the letter and spirit of our company's policies, and all applicable laws and regulations?
- Is my action consistent with company values and the principles set forth in our Code?
- Would I be acting in the best interests of *[Company]*, my co-workers, and our customers?
- What would my family, friends, or neighbors think of my action?
- Would I want my action reported on the front page of a newspaper or on the internet?

If you are unsure as to what action is appropriate, seek guidance by speaking with your supervisor or any of the other resources listed in this Code. Take the time to ask — business pressure, customer demands, and performance goals do not override our obligation to act ethically and in compliance with the law.

## Asking Questions and Raising Concerns

**OUR STANDARD:** *If you observe or suspect any illegal or unethical behavior, you are expected to raise the issue to your management or one of the other resources listed below.*

In most cases, you should first contact your supervisor to raise your concerns. However, if you are uncomfortable talking to your supervisor, contact Human Resources, Legal, a compliance representative, or a member of the Ethics Office. You also have the option to report concerns using the Helpline telephone or through the Internet at:

| **Helpline** | |
|---|---|
| **Phone:** | *[888.888.8888]* |
| **Web:** | *[www.Companyinc.Helpline.com]* |

Any employee who has a concern or complaint regarding accounting, internal accounting controls, or auditing matters may also report the matter to the *[Company]* General Auditor or the *[Company]* Audit Committee on a confidential or anonymous basis by mail c/o the *[Company]* Corporate Secretary, 1234 Street, Suite 1234, City, ST 22222.

In addition, employees may report concerns directly to appropriate government agencies, including the Department of Defense Inspector General Hotline for matters involving DoD programs or personnel, the Department of Justice, the Securities and Exchange Commission, or other regulators. Employees may be eligible for legal protections and, in some circumstances, awards under those programs. Nothing in this Code or any *[Company]* policy requires employees to report internally before communicating with a government agency, limits employees' right to communicate with government agencies, or restricts any legally protected whistleblower activity.

## Expectations when Using the Helpline

**OUR STANDARD:** *The Helpline and web site are always available and all reports will be investigated thoroughly and confidentially.*

The Helpline is available 24 hours, seven days a week. This independent third party provider facilitates the documentation of your concerns and forwards them to the appropriate compliance contact within *[Company]* to address.

When making a report, you are encouraged to identify yourself. Doing so facilitates communication and helps *[Company]* resolve the situation. However, in the United States and elsewhere as allowed by local law, you may make a report anonymously. If you choose to report anonymously, it is important that you check back with the Helpline, as we may have posted additional questions to help us with our investigation or we may have provided feedback to you on your concern. All communications are facilitated by the third party provider. Access to reported issues is restricted, secure, and confidential in a manner consistent with conducting a thorough investigation and meeting any legal requirements. All issues are thoroughly investigated and, if appropriate, corrective actions are implemented.

## Non-Retaliation

**OUR STANDARD:** *There is no tolerance of retaliation for those employees who, in good faith, report possible ethics or compliance violations.*

You can report suspected ethical violations in confidence and without fear of retaliation. *[Company]* will not tolerate any retaliation against an employee who, in good faith, asks questions, reports possible violations of the Code, policy, or law, participates in an investigation. Reporting "in good faith" means making a genuine attempt to provide honest, complete, and accurate information, even if it later proves to be unsubstantiated or mistaken.

Retaliation can take many forms. It includes termination, demotion, pay cuts, and poor performance reviews, but may also include more subtle actions such as reassignment to less desirable work, exclusion from meetings or projects, and changes in how a person is treated socially at work. Retaliation is a violation of our Code, and knowledge or suspicion of retaliation should be immediately reported.

In addition to our internal protections, federal law protects employees of federal contractors from reprisals for disclosing certain information to designated recipients, including information the employee reasonably believes is evidence of gross mismanagement, gross waste of funds, abuse of authority, a substantial and specific danger to public health or safety, or a violation of law related to a federal contract. See the Non-Retaliation Policy for more information.

## Mandatory Disclosures

**OUR STANDARD:** *Timely disclose credible evidence of specified violations on federal contracts.*

As a federal contractor, *[Company]* is required to timely disclose, in writing, whenever we have credible evidence that a principal, employee, agent, or subcontractor has committed a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations under Title 18 of the U.S. Code, or a violation of the civil False Claims Act. We are also required to disclose significant overpayments on federal contracts. These disclosures are made to the agency Office of the Inspector General, with a copy to the Contracting Officer. Only authorized *[Company]* personnel may make disclosures or submissions to government agencies on behalf of *[Company.]*

Decisions about whether a disclosure is required are legally complex and time-sensitive. They are made by the Legal Department in coordination with the Ethics Office and senior leadership, not by individual employees or managers. If you learn of a potential issue that might trigger a mandatory disclosure obligation, report it immediately through one of the channels in this Code. Failing to disclose when required can lead to significant consequences for *[Company.]*

***Make sure you:***

- *Report promptly when you have reason to believe a violation involving fraud, conflict of interest, bribery, gratuities, or false claims has occurred, or may have occurred.*
- *Do not try to evaluate the "credibility" of the evidence on your own.*
- *Preserve relevant documents and records, and do not discuss the matter with anyone other than those involved in the internal review.*

### Cooperating with Inquiries and Investigations

**OUR STANDARD:** *Cooperate with all internal and external inquiries and investigations.*

You are expected to fully cooperate with internal and external audits, investigations, and inquiries that are conducted by the company or by the government. Withholding information or knowingly giving false or misleading information is a serious violation of our duties as employees.

In the course of business, you may receive inquiries or requests for information from government officials. When the company receives an inquiry or investigative request from the government, refer it to the Legal Department before responding on the company's behalf. Nothing in this paragraph limits any employee's right to communicate directly with a government agency.

With respect to all audits, investigations, and inquiries, you must NOT:

- Destroy, alter, or conceal any document in anticipation of or in response to a request for these documents.
- Provide or attempt to influence others to provide incomplete, false, or misleading statements to a company or government investigator.
- Conduct an investigation yourself; appropriate resources will be assigned to conduct the investigation.
- Use personal email, personal devices, ephemeral messaging, or other channels to discuss or conceal information relevant to the matter.

## Responsibilities: To One Another

We are committed to providing a professional, respectful, and safe work environment. We owe it to each other to be honest and respectful. We should treat others as we would want to be treated.

### Non-Discrimination

**OUR STANDARD:** *Maintain a work environment free from discrimination and harassment.*

We do not tolerate discrimination of any kind. We provide equal employment opportunities for all regardless of race, color, ethnicity, ancestry, religion, sex, national origin, age, physical or mental disability, military/veteran status, marital status, genetic information, or any other legally protected classification.

Employment decisions — including recruiting, hiring, promotion, compensation, transfer, discipline, termination, training, mentoring, sponsorship, leadership development, work assignments, and access to *[Company]*-sponsored opportunities — must be based on objective, job-related, and lawful criteria. We do not use protected characteristics as a criterion, preference, factor, target, quota, tiebreaker, or basis for limiting access to opportunities, unless specifically authorized by law and approved by Legal or Human Resources.

For employees working on or supporting U.S. federal contracts or subcontracts, this standard also includes compliance with applicable federal contract anti-discrimination requirements. In connection with federal contract work, *[Company]* does not engage in discriminatory diversity, equity, and inclusion activities, including disparate treatment based on race or ethnicity in recruitment, employment, contracting, program participation, or allocation of *[Company]* resources.

We do not tolerate harassment of any kind. Verbal or physical conduct that harasses another, disrupts another's work performance, or creates an intimidating, offensive, abusive, or hostile work environment will not be tolerated. Harassing conduct can include inappropriate gestures, remarks, or touching, or displaying sexually explicit or offensive pictures. Promises of promotion or special treatment in return for sexual favors also constitute harassment.

***Make sure you:***

- *Treat others respectfully and professionally. and*
- *Review your own decisions to ensure that you are using objective and quantifiable standards and business considerations to drive your actions.*
- *Make workplace decisions based on merit, qualifications, performance, business needs, and other lawful criteria. Avoid discrimination against others on the basis of any characteristic protected by law.*
- *Avoid making comments or jokes, or sending or posting materials, which others might consider offensive.*
- *Report all incidents of discrimination, harassment, and intimidation which you observe.*

## Safe and Healthy Workplace

**OUR STANDARD:** *Maintain a safe, healthy, and secure work environment.*

*[Company]* is committed to providing a safe, healthy, and secure workplace for colleagues and visitors to our facilities and to operating in an environmentally sound manner. *[Company]* requires that all employees practice safe work habits and follow all applicable safety, security, and health rules and practices.

***Make sure you:***

- *Review and follow the safety, security, and health rules and practices that apply to your job and your facility.*
- *Complete required training and follow the additional security procedures required for secure areas.*
- *Immediately report any practices or situation, regardless of severity, that could pose a threat to the environment, or the safety or health of anyone.*

### *Drugs and Alcohol*

To maintain a safe workplace, it is essential that we are able to think clearly and react quickly. Any involvement with illegal drugs — including their use, possession, distribution, purchase, sale, offer for sale, or manufacture — while on *[Company]* premises, on *[Company]* time, or when conducting or traveling on *[Company]* business is prohibited. The abusive use of controlled substances, including prescription drugs or alcohol, is also prohibited. The only exception is when alcohol is consumed responsibly and in observation of applicable laws at business dinners or in accordance with local management direction at an authorized company event.

As a federal contractor, *[Company]* maintains a drug-free workplace consistent with the Drug-Free Workplace Act of 1988 and applicable law. State or local initiatives legalizing the use of marijuana do not alter *[Company]*'s obligations as a federal contractor.

### *Workplace Violence*

Violence of any kind has no place at *[Company.]* We will not tolerate any acts or threats of physical violence against co-workers, visitors, or anyone on *[Company]* property, or by any representatives of *[Company]* during company travel or company-sponsored events. Prohibited activities include:

- Threatening remarks or behavior, obscene phone calls, or stalking.
- Assaults or causing physical injury to another.
- Intimidation or acting aggressively in a manner that causes someone else to fear injury.
- Intentionally damaging someone else's property.
- Bringing prohibited items, such as explosives (fireworks, firearms, or ammunition), knives, or other weapons into company facilities or to company-sponsored events.

Every threat of violence is serious and you are expected to immediately report any observations of violence to your supervisor, any member of management, Human Resources, or Security.

## Environmental, Health, and Safety

**OUR STANDARD:** *Comply with applicable environmental, health, safety, hazardous-materials, and waste-management requirements.*

*[Company]* is committed to operating safely and in compliance with applicable environmental, health, safety, hazardous-materials, and waste-management laws, regulations, contract requirements, and *[Company]* policies. Employees must follow the procedures that apply to their work and promptly report spills, releases, unsafe conditions, hazardous-material concerns, or potential violations.

***Make sure you:***

- *Follow the environmental, health, safety, and hazardous-materials rules that apply to your job and facility.*
- *Report spills, releases, unsafe conditions, or potential violations promptly.*
- *Do not handle, store, transport, label, or dispose of hazardous materials except as authorized and trained.*
- *Cooperate with required inspections, reporting, corrective actions, and recordkeeping.*

## Human Rights

**OUR STANDARD:** *Recognize and adhere to internationally recognized human rights standards, applicable laws, and United States federal government contract requirements in our work and in our supply chain*

We support human rights by complying with internationally recognized provisions in all locations where we operate, regardless of local business customs, and are committed to providing safe and secure conditions for those working on our company's behalf.

We will not knowingly work with business partners, including agents, subcontractors, recruiters/labor brokers/staffing firms, and subcontractors, who employ children or forced labor, including prison or bonded labor. We will not tolerate physical punishment or abuse. We will not engage in human trafficking-related activities, including misleading or fraudulent recruiting practices, charging our employees or potential employees recruiting fees, confiscating or destroying employee identification documents, or supporting prostitution. It is a violation of company policy for employees to, directly or indirectly, purchase commercial sex acts for themselves, for the benefit of employees or third parties, or while conducting company business. Where required by contract, the *[Company]* will maintain an anti-trafficking compliance plan, submit required certifications, and flow down applicable requirements to subcontractors and agents.

***Make sure you:***

- *Immediately report any suspected potential human rights related violations.*
- *Strictly prohibit use of child or forced labor, including prison, bonded, indentured, involuntary, or otherwise unlawful labor.*
- *Commit to obeying the associated laws and regulations and, where these laws vary or conflict, follow the highest standards.*

### Privacy of Employee Information

**OUR STANDARD:** *Handle employee information responsibly.*

For those of us who have access to personal information related to our colleagues and others, we have an obligation to protect this information and exercise caution before disclosing it to others. This includes, but is not limited to, medical, payroll, and personally identifiable information. We may only provide employee information to other employees and third parties where permitted by law, company approval, or employee permission.

***Make sure you:***

- *Learn which types of information are given heightened protection by the law and company policy (such as government-issued identification, bank account numbers, and medical records) and protect them through appropriate means (such as encryption or other types of limited access).*
- *Protect the confidentiality of personal information of current and former colleagues, as well as job applicants, business partners, and customers.*
- *Don't access or share others' personal information unless there is a legitimate business reason to do so.*
- *Immediately report any loss or inadvertent disclosure of confidential employee information.*
- *Ensure recipients of employee information will safeguard the information.*

## Responsibilities: Corporate Citizens

### Anti-Trust and Fair Competition

**OUR STANDARD:** *Recognize and avoid anti-competitive behaviors and activities.*

We believe in fair and open markets and never engage in improper practices that may limit competition. We compete vigorously to be an industry leader and we do so by maintaining high standards of fairness and honesty when engaged in marketing, promotional, and advertising activities. We look to gain competitive advantage through superior performance, price, and quality, and not through unethical or illegal business practices.

We do not enter into agreements with competitors to engage in any anti-competitive behavior, including setting prices, dividing up customers, suppliers, or markets., or restricting the hiring or wages of employees through wage-fixing and no-poach agreements.

Anti-trust laws are complex and compliance requirements can vary depending on the circumstance, but in general, the following activities are "red flags" and should be avoided and reported to your supervisor or the Legal Department:

> **COLLUSION** – when two or more parties secretly communicate or agree on how they will compete. This could include agreements or exchanges of information on pricing, terms, wages, or allocations of markets.
>
> **BID-RIGGING** – when two or more parties manipulate bidding so that fair competition is limited. This may include

comparing bids, agreeing to refrain from bidding, or knowingly submitting noncompetitive bids.

**TYING** – when a company with market power forces customers to take products or services that they do not want or need.

**PREDATORY PRICING** – when a company with market power sells a product or service below cost so as to eliminate or harm a competitor, intending to recover the loss of revenue later by raising prices after the competitor has been eliminated or harmed.

***Make sure you:***

- *Never share the company's sensitive information with a competitor of the company.*
- *Never share sensitive information of business partners or other third parties with others without their permission.*
- *Never take advantage of anyone through manipulation, abuse of privileged information, misrepresentation of facts, or any other intentionally unethical or illegal action.*
- *Never engage in conversations with potential competitors about competitive sensitive information.*
- *Never use or disseminate non-public information about potential competitors from new hires or candidates for employment.*
- *Never have conversations with potential competitors that could be perceived as limiting competition.*

## Anti-Corruption

**OUR STANDARD:** *Do not offer or provide bribes to influence action or accept kickbacks in connection with company business.*

**BRIBE** – the payment of anything of value — such as cash, gifts, services, contributions, internships, or vacations — made for the purpose of improperly obtaining or retaining business.

**KICKBACK** – the return of a sum already paid or due to be paid as part of a legal contract, as a reward for making or fostering business arrangements.

**FACILITATION PAYMENTS** – also known as "grease payments," are modest amounts of money paid as an unofficial fee to low level government employees to speed or initiate the performance of routine and expected government services to which *[Company]* is entitled.

*[Company]* is committed to conducting business ethically, with integrity, and in compliance with applicable laws and regulations prohibiting bribery, kickbacks, and other forms of corruption in our operations worldwide. Because of the complexity of anti-corruption and bribery laws, it is important that employees are aware of company policies and ask questions if they have any doubts about the proper course of action. Bribery and kickbacks are never permitted at *[Company]*, regardless of whether we are dealing with a government or commercial customer.

The U.S. Foreign Corrupt Practices Act (FCPA), the United Kingdom (U.K.) Bribery Act, and the laws of most countries in which we operate all prohibit bribing government officials. For purposes of these laws, the term "government official" is defined broadly and includes civil servants, officials of state-owned or controlled commercial enterprises, representatives of public international organizations, office seekers, political parties, family members, and political party officials. Many countries also have laws that prohibit bribes paid to private individuals.

It is especially important that employees carefully monitor third parties acting on the company's behalf. We must

always be sure to perform due diligence and know our business partners and all those through whom we conduct our business. Our third parties must understand that they are required to operate in strict compliance with our standards and to maintain accurate and complete books and records. *[Company]* can be held responsible for improper payments made by third parties on our behalf.

Facilitating payments — small unofficial payments to low-level officials to expedite routine, non-discretionary government action — are not allowed. You must obtain approval from the Legal Department before making any such payment, no matter how small the amount. The only exception is a payment made under imminent threat to a person's health or safety; any such payment must be reported to the Legal Department as soon as it is safe to do so and recorded accurately in *[Company]*'s books. If you are solicited for a facilitation or expediting payment, contact the Legal Department immediately.

***Make sure you:***

- *Never directly or indirectly offer, provide, or authorize money or any item of value to improperly obtain or retain business or to improperly influence a governmental action.*
- *Never make payments that are intended to improperly influence a government official.*
- *Never directly or indirectly request, agree to receive, or accept kickbacks, payoffs, or other personal payments in connection with company business.*
- *Notify the Legal Department of third parties or agents who are thought to be valuable primarily for their personal ties rather than for the services they are to perform, or who request compensation out of proportion to their services.*

### *Anti-Money Laundering*

*[Company]* does not condone, facilitate, or support money laundering. Involvement in such activities undermines our integrity, damages our reputation, and can expose *[Company]* and individuals to severe sanctions.

**MONEY LAUNDERING** – occurs when companies or individuals attempt to convert, disguise, or hide proceeds of illegal activity by moving illegally obtained funds, or hiding the source so the funds are made to appear legitimate.

Employees must comply with all applicable money-laundering and anti-terrorism requirements which prohibit:

- Engaging in financial transactions involving property, funds, or monetary instruments which, directly or indirectly, promote or result from criminal activity.
- Receiving, transferring, transporting, retaining, using, structuring, diverting, or hiding the proceeds of any criminal activity, or aiding or abetting another in any such action.
- Engaging or becoming involved in financing, supporting, or otherwise sponsoring, facilitating, or assisting any terrorist person, activity, or organization.

***Make sure you:***

- *Never cooperate with efforts to evade reporting requirements.*
- *Report suspicious activity such as payments to offshore banking locations, payments to third parties outside the territory in which the third party operates, and false invoices for sales.*

### *Business Courtesies*

**BUSINESS COURTESY** – any item of value provided to or received from a third party for the purpose of initiating or furthering a business relationship. Business courtesies include such things as cash, entertainment, meals, gifts, social events, sporting events, travel, lodging, favors, gratuities, discounts, and services.

Conducting business with integrity means never seeking to improperly influence business decisions. For this reason, it is important for each of us to exercise common sense and good judgment when giving or receiving business courtesies.

In general, we may not offer or accept a business courtesy if it:

- Violates any law, regulation, or policy applicable to the giver or recipient.
- May be considered a bribe, payoff, or kickback.
- Violates customary business practices.
- Gives the appearance of impropriety or could give rise to a conflict of interest.

We must always avoid situations where business courtesies could harm the reputation of our company or those of us involved. We may never attempt to circumvent these rules by using our personal funds or by engaging an agent or representative to pay for any business courtesy that we cannot pay ourselves.

The rules outlined in this section also govern the actions of our family members and close friends, as well as those of *[Company]*'s agents and representatives.

### *Government Officials*

U.S. Government Officials. The U.S. government has strict laws and rules prohibiting its employees or elected representatives from accepting business courtesies. With the exception of common hospitality and promotional items of nominal intrinsic value, we may not offer or give a business courtesy to a government official without the prior written approval of the Legal Department. These rules stem from the Standards of Ethical Conduct for Employees of the Executive Branch (5 C.F.R. Part 2635), agency-specific supplements, the Procurement Integrity Act, and, for members of the armed forces, the Joint Ethics Regulation.

Non-U.S. Government Officials. Most countries prohibit their official employees from accepting business courtesies. With limited exceptions, business courtesies extended to any government officials require prior written approval from the Legal Department.

***Make sure you:***

- *Coordinate with the Legal Department for review and approval prior to providing any business courtesy to any government official, no matter the country they represent.*
- *Are aware of the perceptions that can be drawn from the provision of business courtesies to government employees.*
- *Exercise caution when dealing with business partners which could appear to be privately owned but are actually considered government entities.*

### *Commercial Third Parties*

Exchanging business courtesies with our commercial third parties must be reasonable, infrequent, for a legitimate business reason, and consistent with normal industry practice and local laws.

> Providing or offering business courtesies to commercial third parties that exceed nominal value may require written Legal Department approval. Exceptions include coffee, soft drinks, light snacks, an inexpensive business-related meal incident to a site visit, recognition awards for program or service achievements, or promotional items. Other than these exceptions, accepting business courtesies from third parties, including suppliers, requires approval by the Legal Department.

***Make sure you:***

- *Seek guidance and approval if you are unsure as to whether the business courtesy is appropriate.*
- *Only provide and accept business courtesies that are justified by the business relationships. Exchanging business courtesies that foster goodwill in business relationships is generally acceptable, but you should never provide or accept business courtesies that obligate or appear to obligate the recipient.*
- *Do not offer or accept lavish, extravagant, or unreasonable business courtesies.*
- *Do not offer travel and lodging without advance approval from the Legal Department.*
- *Understand and comply with both [Company] and third party policies before offering or providing business courtesies.*
- *Raise a concern whenever you suspect that a colleague, third party, or other agent of the company may be engaged in an attempt to improperly influence a decision of a customer.*

***Specifically regarding the acceptance of business courtesies:***

- *Do not request or solicit personal gifts, favors, entertainment, services, or any other type of business courtesy.*
- *Never accept cash or cash equivalents, such as gift cards, of any value.*
- *Never accept business courtesies of any kind from a business partner with whom you are involved in contract solicitation or negotiations.*
- *Refuse business courtesies that seem inconsistent with our business practices and report it to your supervisor.*
- *Seek advance written approval for any exceptions.*

## Export & Import Compliance

**OUR STANDARD:** *Fully comply with export/import laws and do not trade with sanctioned or embargoed countries or entities.*

> **EXPORT** – occurs when a product, service, or technology is transferred either physically across borders, electronically via fax, email, or data-sharing sites, or visually through demonstrations, presentations, and discussions between nationals of different countries. Such exports, if they involve controlled military or dual-use technologies, often require government approval in the form of an export license or other authorization.
>
> **IMPORT** – occurs when products purchased or obtained from a foreign country or external source are brought into another country. Import transactions are subject to laws and regulations and must go through Customs' formalities or the assessment of necessary duties and taxes.
>
> In the U.S. as well as other countries in which *[Company]* operates, governments often have complex and significant restrictions on trade in military and dual-use goods, technology, and services, as well as trade with certain countries. *[Company]* complies with all trade restrictions and import and export control laws of the countries in which we operate, including the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and Office of Foreign Assets Control (OFAC) sanctions. We expect all of our business partners, third parties, consultants, and contractors to do the same.

Export rules may restrict the following:

- Any oral discussion with any non-U.S. person, even someone inside the United States, which discloses technical information and might be considered an export.
- Using business knowledge outside of the employee's country, such as when providing technical assistance to others.
- Transferring technical data to someone in another country, such as through the Internet, email, conversations, meetings, and network or database access. This restriction applies to sharing information with other company employees, as well as non-employees.
- Transferring technology to non-U.S. persons, whether located inside or outside the U.S.
- Transferring technology from an authorized non-U.S. person to one that is not authorized.
- Transporting company assets with certain technology, such as a computer an employee takes on a business or personal trip to another country.
- Dealing with specifically identified sanctioned or embargoed countries or entities acting on their behalf, as well as transactions involving certain named persons or organizations.

***Make sure you:***

- *Comply with all export and import laws, regulations, and requirements, and with [Company] trade control policies.*
- *Understand the trade controls related to [Company] products, technology, and information and the restrictions on transferring those items to entities outside the company.*
- *Obtain licenses or other government approvals prior to exporting and importing products and technology controlled by the government.*
- *Report any known or suspected trade control violation to your local [Company] trade compliance office or the Office of International Trade and Compliance.*
- *Report complete, accurate, and detailed information regarding every imported product, including its proper classification, country of origin, and appropriate value.*

### *Boycotts*

**BOYCOTTS** – occur when a person, group, or country refuses to do business with certain persons, groups, or countries as a means of protest, an expression of disfavor, or a method of coercion.

We may not participate in or promote boycotts that the United States does not support. This means that we may not agree to a contract, document, or verbal request containing language that could be interpreted as an attempt by a person, group, or country to enforce an unsanctioned boycott. U.S. law also requires us to report certain requests to participate in an unsanctioned boycott, even if we decline.

***Make sure you:***

- *Review all transactional documents, including contracts, letters of credit, shipping or import documents, or bid and proposal materials, for any language that may constitute a boycott request.*
- *Notify the Legal Department if requested to join in, support, or furnish information concerning a non-U.S. boycott.*

### Political Involvement

**OUR STANDARD:** *Do not support political parties on the company's behalf or engage in prohibited lobbying activities.*

We believe that our employees benefit from being active in the community through good citizenship. We recognize that our employees have a right to voluntarily participate in the political process, including volunteering in campaigns and making individual political contributions. *[Company]* also has a clear and separate responsibility to obey all applicable laws and regulations with regard to operation of a corporate Political Action Committee and employing registered lobbyists for company business. These separate individual and company activities need not be in conflict, provided that employees exercising their rights do so only in their own name and on their own time.

Never use the company name, funds, assets, services, or facilities to support any political candidate or party, or to engage in any lobbying activity, unless specifically permitted by law and authorized in advance by the Government Relations Department.

***Make sure you:***

- *Consult with our government relations professionals BEFORE interacting with government officials in a manner that might be interpreted as a lobbying activity.*
- *Ensure that your personal political views and activities are not viewed as those of the company.*
- *Do not use the company's name, resources, or facilities to support your personal political activities.*
- *Never apply direct or indirect pressure on another employee, customer, or business partner to contribute to, support, or oppose any political candidate or party.*
- *Avoid the appearance that you are making political or charitable contributions to gain favor on behalf of [Company.]*
- *Notify management prior to accepting or campaigning for political office.*

## Responsibilities: Business Partners

### Honest and Ethical Dealings

**OUR STANDARD:** *Maintain a culture of integrity by being honest and ethical in business relationships.*

We treat all of our business relationships fairly: the government, our non-government customers, business partners, third parties, suppliers, and contractors. We work to understand and meet their needs while always remaining true to our own ethical standards. We tell the truth about our services and capabilities and we do not make promises we know we cannot keep. In short, we treat our business partners as we would like to be treated.

We expect our customers, business partners, and stakeholders to act in a manner that is consistent with our ethical standards and we must bring suspected unethical or illegal activity on their part to the immediate attention of the *[Company]* Legal Department.

***Make sure you:***

- *Talk to your supervisor if you have concerns about any error, omission, undue delay, or defect in quality or customer service.*
- *Report pressure from colleagues or managers to cut corners on quality or delivery standards.*
- *Never follow a customer's or third party's request to do something that you regard as unethical or unlawful.*
- *Respond promptly to customer and business partner requests and questions.*
- *Promise what you can deliver and deliver on what you promise.*

## Procurement Integrity

**OUR STANDARD:** *Understand and comply with the procurement integrity laws and regulations.*

**BID OR PROPOSAL INFORMATION** – typically proprietary information submitted by the bidding entity.

**SOURCE SELECTION INFORMATION** – any information prepared or used by a federal agency for evaluating bids or proposals to enter into a procurement contract.

Since we conduct business with governments and government-owned entities, we are committed to compliance with the many special legal, regulatory, and contractual requirements that apply to government contracting. In compliance with the Procurement Integrity Act, we will not disclose or use any unauthorized confidential contractor bid or proposal information, or source selection information, before a contract award. Employees should contact their Contracts or Legal Departments with questions specific to contracting with the government.

### *Hiring Former Government or Military Personnel*

The U.S. Government and other countries have laws and special restrictions that apply to the recruitment and hiring of current and former government employees and military personnel as employees, consultants, or representatives. Restrictions include limitations on the type and timing of employment-related discussions that government employees may have with *[Company.]* We must ensure that such employment discussions are approved in advance by the Human Resources and Legal Departments. and, once hired, limitations on what matters a former government employee may do for *[Company.]*

***Make sure you:***

- *Avoid seeking or receiving information that the company is not authorized to possess, such as confidential or proprietary data, pricing information of other competitors, and non-public government documents relating to bidding or source selection.*
- *Seek immediate guidance from your division's legal counsel if you inadvertently receive unauthorized bid or proposal or source selection information.*
- *Comply with government conflict of interest restrictions, including any post-employment restrictions set out in an agency ethics letter or similar guidance.*

### *Organizational Conflicts of Interest (OCI)*

**OUR STANDARD:** *Disclose any potential organizational conflicts of interest.*

We are required to recognize and avoid organizational conflicts of interest in connection with direct or indirect contracts with the U.S. Government. An OCI may arise where activities of the company, our employees, partners, or competitors could impair our ability to render impartial services on a government contract. OCIs can also result in unfair competitive advantage from access to information obtained through other contractual relationships with the government. We identify and disclose potential OCIs early and take steps to avoid, neutralize, or mitigate them, steps which may include firewalls, recusal, or declining the work.

### *Accurate Certifications and Representations*

**OUR STANDARD:** *Make only certifications and representations that are accurate, complete, and current.*

Federal contracts require us to make many certifications and representations on cost and pricing data, small business status, cybersecurity compliance, prohibited sources in our supply chain, human trafficking compliance,

and more. Inaccurate certifications can expose *[Company]* to liability under the False Claims Act and related authorities, and can result in suspension or debarment.

Every certification we sign must be accurate, complete, and current at the time of submission, and must be updated when circumstances change. If you are asked to sign — or to provide supporting information for — a certification, do so only if you have verified the facts that support it. If you have any doubt, stop and raise the question before signing.

***Make sure you:***

- *Verify the underlying facts before signing or supporting a certification or representation.*
- *Do not rely on "business-as-usual" assumptions where the facts may have changed.*
- *Promptly report information that would make a prior certification inaccurate so it can be corrected.*

## Business Partner Relations

**OUR STANDARD:** *Business partner relationships must be based on mutual trust and a commitment to act with integrity.*

We deal fairly with our suppliers, consultants, and other third parties and we expect them to act with integrity. In dealings with *[Company]*, we expect business partners to follow the spirit of the Code, as well as any applicable contractual provisions, when working on behalf of *[Company.]*

### *Due Diligence*

Appropriate risk-based due diligence must be performed by *[Company]* before engaging any third party, and enhanced due diligence is required for third parties who will have contact with U.S. and non-U.S. government customers, or who will act on *[Company]*'s behalf in higher-risk markets. We monitor third parties during the relationship and address concerns through the appropriate channels.

### *Supplier Diversity*

Recognizing the importance and benefits of a diverse supplier base, we will work to identify qualified small business concerns, including those owned by women, minorities, veterans, and service-disabled veterans, and those located in historically underutilized business zones, capable of providing products and services. We comply with applicable small business subcontracting plan requirements.

### *Subcontractor Code of Ethics Provisions*

For U.S. government contracts above the applicable thresholds, the law requires us to ensure that applicable subcontracts include the provisions of FAR 52.203-13 — meaning the subcontractor must have a code of business ethics and conduct, an ethics awareness and compliance program that includes training, an internal reporting mechanism, disciplinary action for violations, and timely disclosure to the government of credible evidence of specified violations.

### *Product Origin, Quality, and Substitution*

Our customers, both government and commercial, have the right to insist on strict compliance with contract requirements. We must only deliver products that conform to the contract's specified requirements. We must avoid the substitution of lower quality, different, or inadequately tested products. We must also ensure that suppliers of raw materials, parts, and components used in our products meet our contract requirements, including applicable requirements regarding prohibited sources and counterfeit parts.

## Conflicts of Interest

**OUR STANDARD:** *Disclose and seek guidance on any issues that potentially may conflict with your responsibilities with the company.*

A conflict of interest occurs whenever you have competing interests that may interfere with your ability to make an objective decision in the best interest of *[Company.]* Each of us is expected to use good judgment and avoid situations that can lead to even the appearance of a conflict of interest, as it could undermine the trust that our customers, business partners, fellow employees, and the public place in us.

Below are some areas in which potential conflicts of interest may arise:

> ***Personal Relationships***
> Personal relationships with employees or business partners — such as family members, friendships, and romantic partners — who have influence over one another through the chain of command, in purchasing or contracting decisions, in bidding or proposal related efforts, or in recruiting or hiring decisions.
>
> ***Financial Dealings and Investments***
> Situations where you or a family member has a significant financial ownership interest in a privately owned enterprise with which *[Company]* competes or does business.
>
> ***Outside Employment***
> Since outside employment may appear to bias our decisions in the best interest of *[Company]*, *[Company]* personnel may not be employed by, work as a consultant for, or be affiliated with a *[Company]* competitor, customer, or supplier. You should always discuss any outside work situations with your supervisor prior to undertaking them. Additional disclosure requirements may apply to employees performing "covered" functions under FAR 52.203-16 (Preventing Personal Conflicts of Interest).

***Make sure you:***

- *Always make business decisions in the best interest of [Company.] Seek guidance to avoid potential conflicts of interest.*
- *Disclose potential conflicts immediately by notifying your supervisor or Human Resources in writing.*
- *Update your disclosure if your situation changes.*

## Business Intelligence

**OUR STANDARD:** *Obtain competitive information only through proper means.*

Information about competitors is a valuable asset in today's competitive business environment. When collecting business intelligence, *[Company]* employees and others who are working on our behalf must always live up to the highest ethical standards.

We must never engage in fraud, misrepresentation, or deception to obtain information. Nor should we use invasive technology to "spy" on others. We also need to be careful when accepting information from third parties. You should know and trust their sources and be sure that the knowledge they provide is not protected by trade secret laws, or non-disclosure or confidentiality agreements.

When *[Company]* employs former employees of competitors, we recognize and respect the obligations of those employees not to use or disclose the confidential information of their former employers.

***Make sure you:***

- *Do not request or receive the confidential information of other companies.*
- *Never pressure new employees to discuss confidential information from their previous employer.*
- *Do not disclose suppliers' non-public pricing information.*
- *Never retain papers or computer records from prior employers in violation of laws or contracts.*
- *Do not seek information obtained through any behavior that could be construed as "espionage," "spying," or which you would not be willing to fully disclose.*

# Responsibilities: Shareholders

## Accuracy of Records

**OUR STANDARD:** *Maintain current, accurate, and complete business records.*

> **RECORDS** – any information generated during the course of company business, including not just paper documents, but also tapes, photographs, computer files and records in any other form, including text messages and chat messages.

Our shareholders, business partners, customers, government officials, and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the company so that we can make good decisions.

We are responsible for honesty and transparency in the preparation and maintenance of our business records, including our time cards, expense reports, quality, safety, and procurement records. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate, complete, and maintained in a manner that is consistent with our internal controls.

> ***Charging Costs***
>
> All costs allocated to a particular government contract as direct or indirect costs must be reasonable, allocable, and allowable under applicable procurement cost principles and Cost Accounting Standards in accordance with applicable Disclosure Statements. In addition, when we work on government contracts or subcontracts, we must:
>
> - Accurately record the number of hours worked on the appropriate project.
> - Charge all labor and material costs to the proper contract and charge indirect costs properly.
> - Ensure only costs properly chargeable to a government contract are billed to the government.
> - Never shift costs between contracts to avoid an overrun, reach a ceiling, or for any other improper reason.
>
> ***Records Retention***
>
> We are responsible for the information and records under our control and we must be familiar with the recordkeeping procedures that apply to our jobs. It is also our responsibility to keep our records organized so that they can be located and retrieved when needed.
>
> Documents should only be destroyed in accordance with our record retention schedule, and never in response to, or in anticipation of, an investigation, audit, or pending litigation. Contact the Legal Department if there is any doubt about the appropriateness of record destruction.

> ***Legal Holds***
> A legal hold suspends all document destruction procedures, including deletion of emails and computer files, in order to preserve appropriate records under special circumstances, such as litigation or government investigations. *[Company]* will determine and identify what types of records are required to be placed under a legal hold. Every employee, agent, and contractor must comply with this policy.

If there is any question as to whether a record pertains to an investigation or legal proceeding, contact the Legal Department prior to disposing of any related records.

***Make sure you:***

- *Submit current, accurate, and complete business records at all times.*
- *Report your suspicions or observations of others who create inaccurate records.*
- *Act promptly, in consultation with management, to correct any discrepancies.*
- *Write truthfully, objectively, and clearly in all your business communications, including emails and electronic messages.*
- *Sign documents, including contracts, only if you have reviewed, are authorized to sign, and believe them to be accurate and truthful.*
- *Do not hide or disguise the true nature of any transaction.*
- *Do not use personal email, personal devices, or ephemeral messaging applications to conduct company business that should be preserved as a record.*

## Company Assets

**OUR STANDARD:** *Appropriately use and protect company assets as well as those of our customers and suppliers.*

> **COMPANY ASSETS** – include *[Company]* products, funds, facilities, equipment, vehicles, information technology, intellectual property, proprietary and confidential information, as well as our company's reputation.

We are entrusted with company and government-provided assets and are personally responsible for protecting them against theft, loss, or abuse, and using them appropriately and for business purposes. Property provided by the government customer or other third party must be used and managed according to the terms of the relevant agreement or contract.

> ***Information Technology***
> Information technology is a valued asset and is provided for the business use of our employees. We should use *[Company]* information technology — such as internet, email, computers, and mobile devices — for authorized business purposes and may not use these resources to view, download, or communicate unlawful, harassing, or otherwise prohibited content (as defined elsewhere in this Code). This includes content that could be considered obscene or offensive, unlicensed software, and copyrighted materials.
>
> Personal use of *[Company]* information technology is discouraged and should be kept to a minimum. Any occasional personal use of our information technology should not adversely affect your productivity or the work environment.
>
> Since the information technology we use when working for *[Company]* belongs to our company, you should not have an expectation that emails, internet activity, computer files, and the like are private. *[Company]* reserves the right to review all information technology usage and will do so in accordance with the law.

***Make sure you:***

- *Immediately report any suspicions of fraud, theft, or misuse of company assets.*
- *Do not share passwords or allow other people to use company resources.*
- *Do not attempt to access any data that you are not authorized to view.*
- *Do not download, install, or run unauthorized or unlicensed software on company information technology.*
- *Never copy, install, or use company software for personal purposes.*

### *Cybersecurity*

Cybersecurity is everyone's responsibility. Attacks on defense and aerospace contractors are common and persistent, and the information we hold — about our contracts, our customers, our technology, and our people — is a known target.

We follow the security controls required by applicable law, contract, and company policy, including the requirements for safeguarding Covered Defense Information and Controlled Unclassified Information under the DFARS and the Cybersecurity Maturity Model Certification (CMMC) program, as well as NIST SP 800-171 and 800-172 where applicable. We report cyber incidents promptly as required by contract and law.

***Make sure you:***

- *Follow company cybersecurity policies and complete required training.*
- *Use only approved devices, networks, and applications for company and customer information.*
- *Be alert to phishing, social engineering, and other attempts to obtain credentials or information and report suspected attempts immediately.*
- *Report lost or stolen devices and suspected or actual cyber incidents immediately.*
- *Do not connect unauthorized personal devices or external storage to company systems.*

### *Insider Threat*

*[Company]* maintains an insider threat program consistent with the National Industrial Security Program requirements. An insider threat can come from a malicious actor or from well-intentioned employees whose behavior inadvertently compromises company or customer information. Employees are expected to be alert to concerning behaviors — such as unauthorized attempts to access information, unexplained affluence, or repeated questioning outside a person's role — and to report concerns to Security or through another channel in this Code.

## Sensitive Information

**OUR STANDARD:** *Protect company proprietary, customer confidential, Controlled Unclassified Information (CUI), and classified information, and intellectual property, from unauthorized disclosure.*

### *Proprietary Information*

*[Company]* proprietary information is one of our most valuable assets and each of us must be vigilant in protecting it. This means keeping company proprietary information secure, limiting access to those who have a need to know, and avoiding discussions in public areas. It is also expected that you will not share the company's proprietary information with anyone outside the company, even after your employment with *[Company]* ends.

Some common examples of what may be considered company proprietary information include business plans, contract proposals and bids, company initiatives, pricing, customer information, and other competitively sensitive non-public business information.

***Make sure you:***

- *Use and disclose company proprietary information only for legitimate business purposes and when authorized.*
- *Properly label proprietary information to indicate how it should be handled and distributed.*
- *Dispose of proprietary information in designated receptacles.*
- *Know which types of information are given heightened protection by the law and company policy, such as personally identifiable information, government-issued identification numbers, and bank account numbers.*

### *Customer Confidential Information*

Our customers place their trust in us and in turn we must protect their confidential information. We may only disclose customer confidential information to co-workers who have a legitimate business need to know, and should not disclose it to people outside our company without authorization.

***Make sure you:***

- *Understand and adhere to the laws, regulations, company policy, and agreements on the use, protection, and retention of information from or about customers.*
- *Immediately report any loss or inadvertent disclosure of customer information.*
- *Take steps to ensure that customer information is secure when off company premises.*
- *Never use customer information for personal gain.*

### *Classified Information*

In many situations, governments have entrusted special information to us which may be classified or require special handling. We have a continuing obligation to protect classified information. Security regulations that relate to the protection of government-classified information are complex and vary by country and government agency. We are required to properly safeguard and control access to this information in accordance with the security guidelines prescribed by the contract, country, or government agency.

***Make sure you:***

- *Be familiar with applicable security regulations and hold the applicable clearance prior to accessing classified information.*
- *Immediately report any known or suspected security infraction or violation.*
- *Only give individuals access to classified information if it has been approved, they possess the necessary clearance level, and they have a "need to know."*

### *Intellectual Property*

**INTELLECTUAL PROPERTY** – includes the following types of information: patents, trademarks, and copyrights; trade secrets; technical data and software developed under or used in support of customer contracts; inventions and discoveries; methods, know-how, and techniques; innovations and designs; systems, software, and technology; and brands.

> *[Company]* retains exclusive ownership of the intellectual property in any idea, process, trademark, invention, or improvement you create while working for the company. *[Company]* must protect our intellectual property carefully as a corporate asset.
>
> We must also safeguard the intellectual property entrusted to us by others — particularly customers, suppliers, and business partners — and not infringe upon the intellectual property rights of others.

***Make sure you:***

- *Report any suspected theft, misuse, or improper disclosure of the company's intellectual property.*

## Artificial Intelligence

**OUR STANDARD:** *Use artificial intelligence responsibly, lawfully, and with appropriate human oversight.*

**ARTIFICIAL INTELLIGENCE (AI)** – technology systems, including machine learning and generative AI tools, that perform tasks that would otherwise require human intelligence — such as drafting text, generating images or code, analyzing large data sets, or making recommendations.

AI offers real benefits for our business and our customers, but it also creates new risks. Inputs to AI tools may become training data. Outputs may be inaccurate, biased, or infringe on the rights of others. AI can be misused to commit fraud, deceive others, or bypass controls.

*[Company]* develops, deploys, and uses AI in ways that are lawful, ethical, and safe, and that include human oversight appropriate to the task. Employees must use only approved AI tools and must follow the *[Company]* AI / Data Use Policy.

***Make sure you:***

- *Only use AI tools that [Company] has approved for the type of work you are doing.*
- *Do not submit [Company] proprietary, customer confidential, classified, Controlled Unclassified Information, export-controlled data, personal information, or trade secrets to an AI tool unless the tool has been specifically approved for that category of information.*
- *Verify AI output before relying on it for any material decision or deliverable, and disclose the use of AI where required by a customer, contract, or policy.*
- *Do not use AI to create or circulate false, misleading, or deceptive content — including deepfakes or synthetic content that impersonates another person.*
- *Raise concerns about AI use that may be inconsistent with our values, our policies, or applicable law.*

## Insider Information

**INSIDE INFORMATION** – information that is confidential, material, not yet disclosed to the public, and that a reasonable investor would take into consideration when deciding whether to buy or sell a security.

Some examples of information about a company that might be considered "inside information" are:

- A proposed acquisition, merger, or sale.
- A significant expansion or cutback of operations.
- A significant product development effort.

- Pending award of a substantial contract.
- Changes in company's senior management or executive structure.
- Extraordinary management or business developments.
- Sensitive corporate financial information.

During the course of our employment at *[Company]*, we may come to know material information about our company or business partners before it is disclosed to the public. This information is often called "inside information" and we are prohibited from trading securities or passing information on to others who then trade on the basis of this information.

***Make sure you:***

- *Do not buy or sell securities of our company when you have inside information.*
- *Do not communicate inside information on [Company] to other people, including family members or friends.*

## Public Communications

**OUR STANDARD:** *Only authorized persons may speak on behalf of the company.*

We are committed to providing accurate and consistent information regarding our operations, products, and services to the public, and we must exhibit objectivity, openness, and honesty in our communications. As a publicly-traded company, we are also subject to regulations that govern how we must disclose material financial information. To meet our standards, *[Company]* needs a consistent voice when making disclosures or providing information. It is important that only authorized persons speak on behalf of the company.

***Make sure you:***

- *Do not make statements that purport to be the company's official position, or that identify you as speaking on the company's behalf, without prior authorization from the Communications Department.*
- *Obtain approval from the Communications Department prior to making public speeches or writing articles for professional journals when you are identified as being an employee of the company.*
- *Obtain approval from the Communications Department before distributing any communication intended for a broad employee audience.*
- *Never give the impression that you are speaking on behalf of the company in any personal communication, including user forums, blogs, chat rooms, and bulletin boards.*

## Social Media

**OUR STANDARD:** *Use social media responsibly and in accordance with company values and policies.*

If you participate in online forums, blogs, wikis, chat rooms, bulletin boards, or other social networks, never give the impression that you are speaking on behalf of *[Company]* unless you are authorized to do so. If you reveal that you are a *[Company]* employee, make it clear that your views are yours alone. Despite privacy settings, all social media are inherently public communication channels, so always think carefully before posting content online.

***Make sure you:***

- *Never post company confidential, export-restricted, or classified information. Do not post information you know to be false, defamatory, or that discloses [Company] Confidential Information, customer-confidential information, classified information, CUI, or export-controlled data.*

- *Never post material that is obscene, threatening, or abusive toward a co-worker, consultant, contractor, customer, supplier, or competitor.*
- *Do not post AI-generated images, audio, or video that could be mistaken for genuine content involving [Company], our customers, our employees, or our products.*

If you ever have any questions about what is or is not appropriate, contact a member of the Communications team.

## Summary

The *[Company]* Code of Conduct articulates for our employees, our customers, and other stakeholders the ethical standard which governs both our business conduct and our relationships with one another.

The Code is intended to help *[Company]* employees understand and adhere to these standards in their daily activities, consistent with our core values of *[Value 1, Value 2, and Value 3]*, and is not intended to serve as a replacement for the laws, regulations, and internal policies that govern our operations.

The Code is one part of *[Company]*'s broader ethics and compliance program, which also includes training, a confidential reporting system, investigations, discipline, ongoing monitoring, and periodic risk assessment. The program is reviewed and updated on a regular basis so that it remains effective as our business and risks evolve.

## Contacts

If you have questions or concerns and would like to speak with someone for advice on ethics or compliance matters, contact your supervisor, compliance representative, Human Resources Department, Legal Department, or Ethics Office.

For general information, please visit the Ethics Office website at *[https://company.com > Ethics Office]*

If you prefer to speak with someone outside of your business area, you may contact our third party helpline provider *[VendorName]* at the contact information provided below.

**Helpline**

**Phone:** *[888.888.8888]*

**Web:** *[www.Companyinc.Helpline.com]*

*[Company]* is a registered trademark of *[Company Inc.]*


*Disclaimer: This document is for reference only and to be used at the consumer's own risk. The Defense Industry Initiative (DII) disclaims any and all liability for any consequences arising out of your use of this document. DII does not guarantee that any or all aspects of this document have been updated to reflect any changes or developments in the law. As such, DII is not responsible for any subsequent regulatory or legal changes that may render this document obsolete. By posting this document, DII is not providing legal advice and is not agreeing to enter into an attorney-client relationship. Please consult with legal counsel to advise you on establishing, maintaining, and auditing your compliance program.*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5B: ETHICS & COMPLIANCE PROGRAM POLICY

## OVERVIEW

This policy is to confirm Company's commitment to conduct business ethically and compliantly and to ensure all ethics and compliance issues are resolved appropriately according to our stated values, Code of Conduct, corporate policies, laws and regulations throughout our operations.

## PROGRAM GOVERNANCE

The Board of Directors, acting through the Audit Committee, oversees the program consistent with the expectation of effective board-level oversight.

### Compliance Function — Authority and Independence

Company designates a Chief Ethics & Compliance Officer (or equivalent) who has direct, unfiltered access to the Audit Committee and independent authority to investigate suspected violations of the Code of Conduct, this policy, other Company policies, or applicable law. No employee, officer, or director may interfere with or override that authority.

### Resourcing

Company commits to providing the program with personnel, budget, training, technology, and access to data and systems sufficient to its risk profile and the size and complexity of Company's operations. Resourcing is reviewed at least annually by the Chief Ethics & Compliance Officer (or equivalent) in coordination with the Chief Executive Officer and the Audit Committee, and adjusted as risk, contract scope, or regulatory expectations change. Where the program shares personnel with other functions, the Chief Ethics & Compliance Officer (or equivalent) documents how independence is preserved in practice.

### Individual Responsibilities

All employees are personally responsible for conducting business both internally and externally with all stakeholders ethically and compliantly in accordance with our values, Code of Conduct, corporate policies, and in compliance with all laws and regulations globally.

### Issue Reporting

Any person who suspects or becomes aware of conduct that may violate Company values, the Code of Conduct, this or any other Company policy, or any applicable law or regulation is expected to report the issue. Reports may be made through any of the following channels:

- Employee's supervisor or manager
- Any Human Resources or Legal representative
- Any compliance representative in the areas of Ethics & Compliance, Internal Audit/Finance, Environmental, Health and Safety, Security, or Trade

- Any Ombudsperson
- Ethics Helpline by phone or web at: 888.888.8888 | www.Companyinc.Helpline.com

In addition, any employee who has any concern or complaint regarding accounting, internal accounting controls, or auditing matters may also report the matter to the General Auditor or contact the Audit Committee on a confidential and/or anonymous basis by mail, c/o the Corporate Secretary, 1234 Street, Suite 1234, City, ST 22222.

Nothing in this policy limits any person's right to report suspected violations of law to a government regulator or to participate in any government investigation or proceeding. See the Non-Retaliation section of the Code of Conduct ***(Resource 5a)***.

### Retaliation

Company prohibits retaliation against any person who, in good faith, asks a question, reports a suspected violation, participates in an investigation, or refuses to engage in conduct that would violate the Code of Conduct, this policy, other Company policies, or applicable law. The Chief Ethics & Compliance Officer (or equivalent) monitors for retaliation following any report and treats suspected retaliation as a matter requiring independent investigation.

The full statement of anti-retaliation protections, including federal contractor whistleblower protections, examples of subtle and overt retaliation, and the procedures for monitoring for retaliation following a report, sits in the Non-Retaliation & Whistleblower Protection Policy ***(Resource 5d)***.

### Case Management and Investigations

All ethics and compliance reports are confidentially recorded and managed in Company's case management system. The intake, triage, investigation, adjudication, and close-out of each matter is governed by the Case Management & Investigations Policy ***(Resource 5c)***, which also covers Company's disclosure obligations. The Chief Ethics & Compliance Officer (or equivalent) is responsible for the operation and continuous improvement of the case management system; details of investigations and corrective actions are sensitive and confidential and are shared on a need-to-know basis only.

## STANDARDS OF CONDUCT AND SUPPORTING POLICIES

The Code of Conduct ***(Resource 5a)*** sets out Company's standards of business ethics and conduct and is the foundation of the program. The Code is supported by the topical compliance policies listed in the Cross-References section below. The Code and these policies are reviewed at least annually, distributed to all covered persons, and flowed down to subcontractors as required by applicable law and contract.

## RISK ASSESSMENT, MONITORING, AND AUDITING

Company conducts a documented compliance risk assessment at least annually and on an event-driven basis when material changes occur (new lines of business, new geographies, significant regulatory developments, M&A activity). The Chief Ethics & Compliance Officer (or equivalent) maintains a monitoring and auditing plan calibrated to the risk assessment, uses data analytics where practicable to identify potential issues proactively, and reports results to the Audit Committee. Findings from monitoring and auditing inform updates to policies, training, and the case management system.

## CONTINUOUS IMPROVEMENT

The program is reviewed and updated based on the results of risk assessments, monitoring, internal investigations, regulatory developments, and benchmarking against industry practice. The Chief Ethics & Compliance Officer (or equivalent) reports at least annually to the Audit Committee on the program's effectiveness, gaps identified, and the plan to address them. Substantive changes to this policy and to the Code of Conduct are approved by the Audit Committee.

## TRAINING AND COMMUNICATION

Company maintains an annual ethics and compliance training program that is risk-tailored, role-tailored, and tracked to completion. All employees, officers, and directors complete Code of Conduct training upon hire or appointment and at least annually thereafter. Personnel in higher-risk roles — including those involved in government contracting, international operations, procurement, finance, human resources, and information security — receive additional, role-specific training. The program also communicates timely guidance on emerging risks and on lessons learned from internal investigations. Training content and effectiveness are reviewed at least annually by the Chief Ethics & Compliance Officer (or equivalent).

### Discipline and Incentives

Substantiated violations of the Code of Conduct, this policy, or other Company policies result in consistent disciplinary action, up to and including termination, regardless of the seniority of the individual or the importance of the business unit. Discipline outcomes are tracked and reviewed by the Chief Ethics & Compliance Officer (or equivalent) for consistency. Company also maintains positive incentives for ethical conduct, including consideration of compliance performance in management evaluations and, where applicable, compensation arrangements that condition awards on adherence to the Code and provide for clawback in the event of misconduct.

### Policy Ownership and Review

The Chief Ethics & Compliance Officer (or equivalent) owns this policy, with Legal, Human Resources, and Internal Audit support. The policy is reviewed at least annually and updated when applicable laws, regulations, or contract requirements change. Material changes are approved by the Audit Committee.

**CROSS-REFERENCES**

*Code of Conduct (Resource 5a)*

*Case Management & Investigations Policy (Resource 5c)*

*Non-Retaliation & Whistleblower Protection Policy (Resource 5d)*

*Conflicts of Interest Policy (Resource 5e)*

*Anti-Corruption & Business Courtesies Policy (Resource 5f)*

*Government Contracting Integrity Policy (Resource 5i)*

*Mandatory Disclosures Policy (Resource 5j)*

*Records Retention Policy (Resource 5l)*

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5C: CASE MANAGEMENT & INVESTIGATIONS POLICY

## OVERVIEW

This policy describes how Company receives, triages, investigates, and resolves reports of suspected misconduct or compliance violations, and how Company coordinates internal case management with the disclosure obligations and government-cooperation frameworks that apply to federal contractors.

## SCOPE

This policy applies to every report of suspected misconduct or compliance violation received through any channel described in the Code of Conduct, regardless of source, severity, or whether the matter implicates a federal contract. It covers the full case lifecycle — intake, triage, investigation, adjudication, and close-out — together with the parallel question of whether and when a matter must or should be disclosed to a government agency.

Nothing in this policy is intended to change, modify, or alter the "at-will" employment relationship between Company and its employees. Practitioner judgment governs the steps appropriate to the individual circumstances of each case. Internal case management does not replace any employee's right to report concerns externally to the U.S. Department of Justice, to the Inspector General of a contracting agency, or to other government authorities; non-retaliation for such reports is governed by the Non-Retaliation Policy.

## KEY TERMS

**Case Management System** — The Case Management System ("System") is a centralized database of complaints. It is used to document new complaints, questions and feedback, and steps taken by people involved in the process. The System also provides the means for analysis of collected data and the production of charts, spreadsheets, and other analytical tools related to that data. (Note: several commercial vendors provide software and/or services that provide this support.)

**Investigation Plan** — An Investigation Plan is a document prepared by the Investigator that lays out the fact finding process to be followed. It describes background documentation to be gathered and interviews to be conducted.

**Investigative Report** — An Investigative Report is a document prepared by the Investigator to provide information needed during a second level review to determine: whether a case is substantiated; appropriate corrective and/or disciplinary actions and root cause analysis for substantiated cases.

**Written Determination** — A Written Determination is a document that records findings on the validity of the case and, as applicable, the root cause. The Written Determination also specifies the corrective and/or disciplinary action that will be carried out in substantiated cases.

**Mandatory Disclosure** — A disclosure to the agency Office of the Inspector General, with a copy to the Contracting Officer, that is required under FAR 52.203-13 when Company has credible evidence of specified violations on a federal contract.

**Voluntary Self-Disclosure (VSD)** — A disclosure to the U.S. Department of Justice (or another regulator) that Company elects to make to obtain cooperation credit, including potential declination, under DOJ's Corporate Enforcement and Voluntary Self-Disclosure Policy or a successor program.

**Escalation Trigger** — A factual indicator in a case that requires immediate notification of the Chief Ethics & Compliance Officer and the Legal Department, regardless of where the matter was first reported. The list of triggers is set out below.

## ROLES & RESPONSIBILITIES

Distinct roles are described below although one person may fulfill more than one role simultaneously. The roles are collapsed and combined as needed while being mindful to avoid any real or perceived conflicts of interest, such as a manager investigating a case against someone in his or her reporting line. Any individual with an apparent conflict of interest makes the conflict known and recuses him or herself.

### Referring Source

A Referring Source is any individual who reports potential misconduct or illegal activity. Referring Sources can be employees, customers, subcontractors, or anyone else who expresses concerns about the conduct of company employees, customers, or subcontractors.

### Intake Individuals

Intake Individuals are representatives of the disclosure channels outlined in the Intake section of this document.

They are responsible for documenting the details of the reports they receive and sending the reports for assignment to an Investigator.

### Subject

The Subject is the person the Referring Source alleges is engaged in misconduct or illegal activity.

### Investigative Functional Leads

Investigative Functional Leads (i.e., designated lead for HR, Legal, Security, Audit, Ethics or similar corporate functions) are responsible for:

- Choosing the appropriate individuals to lead investigations in their functional areas
- Supervising investigations conducted in their functional areas
- Ensuring cases in their functional area receive a second-level review to:
- Determine the sufficiency of the investigation
- Determine case substantiation (whether the evidence supports the claim)
- Make a root cause determination in substantiated cases
- Determine the appropriate corrective and/or disciplinary action in substantiated cases

### Investigators

Investigators are responsible for:

- Conducting fact-finding investigations
- Creating Investigative Reports for second-level review

- Documenting their investigations and the results in the System
- Informing management of investigations (as appropriate, with guidance from Investigative Functional Leads and Human Resources Business Partners)
- Answering questions asked about their investigations and facts/information discovered

### Human Resources Business Partners

Human Resources Business Partners are responsible for:

- Serving as resources to assist Investigators in determining which managers should be informed during each stage of the investigation
- Assisting management in carrying out the corrective and/or disciplinary actions determined
- As appropriate, briefing the Referring Source and Subject on the results of the Investigation
- Partnering with a System Administrator to follow up with the Referring Source to ensure no retaliation has occurred

Management (of the Subject in the case) provides input into decisions about the appropriate corrective and/or disciplinary action(s) in substantiated cases and works with the Human Resources Business Partner to implement the corrective and/or disciplinary action(s) determined.

**Chief Ethics & Compliance Officer** — Overall accountability for the case management system, escalation decisions, and the operation and continuous improvement of this policy. Reports case data and significant matters under investigation to the Audit Committee at least quarterly per the Ethics & Compliance Program Policy ***(Resource 5b)***.

**Legal Department** — Owns mandatory-disclosure decisions under FAR 52.203-13 and voluntary self-disclosure decisions under DOJ programs. Issues litigation and document-preservation holds. Coordinates with outside counsel and government counterparts. Provides guidance on privilege and on parallel-proceeding considerations.

## CASE LIFECYCLE

The case lifecycle has five steps: Intake, Triage and Escalation, Investigate, Adjudicate, and Close-Out. Each step is described below.

### 1. Intake

Employees or other individuals who wish to report possible misconduct by company employees, customers, and subcontractors may make their report through any of the following non-exhaustive list of disclosure channels:

- Employee's manager or other individual in the management chain
- Human Resources Manager
- Chief Ethics Officer, or any member of the Ethics Office
- Anonymous and confidential reporting hotline (if this capability is available)
- Anonymous and confidential online submission at a designated URL (if this capability is available)
- General Counsel
- Chief Executive Officer
- Board of Directors, collectively or individually

### *Written Complaints*

When Intake Individuals receive reports by email or a letter, they forward the reports to an Investigative Functional Lead or the Chief Ethics Officer for proper assignment.

### *Oral Complaints*

When Intake Individuals receive reports in-person or by phone, they document the reporter's name and contact information and gather the following additional information, if possible:

- What alleged misconduct occurred
- Who carried out the alleged misconduct
- When the alleged misconduct occurred
- Where the alleged misconduct occurred
- Who witnessed the alleged misconduct
- Whether there is any additional documentation of the alleged misconduct, such as emails, contracts, resumes, etc.

Intake Individuals document the details of the report received from the Referring Source, thank them, explain that the case will be reviewed in accordance with the company's investigation process, inform the Referring Source of the company's non-retaliation policy, direct them to contact one of the disclosure channels if they believe they have been subject to retaliation, and send the information collected to an Investigative Functional Lead or the Chief Ethics Officer.

### *Anonymous Complaints*

For anonymous reports received through a hotline or online submission using a vendor System that supports an interactive follow-up capability, the Investigative Functional Lead will post a note thanking the Referring Source, informing them of the company's non-retaliation policy, and requesting that they refer back to the report about once per week to see if the Investigators have any questions. System Administrators forward the information to an Investigative Functional Lead or the Chief Ethics Officer.

## 2. Triage and Escalation

The Chief Ethics & Compliance Officer (or a designated Investigative Functional Lead) reviews each new case promptly — ordinarily within two business days of intake — and assigns it for handling. Triage answers four questions:

**What functional area is best positioned to investigate?** Allegations involving statutory or contractual violations or litigation risk are typically routed to Legal; safety matters to Security or Environmental, Health and Safety; harassment or discrimination matters to HR; financial-integrity matters to Internal Audit; trade or export matters to Trade Compliance.

**What is the severity?** Cases are tagged at intake as Routine, Significant, or Critical. The escalation triggers below identify cases that must be elevated regardless of where they first land.

**Are there parallel disclosure obligations?** Triage flags any matter that may trigger FAR 52.203-13 mandatory disclosure or warrant DOJ Voluntary Self-Disclosure consideration. See Mandatory and Voluntary Disclosures, below.

**Who needs to know now?** For Significant or Critical matters, the Chief Ethics & Compliance Officer notifies the General Counsel and, where applicable, the Audit Committee Chair without waiting for the investigation to conclude.

*Escalation Triggers.*

The following matters are escalated immediately to the Chief Ethics & Compliance Officer and the Legal Department, irrespective of where they were first reported:

- credible allegations of fraud, kickbacks, false claims, bribery, or anti-corruption violations on a federal contract;
- credible allegations of mischarging labor, materials, or indirect costs;
- credible allegations involving senior management, finance, internal audit, the legal function, or compliance personnel;
- matters that may require notification to a customer, suspension or debarment authority, or law-enforcement agency;
- matters where the reporter has indicated that they have already reported, or intend to report, to a government regulator;
- safety incidents resulting in serious injury or risk to public health or safety;
- cybersecurity incidents involving classified information, controlled unclassified information (CUI), or covered defense information;
- matters involving export-controlled technology, sanctioned-party dealings, or other trade-compliance issues;
- credible allegations of retaliation against any person who has raised a concern, regardless of the underlying matter; and
- any matter, regardless of category, where the Chief Ethics & Compliance Officer concludes that Audit Committee or Board awareness is appropriate.

This list is not exhaustive. Where doubt exists about whether a matter meets a trigger, the rule is to escalate.

When routing cases, Investigative Functional Leads and Intake Individuals make an initial assessment regarding which functional area is best suited to conduct the fact-finding investigation. Investigative Functional Leads monitor cases routed to them to verify and concur that they have been appropriately directed. They then assign an Investigator to the case.

## 3. Investigate

The assigned Investigator prepares an Investigation Plan and obtains approval from the Investigative Functional Lead before fact-finding begins. The plan identifies the allegations, the witnesses to be interviewed, the documents to be reviewed, the evidence-preservation steps to be taken, and the projected timeline. Plans are revised as the investigation evolves.

Fact-finding includes:

- preservation of relevant records, with a hold notice issued by the Legal Department where appropriate;
- review of background documentation — personnel files, timecards, emails, expense reports, contract files, security logs, system-access logs, and other records pertinent to the allegation;
- interviews with witnesses and the Subject, conducted in a manner that preserves the integrity of the investigation; and
- where applicable, engagement of subject-matter experts or outside counsel through the Legal Department.

When interviewing the Subject, the Investigator gives them an opportunity to provide a statement responding to the allegations. The Investigator does not promise confidentiality where confidentiality cannot be maintained. Where an Investigator is acting under attorney direction, the Investigator gives the appropriate Upjohn warning at the outset of the interview.

Once the Investigator believes he or she has gathered information adequate to determine case validity, the Investigator prepares an Investigative Report. The Investigative Report includes:

- A description of the allegation(s) under investigation
- Relevant background information
- Investigative actions
- References for any documents reviewed during the investigations
- A list of all interviewees
- Findings of fact
- References to applicable company policies
- Summary
- Adjudication

**Streamlined timing.** Investigations are conducted as expeditiously as the facts allow. Routine matters target close-out within 30 days of intake; Significant matters within 60 days; Critical matters proceed on the timeline required by the underlying issue (which may be days, not months, where mandatory-disclosure or government-deadline considerations apply). Where any investigation will exceed its target window, the Investigator notifies the Investigative Functional Lead and the reason is recorded in the case record.

## 4. Adjudicate

The second-level reviewer (typically the Investigative Functional Lead) determines:

- whether the Investigator gathered sufficient information to support a judgment;
- whether the allegation is substantiated, partially substantiated, unsubstantiated, or unable to substantiate;
- for substantiated cases, the root cause of the misconduct; and
- the appropriate corrective and/or disciplinary action.
- The reviewer prepares a Written Determination documenting the result. Like cases are treated alike. Discipline outcomes are tracked across the program for consistency, regardless of the seniority of the individual or the importance of the business unit involved.
- Corrective actions mitigate the risks or process gaps that contributed to the misconduct — for example, improvements to guidance, training, controls, or policies. Disciplinary actions are directed at the individual who engaged in the misconduct and may range from verbal or written reprimand to withheld bonuses or promotions, demotion, or termination.

## 5. Close-Out

The Subject's manager, with assistance from the HR Business Partner, implements the corrective and/or disciplinary action prescribed in the Written Determination. The HR Business Partner provides the case manager with documentary evidence that the action was taken — for example, a copy of a memo to the Subject, training-completion records, or a notice of termination.

After close-out, the HR Business Partner provides the Referring Source and the Subject with a high-level briefing on the outcome of the case, consistent with applicable confidentiality and legal constraints.

The HR Business Partner partners with an Investigative Functional Lead to monitor for retaliation against the Referring Source and any witnesses for an appropriate period after close-out. If retaliation is suspected, a new case is opened. The detailed protocol for retaliation monitoring sits in the Non-Retaliation & Whistleblower Protection Policy ***(Resource 5d)***.

## DISCLOSURES

Company takes potential ethics, compliance, and legal violations seriously and will promptly review reports to determine whether disclosure to a government customer, agency Office of Inspector General, Contracting Officer, the Department of Justice, or another government authority is required or appropriate. Employees must promptly report concerns, preserve relevant records, and cooperate with Company reviews; disclosure decisions are made by Legal in coordination with Ethics & Compliance, Contracts, senior leadership, and outside counsel where appropriate.

### Mandatory Government Contract Disclosures

For covered federal contracts and subcontracts, Company will make any mandatory disclosures required by FAR 52.203-13, including where Legal determines that credible evidence exists of certain federal criminal violations, civil False Claims Act violations, or significant overpayments connected to the award, performance, or closeout of a federal contract or subcontract. Employees are not responsible for making this legal determination, but they must promptly escalate facts that may involve fraud, conflicts of interest, bribery, gratuities, false claims, overpayments, or other serious misconduct.

### Voluntary Self-Disclosures

Some matters may not require mandatory disclosure but may warrant voluntary self-disclosure to DOJ or another government authority. Legal will evaluate whether voluntary disclosure is appropriate based on the facts, applicable DOJ policies, potential government interest, cooperation-credit considerations, remediation, and Company's obligation to respond promptly and responsibly.

### Confidentiality, Cooperation, and Non-Retaliation

Company handles investigation files confidentially and on a need-to-know basis. Where Company asks a participant in an investigation to keep specific facts confidential, the request will be tied to a specific need — protecting witnesses, preserving evidence, maintaining attorney-client privilege, or complying with a legal or contractual obligation — and will be explained at the time. Employees must not interfere with an investigation, conduct their own parallel investigation, destroy or alter relevant records, make knowingly false statements, or retaliate against anyone for raising a concern or participating in a review. Nothing in this policy limits any person's right to report suspected violations of law to a government agency or participate in a government investigation or proceeding.

### Records and Program Improvement

Company will maintain appropriate records of reports, investigations, corrective actions, disclosure decisions, and government communications in accordance with its records-retention requirements. Ethics & Compliance will review report and investigation trends to identify root causes, improve controls, update training, and strengthen the compliance program.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5D: NON-RETALIATION & WHISTLEBLOWER PROTECTION POLICY

## OVERVIEW

This policy, which applies to all employees, is to confirm Company's commitment to non-retaliation and providing an environment that supports any individual who in good faith seeks advice, raises a concern, or reports perceived or observed misconduct. This policy applies to every employee, officer, director, and contingent worker of Company, and to applicants and former employees with respect to protected activity that occurred during their candidacy or employment. It also covers subcontractors, vendors, and other third parties to the extent required by federal law, regulation, or by the underlying contract.

## KEY TERMS

**Retaliation** – occurs when an employer takes adverse employment action against an employee for engaging in a legally-protected activity, such as complaining about discrimination or harassment internally or to an outside body such as the Equal Employment Opportunity Commission, or requesting a legal right such as a reasonable accommodation. Examples of adverse employment actions include demotion, discipline, termination, salary reduction, or reassignment.

**Protected Activity** — reporting, in good faith, a known or suspected violation of the Code, a Company policy, or any law or regulation; cooperating with an investigation, audit, or proceeding (internal or external); refusing to participate in conduct that would violate the Code or the law; or making a disclosure protected by federal whistleblower statutes; or engaging in protected concerted activity under Section 7 of the National Labor Relations Act, including discussing wages, hours, or working conditions with co-workers.

**Good Faith** — making a genuine attempt to provide honest, complete, and accurate information. A report does not lose protection because it later proves to be unsubstantiated or mistaken; it loses protection only where the reporter knowingly made false statements or used the reporting process for an improper purpose.

**Chill on Reporting** — any practice or pattern that discourages a person from making a protected activity disclosure, even if no individual retaliatory act has occurred.

## POLICY

Company prohibits any retaliation against an employee who, in good faith, asks questions, reports possible violations of the Code, policy, or law, or participates in an official investigation. Employees are to immediately report, using any of the avenues listed in the Code of Conduct, any witnessed or suspected retaliation. All reports of retaliation shall be thoroughly investigated and employees engaging in retaliation will be subject to disciplinary action, up to and including termination.

**All supervisors and managers shall:**

- Maintain a work environment free of retaliation and respond immediately and appropriately to complaints or indications of such behavior
- Bring complaints to the attention of Human Resources, Ethics Office, and/or Legal
- Administer disciplinary and other corrective action toward any individual determined to have violated this policy.

These protections supplement federal contractor whistleblower protections and the related contractor-employee notice obligations implemented at FAR 52.203-17.

Nothing in this policy limits your right to discuss wages, hours, working conditions, or other terms and conditions of employment with co-workers or others, or to engage in other concerted activity protected by the National Labor Relations Act. Nothing in this policy limits your right to report suspected violations of law to a government agency, regulator, inspector general, law-enforcement agency, court, or Congress, or to participate in a government investigation, or to receive a whistleblower award.

### Investigations

Complaints of retaliation will be promptly, fairly and thoroughly investigated and, where necessary, appropriate corrective action will be taken. Employees are required to cooperate fully with Company's investigations. To the extent possible, confidentiality will be maintained consistent with applicable legal and ethical considerations.

**An employee shall not:**

- Interfere with or obstruct an investigation
- Conduct their own investigation in a manner that obstructs or compromises Company's investigation (for example, by tampering with evidence, coaching witnesses, or interfering with interviews)
- Destroy records, information or evidence reasonably known to be related to an investigation
- Be knowingly untruthful or knowingly misrepresent or omit facts material to an investigation
- Retaliate against others because of their involvement in an investigation
- Discourage a person from reporting, by word, conduct, or pattern of treatment.
- Misuse performance management, compensation decisions, or staffing decisions to disadvantage a reporter or witness.

## TRAINING

All employees receive training on this policy at hire and at least annually. Managers and supervisors receive additional training on recognizing, preventing, and responding to retaliation, and on how protected activity should be documented to prevent inadvertent reprisal.

## GOVERNANCE

The General Counsel (or designee) owns this policy. The Ethics Office and Human Resources jointly maintain the retaliation matter file. Internal Audit periodically reviews the file and the Helpline data for indicators of chill (drop in reporting volume, clusters of post-report departures, repeated allegations involving the same manager) and reports findings to the Audit Committee or equivalent board-level body.

| CROSS-REFERENCES | |
|---|---|
| | *the Code of Conduct (Resource 5a) — reporting channels and the standard for surfacing concerns;*<br><br>*the Ethics & Compliance Program Policy (Resource 5b) — program ownership, oversight, and culture metrics;*<br><br>*the Case Management & Investigations Policy (Resource 5c) — how Company investigates a report;*<br><br>*the Mandatory Disclosures Policy (Resource 5j) — when an investigation triggers a FAR 52.203-13 disclosure;*<br><br>*the Equal Employment Opportunity Policy (Resource 5v) — protected activity under the EEO statutes;*<br><br>*the Records Retention Policy (Resource 5l) — preservation of investigation and disciplinary records; and*<br><br>*the Information Security & Cybersecurity Policy (Resource 5p) — handling of investigation data and reporter identity.* |

## *APPENDIX: Statutory Whistleblower Protections*

*DRAFTING INSTRUCTION — Several federal statutes give reporters rights independent of this policy. The list below is illustrative; the underlying statutes control.*

Several federal statutes give reporters rights independent of this policy. The list below is illustrative; the underlying statutes control.

- **FAR 52.203-17 / 41 U.S.C. § 4712** — Protects employees of covered federal contractors, subcontractors, grantees, subgrantees, and personal-services contractors from reprisal for disclosures they reasonably believe evidence gross mismanagement of a federal contract or grant, gross waste of federal funds, abuse of authority relating to a federal contract or grant, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a federal contract or grant. FAR 52.203-17 requires employee notice and flowdown of the substance of the clause to subcontracts. For DoD and NASA matters, see 10 U.S.C. § 4701.
- **Defense Contractor Whistleblower Protection (10 U.S.C. § 4701)** — parallel protection for disclosures relating to Department of Defense contracts and grants.
- **False Claims Act (31 U.S.C. § 3730(h))** — protects employees, contractors, and agents from retaliation for lawful acts in furtherance of a False Claims Act (FCA) action or other efforts to stop an FCA violation.
- **Sarbanes-Oxley (18 U.S.C. § 1514A) and Dodd-Frank (15 U.S.C. § 78u-6)** — Protects employees of covered public companies, certain subsidiaries and affiliates, nationally recognized statistical rating organizations, and related officers, employees, contractors, subcontractors, or agents from retaliation for reporting specified fraud or securities-law violations.
- **Anti-Money Laundering Act / AML Whistleblower Improvement Act of 2022** — protects disclosures relating to BSA/AML violations and provides for monetary awards through FinCEN's whistleblower program.

- **DOJ Corporate Whistleblower Awards Program** — a Department of Justice pilot program that may provide discretionary awards to individuals who provide original information leading to certain successful corporate enforcement actions, including in areas not covered by another U.S. government or statutory award program.
- **OSHA Section 11(c) and other workplace-safety statutes** — protect employees who raise health and safety concerns to the employer or to the agency.
- **Anti-discrimination statutes** — Title VII, Americans with Disabilities Act (ADA), ADEA (Age Discrimination in Employment Act), Genetic Information Nondiscrimination Act, the Pregnant Workers Fairness Act, the Equal Pay Act, USERRA (Uniformed Services Employment and Reemployment Rights Act), and analogous state laws prohibit retaliation for protected activity, which may include opposing unlawful practices, participating in investigations or proceedings, requesting covered accommodations, or exercising statutory employment rights.
- **National Labor Relations Act, 29 U.S.C. § 157, 158.** Protects employees' rights to engage in protected concerted activity for mutual aid or protection and prohibits employer interference with those rights.
- **State whistleblower statutes** — many states (including New York and Virginia) provide protections that exceed the federal floor. State law applies in addition to federal law and to the extent it is more protective.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5E: CONFLICTS OF INTEREST POLICY

## OVERVIEW

The purpose of this policy is to identify those activities and relationships in which all Company officers and employees may not engage due to the possibility of a conflict of interest with respect to their obligations to Company. This policy explains the activities and relationships Company employees must avoid or disclose, and how Company identifies, evaluates, and resolves conflicts of interest in connection with U.S. Government work.

## SCOPE

This policy applies to every employee, officer, director, and contingent worker of Company, and to consultants and other third parties acting on Company's behalf to the extent required by their engagement. Employees performing functions designated as "covered" under FAR 52.203-16 (Preventing Personal Conflicts of Interest) are subject to additional disclosure and certification obligations identified by Contracts and Legal.

## KEY TERMS

**Conflict of Interest** — for purposes of this policy, a COI is any situation in which a personal, financial, or organizational interest could influence, or reasonably appear to influence, an employee's or Company's ability to act objectively in the best interest of Company or in the performance of a government contract.

**Personal Conflict of Interest** — as used in FAR 52.203-16, a situation in which a covered employee has a financial interest, personal activity, or relationship that could impair the employee's ability to act impartially and in the best interest of the Government when performing under the contract. Sources include financial interests of the employee, close family members, or household members; other employment or financial relationships (including seeking or negotiating prospective employment); and gifts, including travel. A de minimis interest that would not impair impartiality is not covered.

**Organizational Conflict of Interest (OCI)** — as defined at FAR 9.501, a situation in which, because of other activities or relationships with other persons, Company is unable or potentially unable to render impartial assistance or advice to the Government, Company's objectivity in performing the contract work is or might be otherwise impaired, or Company has an unfair competitive advantage. The categories of OCI recognized in case law are impaired objectivity, unequal access to information, and biased ground rules.

**REGULATORY WATCH** — *OCI rules pending wholesale revision. The FAR Council's proposed rule at FAR Case 2023-006, 90 Fed. Reg. 4017 (Jan. 15, 2025) — implementing the Preventing Organizational Conflicts of Interest in Federal Acquisition Act, Pub. L. 117-324 — would relocate the OCI rules from FAR Subpart 9.5 to a new FAR Subpart 3.12 and reorganize the case law taxonomy (impaired objectivity, unequal access to information, and biased ground rules) into two categories: impaired objectivity and unfair competitive advantage, with unequal access to information and biased ground rules treated as sub-types of unfair competitive advantage. The proposed rule also adds new defined terms (including Entity and Firewall) and a new family of 52.203-series solicitation and contract clauses with broader disclosure and tighter timing obligations. Separately, the Revolutionary FAR Overhaul under E.O. 14275 (Apr. 15, 2025) and OMB M-25-26 (May 2, 2025) is rewriting FAR Part 3 but, as of the date of this policy, has not absorbed the proposed OCI rule. Until a final OCI rule issues, FAR Subpart 9.5 and the existing case-law taxonomy govern; Company will conform this definition and related procedures upon issuance.*

**Immediate Family** — spouse or domestic partner, parents, children, siblings, in-laws, and any other person who shares the employee's household.

**Business Associate** – any organization or individual that conducts or seeks to conduct business transactions with Company, which includes, but is not necessarily limited to, customers, contractors, subcontractors, suppliers, vendors, consultants, agents, joint venture members, teaming agreement members, and governmental agencies.

## POLICY

All employees are expected to recognize and avoid engaging in any activities or relationships that would influence or appear to influence their ability to fulfill their duties to Company, or to make objective, ethical business decisions on behalf of Company.

### Potential Conflicts of Interest

Employees are expected to recognize and avoid activities or relationships that interfere with — or appear to interfere with — their ability to make objective decisions on behalf of Company. The list below is not exhaustive; when in doubt, disclose.

### Acceptance of Gifts and Business Courtesies

Employees and their immediate family members may not accept money, gifts, hospitality, services, or other benefits of more than nominal value from a Business Associate in connection with Company business. Cash and cash equivalents (including gift cards) are prohibited regardless of amount. Specific limits and approval procedures are in the Anti-Corruption & Business Courtesies Policy ***(Resource 5f)***.

### Personal Relationships

Personal relationships — household members, close relatives, romantic partners, and close friends — may give rise to a conflict where one party has, or appears to have, influence over the other through the chain of command, in purchasing or contracting decisions, in bidding or proposal related efforts, or in recruiting or hiring decisions. Employees must recognize, avoid, and disclose any such situation. Supervisors who learn of one notify Human Resources or the Ethics Office.

### Political Office and Outside Activity

Employees retain the right to seek elected or appointed government office and to participate in political and civic activity on their own time. Such activity must be disclosed where it could affect, or appear to affect, Company's interests, and may not use Company name, time, funds, assets, or facilities. Lobbying and political-contribution activity is governed by the Government Relations Policy ***(Resource 5ab)***.

### Financial Interests

Employees and their immediate family members may not hold a substantial financial interest in any Business Associate, except for passive investments held as part of a personal investment program (for example, mutual funds or diversified index holdings). A direct ownership stake in a privately held supplier, customer, or competitor must be disclosed.

## Outside Employment, Affiliation, and Board Service

Employees may not be employed by, consult for, serve on the Board of, or be otherwise affiliated with a Company competitor, customer, supplier, or other Business Associate without prior approval. Approval is obtained through the disclosure process below. Subject to time availability and good industry practice, employees are encouraged to participate in professional associations, civic, and charitable activities that do not create a conflict.

## Use of Company Resources

Employees may not use Company facilities, time, equipment, information, or other assets in pursuit of non-Company business activities.

Any employee violating this policy or failing to notify management of a potential conflict of interest shall be subject to disciplinary action up to and including termination.

## Organizational Conflicts of Interest (OCI)

Company identifies and addresses OCIs on every U.S. Government opportunity. The principal OCI types under FAR Subpart 9.5 are:

**Impaired Objectivity** — Company is asked to evaluate or make recommendations about its own (or an affiliate's) products, services, or work.

**Unequal Access to Information** — Company has, or could obtain, non-public competition-sensitive information through one engagement that would give it an unfair advantage in another.

**Biased Ground Rules** — Company has helped set the requirements, ground rules, or evaluation criteria for a procurement in which it now intends to compete.

OCI risk is screened at capture, before bid/proposal submission, on contract award, and whenever a new task order, modification, or affiliate engagement could change the picture. Identified OCIs are documented, evaluated by Legal, and resolved by avoidance, mitigation (firewalls, recusal, divestiture, organizational separation), or declining the work.

## Disclosure and Resolution

Personal conflicts and potential personal conflicts are disclosed in writing to the employee's supervisor and Human Resources or the Ethics Office. Organizational conflicts and potential OCIs are disclosed to Legal. Disclosure does not, by itself, resolve a conflict — Company decides, on the basis of the disclosure, whether the activity may continue, must be modified (recusal, firewall, divestiture), or must be discontinued.

Disclosure is required at the earliest of (i) joining Company, (ii) the change in circumstances that creates the conflict, and (iii) the start of an activity, transaction, or procurement to which the conflict relates. Employees update their disclosure whenever circumstances change.

## Annual Certification

All employees, and any contingent workers and consultants identified by Contracts, complete an annual conflicts-of-interest certification. The certification confirms that the individual has read this policy, has disclosed any personal conflicts or potential personal conflicts, and has no undisclosed financial, employment, family, or other relationship that would create a conflict. Officers, directors, employees performing covered acquisition functions under FAR 52.203-16, and other categories identified by Legal complete a more detailed annual certification.

## TRAINING

All employees receive training on this policy at hire and at least annually. Capture, business development, and program management personnel receive additional training on OCI identification and mitigation. Employees performing covered acquisition functions under FAR 52.203-16 receive role-specific training on personal conflict of interest.

## GOVERNANCE

The General Counsel (or designee) owns this policy. Human Resources administers personal conflict-of-interest disclosures and the annual certification. The Contracts function, supported by Legal, owns OCI screening, mitigation plans, and Contracting Officer disclosures. Internal Audit periodically tests compliance with the disclosure and certification process and reports findings to the Audit Committee or equivalent board-level body.

**CROSS-REFERENCES**

*the Code of Conduct (Resource 5a) — the standard and channels for raising concerns;*

*the Ethics & Compliance Program Policy (Resource 5b) — program ownership, oversight, and culture metrics;*

*the Case Management & Investigations Policy (Resource 5c) — how Company investigates a possible violation;*

*the Non-Retaliation & Whistleblower Protection Policy (Resource 5d) — protection for anyone who raises a conflict-of-interest concern;*

*the Anti-Corruption & Business Courtesies Policy (Resource 5f) — gifts, hospitality, and payments to officials;*

*the Third-Party Due Diligence Policy (Resource 5h) — screening of teaming partners, subcontractors, and consultants;*

*the Government Contracting Integrity Policy (Resource 5i) — bid-and-proposal information, source selection, and certification integrity;*

*the Mandatory Disclosures Policy (Resource 5j) — when a conflict-of-interest matter triggers FAR 52.203-13 disclosure;*

*the Records Retention Policy (Resource 5l) — preservation of OCI screens, disclosures, and mitigation plans;*

*the Procurement Integrity Policy (Resource 5u) — supplier qualification and small business utilization; and*

*the Government Relations Policy (Resource 5ab) — political activity, lobbying, and campaign contributions.*

## VIOLATIONS

Failure to comply with this policy — including failing to disclose a conflict, providing a false or incomplete certification, ignoring a known OCI, or using Company resources for non-Company activity — is grounds for disciplinary action up to and including termination.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5F: ANTI-CORRUPTION & BUSINESS COURTESIES POLICY

## OVERVIEW

This policy prohibits Company employees from engaging or participating in bribery, kickbacks and other forms of improper payments and sets limits on giving business courtesies. Company is committed to conducting business ethically, honestly, and in compliance with the anti-corruption and anti-bribery laws of every country where we operate. We compete on the merits — never through bribes, kickbacks, or other improper payments. This policy sets the standard, identifies the conduct that is prohibited, and tells you what to do when a situation looks risky.

This policy applies to every employee, officer, and director of Company, and to consultants, agents, representatives, distributors, intermediaries, joint-venture and teaming partners, and other third parties acting on Company's behalf to the extent required by their engagement.

## KEY TERMS

**Bribe** — for purposes of this policy, a bribe means anything of value offered, promised, given, requested, or accepted to obtain or retain business or any improper advantage. "Anything of value" is broad: it includes cash and cash equivalents, gifts, hospitality, travel, entertainment, internships and job offers, charitable or political contributions made at someone's direction, and discounts not generally available.

**Kickback** — the return of any portion of a payment, fee, or other consideration as a reward for awarding, retaining, or steering business.

**Facilitating Payment** — a small payment or gift made to a low-level government official to expedite a routine, non-discretionary governmental action (a so-called "grease payment"). These are prohibited under this policy.

**Foreign Official** — any official, employee, or representative of a non-U.S. government, government department or agency, state-owned or state-controlled enterprise, public international organization (e.g., the United Nations, World Bank), or royal family; any foreign political party, party official, or candidate for foreign political office; and the immediate family members and close relatives of any of the above.

**Government Official (U.S.)** — any official or employee of a federal, state, local, territorial, or tribal government in the United States, including legislative, executive, judicial, regulatory, and military personnel.

**Commercial Customer** — any individual or entity that is not, in whole or in part, owned or controlled by a government.

**Business Courtesy** — any item of value offered to or accepted from a third party in connection with Company business, including gifts, meals, entertainment, hospitality, travel, lodging, favors, gratuities, discounts, and services.

**Third Party** — any agent, representative, distributor, intermediary, labor broker, subcontractor, freight forwarder, dealer, consultant, joint venture or teaming partner, or other person retained by Company to act on Company's behalf.

# POLICY

## Anti-Bribery

Bribery is never permitted — anywhere, in any amount, with anyone. Company employees, and anyone acting on Company's behalf, may not directly or indirectly offer, promise, authorize, give, solicit, or accept anything of value to or from any Government Official, Foreign Official, Commercial Customer, or other person to obtain or retain business or any improper advantage.

This policy is anchored to the laws that apply to Company's business, including the U.S. Foreign Corrupt Practices Act (FCPA), the U.S. Foreign Extortion Prevention Act (FEPA), the U.K. Bribery Act, the U.K. Economic Crime and Corporate Transparency Act (ECCTA), and the anti-corruption and anti-bribery laws of the other countries in which we operate. Where laws differ, the strictest standard applies.

## Bribery of Government Officials and Foreign Officials

No one acting for Company may offer, promise, authorize, or give anything of value to any U.S. Government Official or Foreign Official to influence an official act, secure an improper advantage, induce the official to violate a duty, or obtain or retain business. The same prohibition applies to indirect payments — through an agent, family member, charitable contribution, or any other channel.

It is also prohibited to solicit, demand, or accept a bribe from anyone acting for Company. FEPA makes it a federal crime for a Foreign Official to demand or accept a bribe from a U.S. business; if a Foreign Official asks Company for a payment to act, refrain from acting, or steer a decision, the request must be refused and reported to Legal.

## Commercial Bribery

The same rules apply to interactions with Commercial Customers, suppliers, and their employees. No one acting for Company may offer or accept anything of value to obtain or retain business or any improper advantage from a private-sector counterpart. Commercial bribery is prohibited under U.S. and foreign law and under this policy regardless of whether a government is involved.

## Use of Third Parties and Project Partners

Company cannot do through a third party what it is prohibited from doing directly. No agent, consultant, intermediary, distributor, joint-venture partner, or other third party may be used as a channel for an improper payment. Before engaging a third party that will interact with Government Officials, Foreign Officials, or government-affiliated commercial customers on Company's behalf, Company conducts the diligence required by the Third-Party Due Diligence Policy ***(Resource 5h)***, and the engagement is governed by a written agreement that flows down anti-corruption requirements, audit rights, and termination rights.

## Facilitating Payments

Facilitating payments — small unofficial payments to low-level officials to expedite routine, non-discretionary government action — are prohibited under this policy. You must obtain approval from the Legal Department in the event this issue arises, no matter how small the amount. The only exception may be a payment made under imminent threat to a person's health or safety; any such payment must be reported to Legal as soon as it is safe to do so and recorded accurately in Company's books. Although a narrow facilitating-payments exception exists under the

FCPA, the U.K. Bribery Act and many other jurisdictions treat these payments as bribes; Company applies the stricter standard everywhere.

## Books, Records, and Internal Controls

All payments and receipts must be recorded accurately, in reasonable detail, and in accordance with Company's accounting procedures. No undisclosed or off-book funds or assets may be maintained, and no false, misleading, or incomplete entry may be made in any record for any reason. The FCPA's books-and-records and internal-controls provisions apply to issuers and their consolidated subsidiaries; Company applies the same discipline across the enterprise. Managers are responsible for maintaining controls reasonably designed to ensure that transactions are properly authorized and recorded, that assets are safeguarded, and that anti-corruption issues are detected and corrected.

## Business Courtesies

Business courtesies — gifts, meals, entertainment, hospitality, travel, and similar items of value — may sometimes be appropriate for building legitimate business relationships, but extra caution must be taken with government customers. Courtesies are never appropriate when their purpose, or appearance, is to influence a business decision or secure an improper advantage. The rules below apply to courtesies offered or accepted by employees, by family members and close friends in connection with Company business, and by anyone acting on Company's behalf.

## U.S. Government Officials

The U.S. government has strict rules limiting what its officials and employees may accept. Reasonable de minimis hospitality permitted by the applicable statutes, regulations, or congressional ethics rules — for example, coffee and light refreshments at a business meeting, or modest Company-branded items such as a pen or mug — may be extended without prior approval. All other business courtesies for U.S. Government Officials require prior written approval from Legal.

## Foreign Officials

A gift, meal, entertainment, travel, lodging, or other thing of value provided to a Foreign Official can be treated as a bribe under the FCPA, FEPA, the U.K. Bribery Act, or local law. Before offering or providing anything of value to a Foreign Official — other than nominal or de minimis items consistent with this policy and local custom — employees must obtain prior written approval from Legal. Travel, lodging, and meals connected to a legitimate business purpose (for example, a customer site visit) may be permitted with Legal's advance approval and proper documentation.

## Commercial Customers and Counterparts

Business courtesies provided to or accepted from a commercial counterpart must be reasonable, infrequent, in good faith, for a legitimate business purpose, and consistent with industry practice and local law. Cash and cash equivalents (including gift cards) may not be offered or accepted in any amount. Travel, lodging, and meals beyond modest hospitality may require Legal's prior approval. Employees involved in an active solicitation, proposal, source-selection, or contract negotiation with a counterpart may not offer or accept any business courtesy from that counterpart while the activity is open.

### Charitable and Political Contributions

A charitable contribution may not be made by or on behalf of Company at the request, suggestion, or for the benefit of any Foreign Official, Government Official, foreign political party, or candidate for foreign political office. Contributions to organizations outside the United States must be reviewed and approved in advance by Legal. Domestic charitable contributions are made in accordance with Company's charitable-giving procedures. Political contributions and lobbying activity are governed by the Government Relations Policy ***(Resource 5ab)*** — including the prohibition on the use of Company funds or assets for partisan political purposes in any country.

### Reporting and Whistleblower Awards

Any suspected bribery, kickback, facilitating payment, books-and-records irregularity, or other anti-corruption concern must be reported promptly to Legal, the Ethics Office, or through one of the channels described in the Code of Conduct, including the Helpline (888.888.8888). Reports may be anonymous. The Non-Retaliation & Whistleblower Protection Policy ***(Resource 5d)*** protects anyone who raises a concern in good faith.

Federal whistleblower-award programs may pay awards to individuals who report certain corporate misconduct directly to regulators or to DOJ. Company supports these channels: no agreement, policy, or practice may prohibit, condition, or discourage a person's right to report a possible violation of law to a regulator, an Inspector General, law enforcement, or any other authority, or to receive a whistleblower award. Reporting internally first is encouraged so that Company can investigate and remediate, but it is not required.

### Disclosure

Where credible evidence of a federal-criminal-law violation involving bribery or gratuity offenses arises in connection with a federal contract or subcontract, Company's disclosure obligations are governed by the Mandatory Disclosures Policy ***(Resource 5j)*** and the FAR clauses cited there. Cooperation, voluntary self-disclosure, and timing decisions are made by Legal, recognizing that recent DOJ guidance treats prompt, full, and cooperative disclosure as a meaningful mitigating factor.

## TRAINING

All employees receive anti-corruption and business-courtesies training at hire and at least annually. Personnel in higher-risk roles — international sales, business development, supply chain, government engagement, mergers and acquisitions, finance and accounting — receive role-based training tailored to their exposure. Third parties acting on Company's behalf receive or certify to anti-corruption requirements as set out in the Third-Party Due Diligence Policy ***(Resource 5h)***.

## GOVERNANCE

The General Counsel (or designee) owns this policy. The Chief Ethics & Compliance Officer is responsible for the anti-corruption program, including risk assessment, training, monitoring, and reporting to senior management and the Board (or its delegated committee). Internal Audit periodically tests the operation of the program, including books-and-records and internal-controls compliance, in coordination with the Ethics & Compliance Program Policy ***(Resource 5b)***. Company monitors developments and updates this policy and the program as needed.

**CROSS-REFERENCES**

*the Code of Conduct (Resource 5a) — the standard and channels for raising concerns;*

*the Ethics & Compliance Program Policy (Resource 5b) — program ownership, oversight, and culture;*

*the Case Management & Investigations Policy (Resource 5c) — how Company investigates a suspected violation;*

*the Non-Retaliation & Whistleblower Protection Policy (Resource 5d) — protection for anyone who raises an anti-corruption concern;*

*the Conflicts of Interest Policy (Resource 5e) — personal financial interests, gifts in personal-relationship contexts, and outside affiliations;*

*the Third-Party Due Diligence Policy (Resource 5h) — risk-based screening and monitoring of agents, consultants, and other third parties;*

*the Government Contracting Integrity Policy (Resource 5i) — gifts and gratuities involving federal officials and counterparts on a federal contract;*

*the Mandatory Disclosures Policy (Resource 5j) — when an anti-corruption matter triggers FAR 52.203-13 disclosure;*

*the Records Retention Policy (Resource 5l) — retention of diligence files, approvals, and gift/hospitality logs;*

*the Sanctions Compliance Policy (Resource 5n) — restricted-party screening that intersects with anti-corruption diligence;*

*the Procurement Integrity Policy (Resource 5u) — supplier qualification and award integrity; and*

*the Government Relations Policy (Resource 5ab) — political contributions, lobbying, and engagement with public officials.*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5G: ANTITRUST & FAIR COMPETITION POLICY

## OVERVIEW

Company prohibits all business practices that improperly limit competition in those jurisdictions where the Company conducts business. It is Company policy to comply fully and in good faith with the antitrust and competition laws of the countries in which the Company and its affiliates conduct business. The Legal Department is responsible for deployment of this policy, and all Company employees are individually accountable for complying with it.

## SCOPE

This policy applies to every Company employee, officer, and director, and to consultants, agents, teaming partners, joint-venture partners, distributors, and other third parties acting on Company's behalf. It applies to every market and jurisdiction where Company conducts business, whether commercial or government.

## POLICY

### Principal Antitrust and Competition Laws

Antitrust laws prohibit business practices that improperly limit competition. In the U.S., the principal statutes are the Sherman Act, which prohibits unlawful agreements in restraint of trade and prohibits monopolization and attempts to monopolize; the Clayton Act, which prohibits certain customer restraints, acquisitions, exclusive dealing, tying, and interlocking directorates; the Robinson-Patman Act, which prohibits certain discriminations in price or in promotional assistance in the sale of commodities; and the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices. Within the EU, the competition rules are set out in the Treaty on the Functioning of the European Union along with the Member States' national competition laws; abuse of a dominant market position is prohibited, as are agreements that prevent, restrict, or distort competition. Other countries — including Canada, the United Kingdom, and a growing number of jurisdictions in Africa, South America, and Asia — also enforce competition or antitrust laws with which Company must comply, often with extraterritorial reach.

Where laws differ, the strictest standard applies.

### Relations with Competitors

The following non-competitive practices are strictly prohibited by Company because they are per se unlawful under applicable law or because they may present a significant risk of violation of the law:

- **Price-fixing:** agreements between competitors to fix or adhere to prices, or to terms or conditions of sale of products or services sold to or purchased from third parties.
- **Exchange of Prices:** the exchange of competitively sensitive information between competitors relating to prices or to terms or conditions of sale to any third party.
- **Agreements Not to Compete:** bid-rigging; agreements to allocate, divide, or assign customers, markets, or territories.

- **Boycotts:** joint refusals to deal with third parties.
- **Wage-Fixing and No-Poach Agreements:** agreements among employers to fix wages or other terms of employment, or to refuse to solicit or hire each other's employees, which the U.S. Department of Justice now prosecutes criminally under the Sherman Act.

In addition to these practices, all agreements between competitors that unreasonably restrain competition in any market are unlawful and are prohibited. Since the practices described in this policy do not encompass every type of conduct that may constitute an illegal restraint of trade, any proposed practice that appears to have an unreasonable effect on competition shall be brought to the attention of the Legal Department.

### Relations with Customers

Company employees may not engage in the following activities without the prior approval of the Legal Department:

- Resale Price Maintenance: an agreement with a customer to fix the minimum price at which that customer or other customers will resell Company products.
- Tying Arrangement: an agreement to sell one product or service only on condition that the buyer also purchase a different product or service from the seller.
- Exclusive Dealing Arrangement: an agreement by a customer to deal exclusively with Company, or by Company to deal exclusively with one customer.
- Reciprocity: an agreement by one party under which it will buy from another party only if that other party will buy from it.
- Territorial and Customer Restrictions: a restriction upon the territory in which, or customers to which, a customer may resell a product.

Accordingly, Company employees shall seek legal advice from the Legal Department prior to terminating any customer relationship and on all issues of potential price discrimination.

### Reporting and Cooperation with Investigations

Company employees shall promptly report to the Legal Department any inquiries or investigations of antitrust or competition matters. Company shall cooperate with all domestic and international enforcement agencies investigating alleged violations, and all responses to inquiries and investigations shall be coordinated through and supervised by the Legal Department. Employees may not respond to a subpoena, civil investigative demand, or other contact from a competition authority, or destroy or alter related documents, without Legal's involvement.

## TRAINING

Trade associations are a frequent source of antitrust risk. Company business development, sales, marketing, procurement, and other key employees shall receive routine training and guidance regarding antitrust compliance, including membership and participation in trade association meetings.

## GOVERNANCE

The Legal Department is responsible for developing and implementing a corporate-wide antitrust compliance program, which shall include at a minimum the promulgation and maintenance of antitrust policies, the establishment of training requirements, the development and implementation of any necessary assessment tools and review protocols, and

the provision of legal advice as required. Business unit leadership, with the assistance of the Legal Department, shall establish, maintain, and execute accompanying antitrust procedures that deter, detect, and promptly resolve potential issues.

**CROSS-REFERENCES**

*the Code of Conduct (Resource 5a) —*
*the standard and channels for raising concerns;*

*the Ethics & Compliance Program Policy (Resource 5b) —*
*program ownership, oversight, and culture;*

*the Case Management & Investigations Policy (Resource 5c) —*
*how Company investigates a suspected violation;*

*the Non-Retaliation & Whistleblower Protection Policy (Resource 5d) —*
*protection for anyone who raises an anti-corruption concern;*

*the Conflicts of Interest Policy (Resource 5e) —*
*outside affiliations, board service, and competitor-adjacent relationships;*

*the Anti-Corruption & Business Courtesies Policy (Resource 5f) —*
*anti-corruption rules that frequently overlap with antitrust risk in third-party engagements;*

*the Third-Party Due Diligence Policy (Resource 5h) —*
*risk-based screening of teaming partners, distributors, and other intermediaries;*

*the Government Contracting Integrity Policy (Resource 5i) —*
*procurement integrity, certifications, and bid and proposal information protections;*

*the Mandatory Disclosures Policy (Resource 5j) —*
*disclosure obligations when antitrust conduct touches a federal contract;*

*the Records Retention Policy (Resource 5l) —*
*retention of antitrust files, pre-clearance approvals, and trade-association records; and*

*the Procurement Integrity Policy (Resource 5u) —*
*buy-side anti-collusion controls in supplier selection.*

## VIOLATIONS

A violation of this policy by any employee may result in disciplinary action, up to and including termination.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5H: THIRD PARTY DUE DILIGENCE POLICY

## OVERVIEW

This policy establishes how Company evaluates, approves, monitors, and records its relationships with third parties engaged to act for or on behalf of Company. Third parties create legal, regulatory, and reputational exposure for Company. The purpose of this policy is to make sure that exposure is identified before a relationship is formed and is managed for as long as the relationship continues.

This policy applies to every employee, officer, director, contractor, and other person who proposes, sponsors, approves, manages, or oversees a Company relationship with a third party. It applies to all third parties as defined below, regardless of whether the third party is located inside or outside the United States, whether the underlying business is commercial or government, whether the engagement is paid or unpaid, and the form of the engagement (services, distribution, teaming, joint venture, MOU, retainer, or other). This policy applies globally. It is not limited to third parties operating outside the United States.

## KEY TERMS

**Foreign Official** — As defined in the Anti-Corruption & Business Courtesies Policy ***(Resource 5f)***. Includes employees and officials of non-U.S. governments and state-owned enterprises, candidates for foreign office, officials of public international organizations, and members of royal families, together with their close relatives.

**Third Party** — Any agent, representative, distributor, reseller, consultant, intermediary, labor broker, lobbyist, subcontractor, freight forwarder, dealer, joint-venture or teaming partner, or any other person or entity engaged by Company to provide goods or services to, for, or on behalf of Company. The term includes lower-tier subcontractors and suppliers where the Company contractually requires flowdown of this policy or its substantive elements.

## POLICY

Company may use third parties in connection with executing its business. Company employees must follow the procedures set forth in this policy. No third party shall be retained if the third party, any person employed by the third party or any person financially interested in the third party's business is an employee or official of a customer or potential customer of Company or is a close relative of such an employee or official.

### Due Diligence Review

Due diligence must be performed and documented by Company before engaging third parties. Due diligence, at a minimum, will include screening the third party and known employees against the U.S. and foreign governments denied parties' lists and an annual compliance certification signed by the third party.

Increased due diligence will be conducted on third parties according to their location, type of third party (i.e. consultant, dealer, marketing representative, subcontractor etc.), estimated volume of sales or amount of subcontract, and the level of contact with foreign commercial customers and Foreign Officials on behalf of Company. Due diligence on supply-chain third parties also addresses forced-labor risk. Similar foreign supply-chain due-diligence regimes may also apply to Company operations or counterparties; Legal will determine applicability case by case.

Government contracting considerations: where a third party will support performance of a U.S. government contract, additional considerations may apply including CMMC and cybersecurity flowdowns, Buy American and country-of-origin representations, Code of Conduct reporting obligations, and prohibitions on consulting and advisory arrangements involving adversary nation entities.

## Screening Requirements

**Restricted-Party Screening** — Every prospective third party, and to the extent practicable each known director, officer, beneficial owner, and on-site participant, is screened against the Sanctioned-Party lists before engagement and re-screened at least annually and upon any material change. Hits are escalated to Legal before any further engagement activity.

**Beneficial Ownership Screening** — Third parties are screened for ownership and control sufficient to identify Beneficial Owners. Screening accounts for applicable U.S. ownership-aggregation rules (e.g., OFAC's 50 Percent Rule and the Bureau of Industry and Security (BIS) Affiliates Rule), under which an entity may be treated as restricted where one or more restricted persons hold 50 percent or more of the entity in the aggregate, directly or indirectly. Where a Beneficial Owner is from an Adversary Nation, or where ownership cannot reasonably be determined, the engagement is escalated or declined.

**Sanctions, Export, and End-Use Screening** — Trade-related screening — including end-use, end-user, and destination — is performed in coordination with the Export & Import Compliance Policy ***(Resource 5m)*** and the Sanctions Compliance Policy ***(Resource 5n)***.

## Requirement for a Written Agreement

All third parties engaged by Company must have a written agreement that fully describes all services and compensation prior to the performance of any services. A third party, its employees, and owners must be engaged in providing legitimate business services for a fee or discount not in excess of the customary local rates. Compensation must be commensurate with the services performed and consistent with customary local rates. Payments are made in the name of the contracted entity, in the location where services were performed, in local currency where required, and only by traceable means (bank transfer or check), unless an exception is approved in writing by the Controller and Legal.

## Monitoring Third Parties

Company personnel, who are responsible for engaging third parties, must monitor the performance of third parties to ensure that they are complying with all applicable laws, the Company Code of Conduct, Company policies and procedures, and contract requirements on all matters including anti-corruption provisions. The business will maintain a list of third parties that, at a minimum, is updated annually.

## Payments and Recordkeeping

Accurate books and records must be maintained of payments made to third parties, in accordance with Company Financial policies.

Payments to third parties may only be made after confirmation that services have been performed or goods have been received. No third party may use its fees or any other funds to make any payments to any Foreign Official, government customer, or commercial customer of Company or any other persons or entities related to their work for Company in violation of US or local law.

## Anti-Corruption Compliance Regarding Third Parties

Company is committed to conducting its business in accordance with its strict anti-corruption policies, the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, the Foreign Extortion Prevention Act, and the anti-corruption laws of the countries in which it operates by prohibiting the offer, payment, or receipt of corrupt and other improper payments. Improper payments made on behalf of Company by third parties are strictly prohibited. No person or third party shall ever be used as an instrument to make improper payments in connection with Company business. Company cannot do indirectly what it is prohibited from doing directly. Reference the Anti-Corruption / Business Courtesies policy for further information.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5I: GOVERNMENT CONTRACTING INTEGRITY POLICY

## OVERVIEW

The purpose of this policy is to provide each Company employee with general guidance for compliance with the laws and regulations specific to contracting with the U.S. Government. It is not intended to cover each and every specific situation or topic. Consult with Company legal departments for further information and guidance.

Doing business with the U.S. Government carries obligations that go beyond commercial contracting. The complex legal framework creates binding obligations whenever Company performs federal work. Compliance is not optional, and obligations cannot be displaced by a customer instruction, a teaming agreement, or internal pressure to win or deliver: The Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), the False Claims Act, the Anti-Kickback Act, and the Procurement Integrity Act create a regulatory floor that applies to every prime contract, every subcontract under a federal flow-down, and every certification or representation we sign.

This policy applies to every employee, officer, director, and contingent worker who participates in any aspect of a federal prime contract or federally-funded subcontract, including: pursuit decisions, proposal preparation, certifications and representations, contract negotiation, performance, subcontracting, billing, and close-out. It also applies to anyone who signs a representation or certification on behalf of Company in connection with a federal contract, grant, cooperative agreement, or other transaction.

## POLICY

Company employees involved in doing business with the U.S. Government are expected to perform their jobs with honesty and integrity, to comply with the Company Code of Conduct, to comply with all applicable U.S. Government contracting laws and regulations, and to comply with all applicable U.S. Government contract terms and provisions.

### Policy — Consequences

Disregard of these principles and expectations can expose Company to price reductions, the withholding of payments, civil and criminal fines and penalties, contract termination, suspension and debarment, and will be grounds for appropriate disciplinary action, including termination of employment. Individuals found guilty of violations of certain laws and regulations referenced in this policy may also be subject to fines and imprisonment.

### Recording, Allocating and Charging Costs

It is the responsibility of all Company employees who charge time to a U.S. Government contract to comply with the requirements of Company's timekeeping system. All employees must be aware of the rules that govern the recording, allocating and charging of costs to the U.S. Government. Employees must also ensure that no improper or false entries are made to accounting records or other company records, and that no improper amounts are charged to U.S. Government contracts.

### Recording, Allocating and Charging Costs — Individual Responsibility

Each employee is responsible for properly recording, allocating and charging their own time and attendance data. No supervisor shall approve an employee's labor record knowing it contains false information.

Charge time only to the contract or project actually worked, in the period actually worked. Escalate any pressure — direct or implied — to mischarge labor, shift costs between contracts, or backdate cost or pricing data. Detailed timekeeping, cost-allocation, indirect-rate, and Defense Contract Audit Agency (DCAA) business systems requirements are addressed in the Time Charging Policy ***(Resource 5k)***.

### Preparing Proposals and Negotiating Contracts

Employees involved in the preparation or submission of proposals must ensure that all proposals are in compliance with applicable cost accounting standards and cost principles. Only reasonable, allocable and allowable costs may be charged to negotiated contracts or included in pricing proposals (i.e., forward pricing rate agreements, final overhead submissions, progress payment requests, etc.).

### Preparing Proposals and Negotiating Contracts — Cost and Pricing Data

Employees involved in the negotiation of contracts or subcontracts must ensure that all cost and pricing data are disclosed as of the date of agreement or "handshake" on price, and all data are current, accurate and complete as required by law. Where a regulation or solicitation provision is reasonably ambiguous, employees should document in writing the Company's interpretation and the basis for it.

Confirm the applicable CAS and TINA thresholds with Contracts at the start of any negotiated procurement.

### Preparing Proposals and Negotiating Contracts — Pre-Award Compliance

In addition, employees involved in the preparation or submission of proposals must ensure that all contractual, regulatory, and statutory requirements are complied with, or will be complied with, before contract award.

For DoD acquisitions subject to the Cybersecurity Maturity Model Certification (CMMC) Program, proposal teams confirm that the Company holds the required CMMC certification level prior to award; substantive cybersecurity requirements are addressed in the Information Security & Cybersecurity Policy ***(Resource 5p)***. Do not submit a proposal that requires a CMMC level Company does not currently hold or have a credible plan to hold by the required milestone.

## CERTIFICATIONS AND REPRESENTATIONS

Every certification and representation we make to the federal government — in System for Award Management (SAM) registrations, in proposals, on invoices, in compliance attestations, in subcontract flow-downs — is a statement Company stands behind.

***Make sure you:***

- *Read every certification and representation before signing. If you do not understand what is being certified, do not sign — escalate to Contracts or Legal.*
- *Confirm the underlying facts are current as of the date of the certification, not as of the last time someone checked.*
- *Document the basis for any certification that depends on a judgment call — what facts supported it, who reviewed them, and what Company believed at the time. Contemporaneous records are a best practice.*
- *Re-confirm continuing representations (those that must remain accurate throughout performance) on a defined cadence — not only at award.*

## DEI-Related Contract Compliance

Company is committed to equal employment opportunity, nondiscrimination, and lawful administration of all workplace programs, including recruiting, hiring, promotion, compensation, training, mentoring, leadership development, educational opportunities, employee-resource initiatives, contracting, and allocation of Company resources. These programs must be designed and carried out in a manner consistent with applicable anti-discrimination laws and any federal contract requirements.

Employees must not make, approve, or support any government certification, representation, proposal statement, subcontract flowdown, or contract response about these matters unless it is accurate, complete, and supported by appropriate review. Any questions or concerns about potentially discriminatory program criteria, DEI-related contract requirements, subcontractor obligations, government requests for related records or information, or the accuracy of a related government representation must be raised promptly to Legal, Compliance, Human Resources, or Contracts.

## Domestic Content and Supply Chain Representations

Company must comply with domestic-content, country-of-origin, and supply-chain restrictions that apply to its federal contracts, including requirements under the Buy American Act, Trade Agreements Act, Berry Amendment, specialty-metals rules, Section 889 telecommunications restrictions, and similar contract-specific sourcing obligations. These requirements may affect what products, components, materials, equipment, services, suppliers, and subcontractors Company may use in contract performance.

Anyone certifying domestic content — whether in a SAM representation, a proposal, or an invoice — must verify the actual content as of the certification date, document the calculation, and update the calculation when the threshold steps up. Employees must not make or support any representation, certification, proposal statement, invoice, or contract response about domestic content, country of origin, supplier eligibility, telecommunications equipment or services, or other supply-chain matters unless it has been appropriately reviewed and supported by current documentation. Supply-chain representations must be checked when made and revisited when there is a change in law, contract terms, suppliers, products, components, equipment, services, or subcontractors. Questions must be raised promptly to Contracts, Legal, Compliance, Supply Chain, or Information Security, as appropriate.

## Dealings with Subcontractors

Where Company is a prime contractor on a U.S. Government contract, Company must ensure that all subcontracts are awarded to qualified subcontractors in accordance with both the terms of the prime contract and Company's purchasing system. In addition, Company must incorporate applicable U.S. Government flow-down provisions into all such subcontracts.

Anyone awarding a federal subcontract on behalf of Company must:

- Confirm the subcontractor is not debarred, suspended, or otherwise excluded (SAM Exclusions check).
- Verify all required FAR/DFARS clauses are flowed down at the appropriate tier.
- Document the subcontractor's representations and certifications and refresh them on the cadence required by the prime contract.
- Treat any subcontractor noncompliance as a Company compliance issue.

## Design, Manufacture and Testing Of Products

Under no circumstances may any Company employee deviate from the requirements of a U.S. Government contract without customer authorization from the appropriate contracting officer.

Customer engineers, end users, and program offices cannot waive contract requirements — only the contracting officer can. Surface delivery, schedule, or technical problems through Program Management and Contracts so they can be addressed openly with the customer.

## Design, Manufacture and Testing of Products — Tests and Certifications

All tests required to be performed under a contract must be performed accurately and completely and must be accompanied by all required certifications. Treat product substitutions, counterfeit parts, and undisclosed deviations as serious compliance events.

Falsification of inspection or test results or failure to accomplish required inspections or tests is strictly forbidden.

## Entertainment, Gifts and Gratuities

Strict rules apply to the offering and acceptance of entertainment, gifts, gratuities and other business courtesies by government employees, prime contractors and subcontractors. All Company employees must seek guidance from the Legal Department prior to offering or accepting any gift, regardless of value, to or from a U.S. Government employee, or a prime contractor or subcontractor under a contract in which Company is itself a prime contractor or subcontractor.

Specific guidance regarding foreign officials, anti-bribery, and the FCPA are addressed in the Anti-Corruption & Business Courtesies Policy ***(Resource 5f)***.

## Prohibition on Kickbacks

Company employees are prohibited from providing, attempting or offering to provide, and soliciting, accepting or attempting to accept, any kickback.

## Procurement Integrity and Receipt and Use of Competitive Information

All Company employees who work with any aspect of U.S. Government contracting are expected to be knowledgeable about the specific laws and regulations governing federal procurements. All personnel must also comply with the laws that protect third-party confidential or proprietary information.

Notably, the Procurement Integrity Act prohibits Company personnel from knowingly obtaining, disclosing, or using contractor bid or proposal information or source selection information before contract award, except as authorized by law. Do not solicit or accept any non-public procurement information from a federal official, a competitor, or a former federal official.

## Procurement Integrity — Inadvertent Receipt of Third-Party Info

Company personnel receiving third-party proprietary/confidential information that is not pursuant to a confidentiality, non-disclosure or similar agreement must discontinue reading such information as soon as it becomes apparent to the recipient that he or she is not the intended recipient or is not authorized to have such information. In such a case, the recipient must immediately contact the Legal Department. Such a recipient must not forward such information because forwarding such information to anyone other than a Legal Department representative may result in

compounding the "information contamination," if it is determined that the company is not properly in receipt of such information. If the information is in email form, the recipient must not delete the email from their computer until advised to do so by the Legal Department.

In short: if you receive what looks like another contractor's proposal, source selection material, or any document marked or evidently treated as confidential — stop reading, do not forward it, do not delete it, and contact the Legal Department immediately.

## Procurement Integrity — Former Competitor Employees

Company employees must not ask former employees of competitors to provide any confidential or proprietary information. This includes any request for oral or written information. Former or current Company employees are obligated to continue to protect the confidential information of their former and current employer, respectively. Company policy prohibits requesting third-party confidential information from current employees of a competitor without an executed confidentiality, non-disclosure or similar written agreement executed by authorized representatives of Company and the competitor/supplier company.

Additionally, to avoid the appearance of a conflict of interest, legal approval is required prior to appointing a former employee of a competitor to a company proposal team for a competition that is the same, or similar to, one the employee worked on as an employee of a competitor. It is imperative that Company personnel avoid the appearance of impropriety.

Do not ask former employees of competitors for any non-public information about pricing, strategy, customer relationships, or proposals — including in interviews. Former employees likely remain bound by the confidentiality obligations they owe their prior employer. Before placing a former employee of a competitor on a proposal team for a procurement that is the same as or substantially similar to one they worked on, get written approval from Legal; even where it is permitted, build a documented information barrier. Comply with post-employment restrictions and "cooling-off" rules before discussing employment with any current federal official involved in a Company contract or competition.

## Economic Espionage Act

The Economic Espionage Act is a criminal statute prohibiting theft of trade secrets. Any Company employee who is provided with information they believe may have been taken in violation of the Economic Espionage Act must not read any such information. As soon as such person suspects that they are not authorized to have such information, they must immediately contact the Legal Department for further instruction. Recipients must not forward or share such information with any person other than a member of the Legal Department.

## Reporting of Violations

All employees are responsible for reporting suspected violations of company policy, law or regulations to their supervisor, to a member of the Legal Department, to the Company's Ethics and Compliance Officer, or to the Company Hotline. Reports may be made anonymously where permitted by local law and are managed under the Case Management & Investigations Policy (***Resource 5c***; see also the Non-Retaliation & Whistleblower Protection Policy ***(Resource 5d)***).

## ROLES AND RESPONSIBILITIES

Every employee touching federal work — knows which rules apply to their role, asks before acting when something is unclear, and escalates problems early.

- **Contracts** — owns certifications and representations, flow-down, and the contract record. Confirms TINA/CAS coverage, Buy American/TAA applicability, Section 889, and CMMC level for each procurement.
- **Program Management** — owns delivery, quality, and contracting-officer-approved deviations. Surfaces performance risk early.
- **Finance** — owns cost accounting, pricing data, indirect rates, and timekeeping integrity, with detail in the Time Charging Policy ***(Resource 5k)***.
- **Information Security** — owns the underlying CMMC posture, SPRS scoring, and incident reporting, with detail in the Information Security & Cybersecurity Policy ***(Resource 5p)***.
- **Legal / Ethics & Compliance** — owns FAR 52.203-13 disclosure decisions, investigation oversight, and authorization to sign certifications. Reviews any gift, hospitality, or post-government-employment situation involving federal officials.
- **Officers and Senior Managers** — set the tone, do not pressure teams to win or deliver in ways that compromise these obligations, and are personally accountable for certifications they sign.

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5J: MANDATORY DISCLOSURES POLICY

## OVERVIEW

This policy is to establish the process by which Company will comply with the Mandatory Disclosure requirements established by the Federal Acquisition Regulation (FAR).

## KEY TERMS

**Principal** — an officer, director, owner, partner, or person having primary management or supervisory responsibility within Company or a covered subcontractor.

**Covered Contract** — a federal prime contract or subcontract where the FAR 52.203-13 disclosure clause has been included or flowed down. The clause is included in solicitations and contracts above the simplified acquisition threshold and lasting more than 120 days; the specific dollar threshold is confirmed by Contracts and may change from time to time.

**Disclosable Conduct** —federal criminal violations of Title 18 of the U.S. Code involving fraud, conflict of interest, bribery, or gratuity offenses, in connection with a federal contract or subcontract; civil False Claims Act violations in connection with a federal contract or subcontract; and significant overpayments on a federal contract (other than overpayments resulting from contract financing payments).

**Credible Evidence** — for purposes of this policy, credible evidence means facts that, after a reasonable internal review, support a good-faith belief by Company that disclosable conduct may have occurred. The "timely" disclosure clock runs from the point credible evidence is identified by Legal, not from the first rumor or anonymous tip.

**Voluntary Self-Disclosure (DOJ VSD / CEP)** — the Department of Justice Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy. Under the May 2025 update, a disclosure required by FAR 52.203-13 may still qualify as voluntary for DOJ enforcement-credit purposes if it is made promptly and is accompanied by full cooperation and timely remediation. That determination is made by Legal in coordination with outside counsel, not by the FAR disclosure team.

## POLICY

All employees, consultants and agents are expected to conduct all company business in full compliance with the Code of Conduct.

All Company principals shall be trained with respect to this policy and compliance with the FAR Mandatory Disclosure Requirements.

Upon becoming aware of a possible disclosable violation, Company Principals are responsible for:

- Conducting an investigation to determine whether credible evidence of a violation exists
- Making a recommendation to the Legal Department as to whether the possible disclosable violation should or should not be disclosed consistent with the FAR and this policy

## Internal Reporting and Investigation

Anyone — employee, principal, or subcontractor — who becomes aware of facts that may amount to disclosable conduct is expected to report immediately through any of the channels in the Code of Conduct: a supervisor, the Ethics Office, the Helpline (888.888.8888), the Legal Department, or a member of senior leadership. Reporting in good faith is protected by the Non-Retaliation Policy.

The Legal Department, in coordination with the Ethics Office and the relevant program owner, conducts an investigation under the Case Management & Investigations Policy ***(Resource 5c)*** to determine whether the evidence is credible. Investigations are conducted under privilege where appropriate, and on a fact pattern that allows the Company to make — and document — its disclosure decision.

## Mandatory Disclosure

The Legal Department is responsible for determining whether a matter must be disclosed under FAR 52.203-13 or any other applicable law, regulation, contract clause, or company requirement. Employees, managers, and business leaders must promptly report potential issues internally and must not decide on their own whether external disclosure is required.

When evaluating a potential disclosure, Legal will consider whether the matter should also be reported under any applicable voluntary self-disclosure program. That evaluation may include the promptness and completeness of the disclosure, whether any preexisting disclosure obligation exists or has already occurred, the Company's cooperation with the government, and whether appropriate remedial action has been taken.

Where a disclosure decision involves an ambiguous legal, regulatory, or contractual requirement, the Company will document its good-faith interpretation of the requirement, the facts known at the time, and the basis for the decision. This documentation should be maintained as part of the investigation or disclosure file.

Before any disclosure is made under this policy, it shall first be marked or identified as Company Proprietary Information.

## Cooperation

Once a disclosure is made, the Company cooperates with any agency review or investigation that follows, in coordination with Legal. Cooperation includes timely production of non-privileged documents, identification of witnesses, and preservation of records under the Records Retention Policy ***(Resource 5l)*** and the Information Security & Cybersecurity Policy ***(Resource 5p)***. Document preservation begins at the point an investigation is opened, not at the point a disclosure is made.

Privileged or work-product communications are handled by Legal. Employees should not forward, summarize, or excerpt privileged material outside the investigation team without Legal's authorization.

## Subcontract Flow Down Requirements

All subcontracts that fall under a covered contract shall include language that requires subcontractors to comply with the FAR mandatory disclosure requirements.

## TRAINING

All Company principals receive training on this policy at hire and at least annually. Personnel in roles with elevated exposure — Contracts, Program Management, Finance, Legal, Ethics & Compliance, Internal Audit, and senior management of any covered business unit — receive role-based training that includes the timing, content, and audience of FAR 52.203-13 disclosures, and the interaction with DOJ voluntary self-disclosure.

## GOVERNANCE

The General Counsel (or designee) owns this policy. The Ethics Office maintains the matter file and the disclosure record. Internal Audit periodically reviews the disclosure-decision record to confirm that potential disclosable matters identified through internal channels were evaluated, documented, and either disclosed or closed with the reasoning preserved in the file. The policy is reviewed at least annually and after any material change in the FAR, the DOJ Corporate Enforcement Policy, or relevant case law.

**CROSS-REFERENCES**

*the Code of Conduct (Resource 5a) — reporting channels and the standard for surfacing concerns;*

*the Ethics & Compliance Program Policy (Resource 5b) — program ownership, oversight, and internal controls;*

*the Case Management & Investigations Policy (Resource 5c) — how Company investigates a matter to credible-evidence findings;*

*the Government Contracting Integrity Policy (Resource 5i) — certifications, representations, and underlying federal contracting obligations;*

*the Records Retention Policy (Resource 5l) — preservation of records relevant to a disclosure or investigation;*

*the Information Security & Cybersecurity Policy (Resource 5p) — preservation of electronic records and incident-related data; and*

*the Non-Retaliation Policy (Resource 5d)— protection of any person reporting a concern in good faith.*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5K: TIME CHARGING POLICY

## OVERVIEW

The purpose of this policy is to provide timekeeping guidance within Company to ensure accurate time recording of all Company personnel, directly and indirectly supporting Company contracts. Specifically, this policy establishes guidelines and procedures for preparing, submitting and correcting time within the timekeeping system. This policy applies to every employee, officer, director, and contingent worker who records time at Company, and to every supervisor who approves time records, regardless of work location (on-site, remote, hybrid, customer site, or travel).

## KEY TERMS

**Direct Cost** — Any cost that can be identified specifically with a particular final cost objective.

**Indirect Cost** — Any cost not directly identified with a single, final cost objective, but identified with two or more final cost objectives or an intermediate cost objective.

## POLICY

Federal regulations and contractual obligations require accurate reporting of labor hours for recording contract labor costs and creating payroll expense. Company policy is to maintain a reliable and accurate timekeeping system that accurately records labor for all clients and complies with U.S. government timekeeping requirements. All employees are expected to be familiar with the Company timekeeping procedures and to be prepared at any time to demonstrate compliance during internal and government audits.

Company employees incurring both direct labor hours and indirect labor hours, shall be required to timely and accurately:

- Charge time to appropriate job codes,
- Charge time based on activities performed,
- Complete time report daily; do not back-fill or batch-enter,
- Account for all time worked,
- Ensure unallowable or non-billable labor costs are properly flagged and segregated,
- Ensure that audit trails exist for any material changes to their labor or timekeeping report,
- Authenticate any change to labor or timekeeping report at the end of each reporting period,

If acting as a supervisor, perform reasonable inquiry of the labor and timekeeping reports provided by subordinate personnel prior to approving the completeness and accuracy of such documentation at the end of each reporting period.

### Cost Accounting Standards

Where Company performs work subject to the Cost Accounting Standards (CAS), additional disclosure, consistency, and allocation requirements apply. CAS applicability — full coverage, modified coverage, or exemption — is determined by Contracts at the time of award. If you are unsure whether the contract you charge to is subject to CAS, or to any other heightened cost-accounting requirement, ask Contracts or Finance before submitting your timecard.

### Business Systems Compliance

Company complies with applicable laws, regulations, and contract requirements governing federal contractor business systems and timekeeping, including DFARS 252.242-7005, Contractor Business Systems, which applies to contracts containing one or more of the six covered business-system clauses: accounting; earned value management; estimating; material management and accounting; property management; and purchasing. If you charge time on a contract subject to these requirements, follow the procedures Finance prescribes for the contract, correct any timekeeping errors through the corrections process, and raise any concerns about timekeeping system gaps or controls to your supervisor, Contracts, or Finance. Specific clause applicability and any procedures Personnel must follow are determined by Contracts and Finance on a contract-by-contract basis.

To ensure compliance with this policy, Company management will periodically test compliance with this policy by performing, among other methods, random desk audits. Personnel cooperate with such audits and preserve relevant records in accordance with applicable laws, regulations, and Company policies.

## TRAINING

All Company personnel who record or approve time receive timekeeping training at hire and at least annually thereafter. Personnel charging to contracts subject to DFARS Business Systems clauses, CAS, or other heightened timekeeping requirements receive role-based refresher training. Finance maintains training records.

**CROSS-REFERENCES**

*the Code of Conduct (Resource 5a) — honesty and transparency in business records, reporting channels;*

*the Non-Retaliation & Whistleblower Protection Policy (Resource 5d) — protection of any person reporting a concern;*

*the Government Contracting Integrity Policy (Resource 5i) — recording, allocating, and charging costs on federal contracts;*

*the Mandatory Disclosures Policy (Resource 5j) — disclosure of credible evidence of mischarging that may amount to fraud or False Claims Act exposure;*

*the Records Retention Policy (Resource 5l) — preservation of timekeeping records, including legal-hold preservation; and*

*the Information Security & Cybersecurity Policy (Resource 5p) — preservation and protection of timekeeping system data.*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5L: RECORDS RETENTION POLICY

## OVERVIEW

The purpose of this policy is to establish U.S.-based retention guidelines for identifying, maintaining, and properly destroying records for operational integrity, historical review, litigation, claims, government inquiries, compliance, tax audits, and other internal requirements. This policy applies to records in any format — paper, email, chat, voice, video, structured data, ephemeral messaging — and regardless of where the record physically resides.

This policy applies to every employee, officer, director, contractor, consultant, intern, and third party who creates, receives, processes, or stores Company records, regardless of location. It covers records held on Company systems, on personal devices used for Company business, in cloud or third-party services, and in physical storage (Company-owned or vendor-managed).

When a customer-owned or government-owned system is used to fulfill a contract, the system's recordkeeping rules are determined by both the contract and the customer. Employees working with such systems must comply with customer requirements as well as this policy.

## KEY TERMS

**Record. Any information** — regardless of format — that documents a Company business activity, decision, transaction, communication, or compliance obligation, and that has value to Company for operational, legal, financial, contractual, audit, or historical reasons.

**Records Retention Schedule** — The written schedule maintained by Company that lists categories of records, the minimum retention period for each category, and the legal, contractual, or business basis for that period.

**Disposition** — The final action taken on a record at the end of its retention period — typically destruction, but in some cases transfer to archival storage or to a customer.

**Legal Hold** — A written directive issued by the Legal Department suspending the normal disposition of identified records when litigation, a government investigation, an audit, or a regulatory inquiry is reasonably anticipated or underway.

**Ephemeral Messaging. Communication tools or modes** — including but not limited to disappearing-message settings on chat platforms, auto-deleting text messages, and consumer messaging apps configured to auto-delete — that delete content automatically after a set period.

**Controlled Unclassified Information (CUI)** — Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that the law, regulations, or government-wide policies require or permit an agency to handle using safeguarding or dissemination controls.

**Cyber Incident Data** — Information generated in connection with a cyber incident reportable under DFARS 252.204-7012 — including affected media, packet captures, system images, log files, and the malware sample, where available.

# GOVERNANCE AND ACCOUNTABILITY

## Records Officer

Company designates a senior employee as the Records Officer, accountable for the design, operation, and continuous improvement of the records retention program. In small organizations, this responsibility may sit with the General Counsel, the Compliance Officer, or another senior official with sufficient authority and resources to perform the role.

## Legal Department

Owns the Records Retention Schedule, periodically reviews it for legal and contractual changes, issues legal holds, and is the point of contact for any question about the appropriateness of destroying or preserving a specific record.

## Information Technology

Configures Company systems so the Records Retention Schedule and any active legal holds can be implemented and enforced — including email retention, backup retention, cloud and SaaS retention settings, ephemeral messaging controls, and audit logging of disposition actions.

## Functions, Departments, and Business Units

Apply the Records Retention Schedule to the records they own, work with IT to ensure systems support the applicable retention periods, and implement legal holds when notified.

## Internal Audit

Tests compliance with this policy on a risk-based cycle, including coverage of the contract types and record categories with the highest retention exposure (CMMC artifacts, cyber incident records, government contract records, employment records).

## Affirming Official, where applicable

Where Company holds or seeks contracts subject to CMMC, the Affirming Official designated under the Information Security & Cybersecurity Policy ***(Resource 5p)*** confirms that records evidencing CMMC compliance are retained for the full required period.

# POLICY

At a minimum, records shall be maintained in accordance with the retention periods set forth in the Records Retention Schedule in Appendix A which are based upon compliance with standard contractual and legal requirements. Under special circumstances or for specific operational requirements, records may be retained beyond these minimum retention times for purposes with the approval of the Legal Department.

Records containing any extraneous and immaterial data (e.g., unnecessary preliminary drafts, rough notes, etc.) shall be purged in a timely fashion and do not need to be retained.

Unless impracticable, records generated or received by multiple areas of the company (i.e. corporate Headquarters, divisions, business units or subsidiaries) should be retained by the area primarily utilizing or making those records available in the ordinary course of business and not retained in duplicate areas (others should destroy the records when they have outlived their usefulness).

Retention periods published in the Records Retention Schedule are established for general categories of records, since similar record types may be identified differently throughout the various areas of the company. Managers should exercise good judgment in determining how long records which cannot be classified to one of the general categories listed in the schedule guideline should be retained. Any questions regarding the retention period for a specific record should be referred to the Legal Department.

For company's Cybersecurity Maturity Model Certification (CMMC) Program, hashed assessment artifacts and other CMMC assessment-related records must be retained for at least six (6) years from the CMMC Status Date. Following any reportable cyber incident under DFARS 252.204-7012, the Company also preserves images of affected information systems and related monitoring or packet-capture data for at least 90 days from submission of the cyber incident report.

## Disposition and Destruction

At the end of the retention period, records must be destroyed or otherwise dispositioned in a manner appropriate to the format and sensitivity — incineration, cross-cut shredding, secure media erasure, or cryptographic deletion for cloud and managed-service data. Destruction of records subject to a legal hold is prohibited.

Functional owners may not unilaterally extend a record's life beyond the Schedule, and may not destroy records before the Schedule period ends, without written approval from the Legal Department.

Each disposition action — particularly for records subject to specific legal or contractual retention floors — must be logged in a manner sufficient to demonstrate compliance to a customer, regulator, or auditor. The level of logging must be proportionate to the sensitivity and regulatory exposure of the record.

Auto-deletion or disappearing-message features on Company-managed messaging systems used for substantive Company business must be disabled, and use of personal messaging accounts or third-party ephemeral-messaging applications for substantive Company business is prohibited.

## Storage, Access, and Security

Records must be stored so they remain readable, retrievable, and protected against unauthorized access, alteration, or loss for the full retention period. Records containing CUI or other sensitive information must be stored and accessed in accordance with the Information Security & Cybersecurity Policy ***(Resource 5p)***. Records containing personal information must additionally be handled under the Data Privacy & Protection Policy ***(Resource 5t)***.

Off-site and third-party storage is permitted where the vendor relationship has been reviewed under Company's vendor due-diligence process and the vendor's controls are commensurate with the sensitivity of the records. Vendors holding CUI must meet the relevant federal cybersecurity contract requirements.

Records placed into storage must be labeled with: (a) the date placed into storage; (b) a description of the contents at the level needed to retrieve them; and (c) the disposition date based on the Schedule. Storage media must not contain classified information unless the storage arrangement is itself accredited under the Industrial Security Program Policy ***(Resource 5o)***.

## State Privacy Conflicts

State privacy laws sometimes give individuals a right to request deletion of their personal information. Where a deletion request collides with a retention obligation under this policy — for example, a federal contract requirement,

a tax requirement, or an active legal hold — Company applies the retention obligation and responds to the requester explaining the basis. The Data Privacy & Protection Policy ***(Resource 5t)*** describes how requests are received, routed, and responded to; this policy controls when the retention duty wins.

## Training and Awareness

All employees receive records retention training at hire and annually. Functional and IT staff with day-to-day responsibility for retention controls receive role-based training appropriate to their function. The Legal Department maintains training content and tracks completion in coordination with HR.

## Records Retention

Company maintains a written Records Retention Schedule (Appendix) that lists, by category, the minimum period for which records must be kept and the legal, contractual, or operational basis for that period. The Schedule is owned by the Legal Department and is reviewed at least annually and on an event-driven basis when contract scope or regulatory requirements change materially.

The Records Retention Schedule is the operational source of truth. Where this policy and the Schedule differ, the Schedule controls — except that Schedule periods may never be shorter than the statutory or contractual floor identified in the next section.

Records may be retained beyond the period in the Schedule where there is a documented operational, legal, or contractual reason. Records may not be destroyed before the period in the Schedule expires.

Records containing extraneous and immaterial data — preliminary drafts, working notes, transitory communications — should not be retained once they have served their purpose, unless they document a substantive decision, are subject to a legal hold, or are required to be retained by the Schedule.

## Statutory and Contractual Floor

The Records Retention Schedule incorporates, at minimum, the floors below. These are illustrative of the categories Company most often encounters; the Schedule itself enumerates the full list and the specific source for each.

- **Government contract records** — Three years from the date of final payment for most contract files, with longer periods for specific categories listed in the FAR. The Schedule reflects the FAR's category-specific periods, which can run four years or longer.
- **CMMC certification artifacts** — Six years for assessment objective evidence, affirmations, and supporting artifacts that demonstrate continuing compliance with the CMMC level applicable to the contract. This is longer than the FAR 4.703 floor and is non-waivable for contracts subject to CMMC.
- **Cyber incident data** — All images of affected systems and any monitoring or packet capture data must be preserved for a minimum of 90 days from the submission of a cyber incident report to allow DoD to request the media. Preservation must continue beyond 90 days where DoD elects to receive the media or where a legal hold applies.
- **Tax records** — Per Internal Revenue Code requirements; the Schedule reflects the periods set by IRS Publications 583 and 552, any state tax authority requirements applicable to Company.
- **Employment records** — Per Title VII, the Americans with Disabilities Act (ADA), the ADEA (Age Discrimination in Employment Act), the FLSA, OFCCP, OSHA, ERISA, and applicable state requirements. Where requirements overlap, the longest applicable period controls.

- **Export and trade compliance records** — Five years from the latest of the date of the relevant transaction, the date the export license expired, or the date the related contract terminated.
- **Environmental, health, and safety records** — Per OSHA, EPA, and applicable state requirements, including OSHA's expanded electronic recordkeeping requirements for establishments with 100 or more employees in designated industries.

Where two requirements apply, the longer period controls. Where Company is a subcontractor and a prime contract or flow-down clause requires a longer period than the Schedule, the prime/flow-down requirement controls.

*APPENDIX: Records Retention Schedule*

*DRAFTING INSTRUCTION — Placeholder — each company's Records Retention Schedule will differ. Replace this block with the company-specific schedule before publication.*

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5M: EXPORT & IMPORT COMPLIANCE POLICY

## OVERVIEW

This policy outlines Company's responsibilities under U.S. and applicable non-U.S. export and import laws when we move goods, software, technology, technical data, or services across borders or share them with non-U.S. persons. It applies to all Company employees, officers, and directors wherever located, and to contractors, consultants, and other third parties who act for or on behalf of Company.

## KEY TERMS

**Foreign Persons** — Individuals who are not U.S. citizens, U.S. permanent residents (i.e., green card holders), protected persons (i.e., refugees or political asylees) or entities not incorporated to do business in the U.S.

**U.S. Persons** — Individuals who are U.S. citizens, U.S. permanent residents, protected persons (i.e., refugees or political asylees) or entities incorporated to do business in the U.S. (including U.S. overseas affiliates).

**Technical Data** — Under the ITAR, information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of Defense Articles. Under the EAR, information necessary for the development, production, or use of a product.

**Defense Article** — A defense article is any item, equipment, component, material, software, technical data, model, mockup, or unfinished product that is controlled under the ITAR because it is listed or designated on the U.S. Munitions List. Basic marketing information and general system descriptions are not defense articles.

**Defense Service** — A defense service is assistance provided to a foreign person, whether in the United States or abroad, involving defense articles or ITAR-controlled technical data. This includes technical support, training, engineering, design, development, manufacturing, testing, repair, maintenance, modification, operation, use, or similar assistance related to defense articles, as well as furnishing controlled technical data or providing military training or advice to foreign persons or forces.

**Broker** — A broker is a person or entity that engages in the business of brokering activities involving defense articles or defense services. This may include U.S. persons wherever located, foreign persons located in the United States, and certain foreign persons outside the United States that are owned or controlled by U.S. persons.

**Brokering Activities** — Brokering activities are actions taken on behalf of another person or entity to facilitate the manufacture, export, permanent import, transfer, reexport, retransfer, purchase, sale, lease, loan, financing, transportation, or insurance of a U.S. or foreign defense article or defense service. This includes soliciting, promoting, negotiating, arranging, contracting for, or otherwise assisting with a covered defense transaction.

# POLICY

Many countries have laws that restrict the export of goods and technology. Items which are for military purposes, or which may be involved in the development or production of products or technology for military purposes, are often a primary focus of such controls.

The U.S. has regulatory controls that restrict the export of certain products, services, technical data and software to other countries and nationals of those countries, as well as the re-export of those items from one non-destination to another. There are also U.S. Trade embargoes against certain countries and individuals and entities associated with those countries, as well as named terrorists and drug traffickers. Company must comply with all applicable U.S. export control laws, as well as applicable laws of other countries.

Before any cross-border transaction or any release of technology to a Foreign Person, determine which export regime applies and obtain the export classification of each item, software, and technology involved. Re-validate classifications periodically because the munitions list can and does change. Engineering, sales, supply chain, and program management coordinate with Trade Compliance / Legal before quoting, accepting an order, or shipping.

## Exports

Company products, software, technical data, and technical assistance may not be shared, shipped, released, or otherwise provided to a foreign person or foreign destination unless the Company has completed the required trade compliance review. This includes transfers outside the United States as well as releases to foreign persons within the United States. Before any export, reexport, transfer, or technical exchange occurs, employees must confirm the applicable export classification, screening requirements, licensing obligations, and availability of any license exception or exemption. Transactions involving sanctioned or highly restricted countries, including Russia and Belarus, require additional review and approval by the Trade Compliance Office before proceeding.

## AUKUS ITAR Exemption

Certain ITAR-controlled exports, reexports, retransfers, temporary imports, defense services, and brokering activities between or among eligible parties in the United States, Australia, and the United Kingdom may qualify for the AUKUS ITAR exemption. Employees may not rely on this exemption without prior Trade Compliance Office approval. Before use, the Trade Compliance Office must confirm that the item, service, destination, end user, end use, recipient status, and any applicable excluded-technology restrictions satisfy the exemption's requirements, and that required records are maintained.

## Imports

All Company imports must comply with applicable customs, trade, ITAR, and other government agency requirements. Employees arranging imports must coordinate with the Trade Compliance Office to confirm the proper classification, valuation, country of origin, marking, documentation, permits, licenses, and customs broker instructions before shipment. The Company remains responsible for exercising reasonable care in import transactions, even when a customs broker or freight forwarder is used.

## Restricted Party Screening

Prior to entering into any commercial agreement which could involve an export, and before actually initiating such export, all parties to the transaction shall be screened against the restricted parties lists maintained by various U.S.

government agencies. Sanctions screening obligations administered by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), including the Specially Designated Nationals and Blocked Persons List and country-based sanctions programs, are addressed in the Sanctions Compliance Policy.

## High-Risk Destinations and End-Uses

Some destinations and end-uses require additional caution and, in many cases, separate licensing or are effectively prohibited:

- **China** — heightened controls apply to advanced computing items, semiconductors, semiconductor manufacturing equipment, and related technology, including controls that reach activities of U.S. Persons regardless of where they occur. Confirm current rules with Trade Compliance / Legal before any transaction touching these items, technologies, or end-users.
- **Russia and Belarus** — near-total U.S. and allied export and re-export prohibitions, with the Foreign Direct Product Rule extending EAR jurisdiction to many foreign-made items derived from U.S. technology, software, or specified production equipment. Sanctions on these jurisdictions are addressed in the Sanctions Compliance Policy.
- **Other high-risk end-uses** — military, military-intelligence, weapons-of-mass-destruction, hypersonics, and similar end-uses trigger separate license requirements that can apply to items that are otherwise uncontrolled.

When in doubt, do not proceed without Trade Compliance / Legal sign-off.

## Marking Technical Documents

All export-controlled Technical Data created by Company should contain one of the following legends based on whether it is controlled by the ITAR or whether it is controlled by the EAR.

## Export Warnings for Commercial Items (EAR Legend)

**EXPORT CONTROL WARNING:** This document contains Technical Data whose export, transfer, disclosure and further publication are restricted by the applicable export laws and regulations of the United States and the Export Administration Regulations. Violations of these laws and regulations are subject to severe civil, criminal and administrative penalties.

## Export Warnings for Defense Articles (ITAR Legend)

EXPORT CONTROL WARNING: This document contains Technical Data whose export, transfer, disclosure and further publication are restricted by the applicable export laws and regulations of the United States of America, including the U.S. Arms Export Control Act and the International Traffic in Arms Regulations. Violations of these laws and regulations are subject to severe civil, criminal and administrative penalties.

When a document contains information subject to both the ITAR and the EAR, the ITAR Legend should be used. In addition to the applicable Export Control Warning, Company personnel shall take steps to ensure that the specific export classification is provided to outside parties who receive Technical Data and/or products from the company.

## Protecting Export-Controlled Information

Apply the appropriate EAR or ITAR legend to controlled technical data. Store and transmit controlled technical data only on Company-approved systems; do not use personal email, personal cloud storage, or unmanaged messaging applications. Foreign travel with laptops, phones, or other devices that hold controlled software or technical data may itself constitute an export — use loaner devices or approved travel kits, and consult Trade Compliance / Legal

before traveling to a sensitive destination. The protection requirements for export-controlled information are detailed in the Information Security & Cybersecurity Policy.

### Record Keeping

Maintain export and import records — license applications and authorizations, classification determinations, screening results, shipping documents, end-use and end-user statements, broker records, and related correspondence — for the periods specified in the Records Retention Policy.

## TRAINING

Anyone whose role involves international shipments, foreign-person interactions, controlled technology or technical data, restricted-party screening, or customs declarations completes export and import compliance training at hire and annually. The Trade Compliance function maintains the training matrix and tracks completion.

## GOVERNANCE

The Trade Compliance function (or the General Counsel where there is no separate Trade Compliance function) is accountable for the operation of this policy, the maintenance of classification and screening tools, the training program, and the management of licenses and authorizations. The function reports to the Chief Ethics & Compliance Officer or equivalent on program activity, screening hits, and disclosures, in line with the Ethics & Compliance Program Policy.

## VIOLATIONS

Violations of this policy may subject Company to fines, potential suspension or debarment from contracting with the U.S. Government, jeopardize export privileges, and subject employees to fines and/or imprisonment as specified in the ITAR and EAR. Each Company employee has a responsibility to promptly report suspected or known violations of this policy.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5N: SANCTIONS COMPLIANCE POLICY

## OVERVIEW

The purpose of this policy is to confirm Company's commitment to comply with United States economic and trade sanctions laws, including those administered by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) under the International Emergency Economic Powers Act (IEEPA) and other authorities.

This policy applies to all Company employees, officers, directors, contractors, and Company-controlled entities, in all locations.

## KEY TERMS

**OFAC** — The U.S. Department of the Treasury Office of Foreign Assets Control, the principal U.S. government agency that administers and enforces economic and trade sanctions.

**Sanctioned Party** — Any individual, entity, vessel, aircraft, or other party listed on the OFAC Specially Designated Nationals and Blocked Persons List, any other applicable sanctions list, or any entity owned 50% or more, directly or indirectly and in the aggregate, by one or more sanctioned parties.

**Comprehensively Sanctioned Jurisdiction** — Any country, region, or territory subject to comprehensive U.S. sanctions, as identified and updated by OFAC. The Trade Compliance Office maintains or identifies the current applicable list.

## POLICY

Company prohibits any transaction, payment, dealing, or relationship that would violate U.S. economic or trade sanctions, including any direct or indirect transaction with a Sanctioned Party or any unauthorized transaction involving a Comprehensively Sanctioned Jurisdiction. This prohibition applies regardless of whether the transaction is conducted by a U.S. person or by a non-U.S. person where U.S. jurisdiction otherwise exists (for example, U.S.-origin goods, technology, or services; transactions in U.S. dollars; or transactions involving the U.S. financial system).

Transactions involving Russia, Belarus, or Russian or Belarusian counterparties present heightened sanctions and export-control risk and require Trade Compliance Office review before proceeding.

### Restricted Party Screening

Before entering into any new commercial relationship — including with customers, suppliers, distributors, agents, joint-venture partners, and significant counterparties — and at appropriate intervals during the relationship, Company screens the proposed counterparty (and its principal owners) against the OFAC SDN List and other applicable U.S., E.U., U.K., and U.N. sanctions lists. Apparent matches are escalated to the Trade Compliance Office for resolution.

### Authorizations

Where a transaction would otherwise be prohibited but a general or specific OFAC license, exemption, or authorization is potentially available, the transaction must be reviewed and approved in writing by the Trade Compliance Office or Legal before proceeding.

## Reporting and Self-Disclosure

Apparent violations are reported promptly to the Trade Compliance Office for assessment and, where required, voluntary self-disclosure to OFAC.

## Recordkeeping

Records of sanctions screening, license determinations, and transactions involving sanctioned counterparties or jurisdictions are maintained in accordance with the Records Retention Policy and applicable OFAC recordkeeping requirements (currently 10 years).

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 50: INDUSTRIAL SECURITY PROGRAM POLICY

## OVERVIEW

This policy establishes the framework for Company's Industrial Security Program. We protect classified information at every stage — from contract award through closeout — and we treat the obligations of cleared personnel as personal obligations that travel with the individual.

It applies to every Company location, business unit, and employee that holds, accesses, or is eligible to access classified information under a U.S. Government contract, agreement, or sponsorship. It also covers contractors, consultants, and other third parties acting on Company's behalf where they perform on a classified contract or interact with cleared facilities or systems. This policy also applies wherever Company performs classified work or holds classified information, including at Company-controlled facilities, customer facilities, and any approved alternate work location. Nothing in this policy supersedes a more specific contractual security requirement, a Cognizant Security Agency direction, a classification guide, or the DD Form 254 for a given contract.

Classified work is governed by a separate body of law from the rest of the toolkit. The principal authority is the National Industrial Security Program ("NISP"), administered for most contractors by the Defense Counterintelligence and Security Agency ("DCSA"). Intelligence Community contracts add Intelligence Community Directives and customer-specific accreditation requirements. Where a contract clause, classification guide, or DD Form 254 imposes a stricter requirement, the stricter requirement controls.

## KEY TERMS

**Classified Information** — Information the U.S. Government has determined must be protected from unauthorized disclosure for national security reasons. Classified information is generally designated as Confidential, Secret, or Top Secret, depending on the level of potential harm from disclosure. Some classified information, such as Special Access Program, Sensitive Compartmented Information, Restricted Data, or Formerly Restricted Data, may be subject to additional access and handling requirements.

**Facility Clearance (FCL)** — A determination by DCSA (or an applicable Cognizant Security Agency) that a contractor facility is eligible to access classified information at a specified level. An FCL is required before a contractor may be awarded a classified contract or have cleared employees access classified information at the facility.

**Personnel Security Clearance (PCL)** — An eligibility determination that an individual may access classified information at a specified level, granted following a personnel security investigation and adjudication. A PCL must be paired with a contractual "need to know" before access is permitted.

**Cognizant Security Agency (CSA)** — The federal agency responsible for administering industrial security on a given contract. For DoD and other-agency contracts the CSA is the Department of Defense, with industrial security administered by DCSA as the Cognizant Security Office; for IC contracts the CSA is the sponsoring IC element.

**SEAD 3** — Security Executive Agent Directive 3, the government-wide policy that establishes reporting obligations for individuals with access to classified information or who hold sensitive positions. For cleared employees, this generally means promptly reporting certain activities or events that could affect continued eligibility, such as foreign travel, certain foreign contacts, security concerns, or other reportable conduct.

## Roles and Accountability

**Senior Management Official (SMO).** The SMO is the most senior officer of the cleared facility, holds a personnel security clearance at the level of the FCL, and is personally accountable for ensuring that Company maintains a security program meeting 32 CFR Part 117, applicable IC directives, and contractual security requirements, with the resources and management attention to operate.

**Facility Security Officer (FSO).** The FSO is a U.S. citizen employee, cleared at the level of the FCL, who runs the day-to-day Industrial Security Program. The FSO completes all DCSA-required FSO training and is the interface with the Cognizant Security Agency on FCL maintenance, personnel security actions, classified visits, self-inspections, and incident reporting.

**Insider Threat Program Senior Official (ITPSO).** The ITPSO is a U.S. citizen employee, designated in writing, who is cleared at the level of the FCL and is a senior official of the company. The ITPSO establishes, oversees, and maintains the Insider Threat Program required by 32 CFR § 117.7. The SMO, FSO, and ITPSO functions may be combined in a small business if the same individual is qualified to perform each, subject to CSA approval.

**Program Managers and Cleared Employees.** Each classified program has a designated program security representative — which may be a collateral duty — who works with the FSO to identify and maintain security requirements across the program lifecycle, including DD Form 254 updates. Cleared employees are personally responsible for protecting classified information they access, completing required training, and complying with the SEAD 3 self-reporting obligations described below.

## Facility Clearance and Foreign Influence

Company maintains its FCL through DCSA (or, for IC contracts, through the sponsoring IC element). FCL records, KMP designations, and changes in ownership, organizational structure, or operating arrangements are reported to DCSA through the National Industrial Security System ("NISS") within the applicable timeframes. The FSO promptly reports any event that may affect the FCL, including changes in Foreign Ownership, Control, or Influence (FOCI). Where FOCI mitigation is required, Company implements and complies with the mitigation instrument (Special Security Agreement, Proxy Agreement, Board Resolution, or other) as approved by DCSA.

*REGULATORY WATCH — DoD has proposed extending FOCI disclosure and mitigation obligations to certain unclassified DoD contracts above an established dollar threshold (DFARS proposed rule, May 2026). If finalized, those requirements would operate alongside the NISPOM FOCI obligations above; the FSO and Contracts function will coordinate Company's response.*

## Personnel Security and SEAD 3 Reporting

Each cleared employee signs an SF Form 312 Classified Information Nondisclosure Agreement before being granted access. Personnel security clearances are submitted, maintained, and adjudicated through the systems of record designated by DCSA (currently the Defense Information System for Security, "DISS"), and Company participates in Continuous Vetting under Trusted Workforce 2.0 in lieu of periodic reinvestigations.

Cleared employees comply with the self-reporting obligations of SEAD 3, including:

- foreign travel and unusual or close-and-continuing foreign contacts;
- arrests, charges, and detentions, regardless of disposition;
- unofficial contact with the media regarding classified work;
- significant changes in personal status (marriage, cohabitation, divorce, change of citizenship of a household member);
- significant adverse financial events, including bankruptcy, garnishment, tax lien, or unexplained affluence;
- any approach, attempt, or actual unauthorized disclosure of classified information; and
- any other matter required to be reported by SEAD 3 or by the cleared employee's contract.

Reports are made promptly to the FSO, who is responsible for entering reportable information into DISS and notifying DCSA or the appropriate IC element under the timelines required by 32 CFR Part 117 and applicable IC directives. Cleared employees are also responsible for reporting credible information that may bear on the clearance eligibility of a coworker.

## Physical Security and Information Systems

Closed Areas, Restricted Areas, classified storage containers, and SCIFs are constructed, accredited, and maintained to the applicable requirements. Classified information systems are accredited and operated under the requirements applicable to the contract, and changes affecting accreditation are coordinated with the Information System Security Manager and the Cognizant Security Agency before implementation.

## Insider Threat Program

Company maintains an Insider Threat Program meeting the requirements of 32 CFR § 117.7 and applicable IC directives. The program is led by the ITPSO and integrates Security, Human Resources, the Legal function, Information Security, and program management to identify, assess, escalate, and respond to potential insider threats — including unauthorized disclosure, espionage, and unauthorized transfer of classified information. Reporting under the Insider Threat Program runs in parallel with, and does not displace, the channels available under the Code of Conduct and the Non-Retaliation Policy. Information collected for insider-threat purposes is used only for that purpose and is retained per the Records Retention Policy.

## Security Training

- All employees shall complete Company required general security training.
- Cleared employees shall complete additional Company required training, such as re-indoctrination as well as Government mandated security training on an annual basis.

## Counterintelligence and Suspicious Activity Reporting

Cleared employees report attempted elicitation, suspicious contacts, suspected foreign-intelligence activity, and any indication of espionage, sabotage, or unauthorized disclosure to the FSO immediately. The FSO reports the matter to DCSA (or the applicable IC element) and the Federal Bureau of Investigation in coordination with the Legal function.

## Classified Programs and Contracts

Security is engaged before a classified pursuit begins. The FSO and the assigned program security representative review every RFI, RFP, contract award, contract modification, and DD Form 254 to identify security requirements (classification level, special access requirements, foreign-disclosure restrictions, derivative classification authority, and OPSEC). Classification guides and contract security clauses are applied to all derivative classification decisions, and changes to security clauses or DD Form 254s are tracked and communicated to affected program personnel.

## Security Incidents and Violations

Loss, compromise, or suspected compromise of classified information is reported to the FSO immediately. The FSO conducts a preliminary inquiry, and where required, an administrative inquiry, and reports to DCSA (or the applicable IC element) under the applicable timelines and content requirements. Disciplinary consequences for security infractions and security violations follow Company's graduated disciplinary framework and are coordinated with Human Resources and the Legal function. A security infraction does not involve actual or potential compromise of classified information; a security violation does. Both are documented; the latter is reportable to the Cognizant Security Agency.

*Note : Scaling for Small Businesses. The Scaling for Small Businesses section that follows is included as drafting guidance, not as policy text.*

A small business newly pursuing or holding an FCL should expect that one individual will often hold the SMO, FSO, and ITPSO roles simultaneously, that DCSA training requirements still apply in full, and that the Insider Threat Program scales to the size of the cleared workforce but is not optional. Where Company does not yet have classified information at the facility, the FSO maintains the FCL, ensures KMP clearances remain in scope, and is prepared to stand up safeguards before any classified information is received.

**CROSS-REFERENCES**

***the Code of Conduct (Resource 5a) (general protection of classified information; insider-threat statement of expectations; whistleblower channels);***

***the Information Security and Cybersecurity Policy (Resource 5p) (Federal Contract Information/CUI handling and accreditation of unclassified systems — distinct from accredited classified systems governed here);***

***the Third-Party Due Diligence Policy (Resource 5h) (FOCI screening of suppliers, teaming partners, and beneficial owners);***

***the Export and Import Compliance Policy (Resource 5m) (deemed-export and foreign-national access issues that are separate from classification);***

***the Sanctions Compliance Policy (Resource 5n) (restricted-party screening of cleared-program counterparties);***

***the Non-Retaliation and Whistleblower Protection Policy (Resource 5d) (no employee is retaliated against for SEAD 3, insider-threat, or counterintelligence reporting);***

***the Mandatory Disclosures Policy (Resource 5j) (how security incidents that touch federal contracts feed into the Mandatory Disclosure analysis); and***

***the Records Retention Policy (Resource 5l) (clearance, training, self-inspection, and incident records).***

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5P: INFORMATION SECURITY & CYBERSECURITY POLICY

## PURPOSE & SCOPE

Company is committed to protecting the confidentiality, integrity and availability of corporate, customer and business partner data for which it has stewardship through a comprehensive and systematic Information Security Program. This policy establishes how Company protects the confidentiality, integrity, and availability of company, customer, employee, and government information that we receive, create, process, or store on company systems. It also sets the framework Company uses to meet federal cybersecurity contract requirements — including the Defense Federal Acquisition Regulation Supplement (DFARS) cyber clauses and the Cybersecurity Maturity Model Certification (CMMC) program.

This policy applies to every employee, officer, director, contractor, consultant, intern, and third party who accesses Company information assets, regardless of location. It covers all systems Company owns, leases, or operates; all cloud and managed services Company uses; and all data — wherever stored — that Company creates, receives, processes, or transmits in connection with Company business.

Where a customer-owned, customer-accredited information system is used to perform a contract, that system is governed by the customer's accreditation and the relevant contract; Company personnel using such a system must follow customer requirements in addition to this policy.

This policy covers unclassified information, including Federal Contract Information and Controlled Unclassified Information (CUI). Classified information is governed by the Industrial Security Program Policy ***(Resource 5o)*** and the National Industrial Security Program Operating Manual.

## KEY TERMS

**Information Asset** — A system, network, device, application, or storage medium that creates, processes, transmits, or stores information.

**Federal Contract Information** — Information provided by or generated for the U.S. Government under a federal contract that is not intended for public release.

**Controlled Unclassified Information (CUI)** — Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that the law, regulations, or government-wide policies require or permit an agency to handle using safeguarding or dissemination controls.

### Governance and Accountability

> ***Chief Information Security Officer***
>
> Company designates a Chief Information Security Officer (CISO), or equivalent senior official, accountable for the design, operation, and continuous improvement of the information security program. The CISO reports to the Chief Executive Officer (or equivalent) and has direct, unfiltered access to the Audit Committee of the

Board of Directors. In small organizations where a dedicated CISO is not practical, Company designates a senior official with sufficient authority, independence, and resources to perform this role.

### *Affirming Official*

Where Company holds, or seeks, contracts subject to CMMC, Company designates a senior officer as the Affirming Official. The Affirming Official is responsible for ensuring continuing compliance with the requirements of 32 CFR Part 170 and for executing each annual affirmation in SPRS. The Affirming Official may rely on the CISO and other functional leaders for the underlying assessments and evidence, but the affirmation itself is non-delegable.

### *Resourcing*

Company commits the personnel, budget, training, and tooling sufficient to operate the information security program at a level consistent with Company's risk profile, the sensitivity of the data Company handles, and the obligations of Company's customer contracts. Resourcing is reviewed at least annually.

### *Policy Exceptions*

Technical or business circumstances may require an exception from a specific control in this policy. Each exception must (a) be documented in writing, (b) be supported by a current risk assessment, (c) identify a compensating control where the underlying risk is non-trivial, (d) carry an expiration date, and (e) be approved by the CISO. Exceptions are reviewed at least annually.

### *Policy Review*

This policy is reviewed at least annually and on an event-driven basis when contract scope, regulatory requirements, or threat conditions change materially.

## Risk Management

Systematic assessments of the security risks to information, services and systems must be performed, using a standardized methodology, in response to changes in technologies, the organization and/or the threat environment and to inform decisions that impact the security of Company information assets. For each risk quantified by a risk assessment, a specific risk treatment must be identified and applied. For Department of Defense contracts and subcontracts that involve Federal Contract Information or Controlled Unclassified Information, the Information Security Program also implements (i) the cybersecurity safeguards in DFARS 252.204-7012, including reporting cyber incidents to DoD via the DIBNet portal at https://dibnet.dod.mil within 72 hours of discovery and preserving images of affected systems and related monitoring data for at least 90 days from report submission; (ii) the security requirements of NIST Special Publication 800-171; and (iii) the Cybersecurity Maturity Model Certification (CMMC) Program at 32 C.F.R. Part 170 (effective December 16, 2024), at the certification level required by the contract.

## Asset Management

Protection of Information Assets: Company management will identify and maintain appropriate protections of Information Assets and designate information asset owners who are responsible for ensuring the appropriate information security protections for all information assets.

**Acceptable Use of Information Assets:** Rules for the acceptable use of Company information and assets associated will be identified and documented by Information Security. Employees and Third Parties using Company information assets must acknowledge, in writing, their responsibilities when using those assets.

**Classification, Labeling and Handling of Information Assets:** Company management, information asset owners, information custodians and users will ensure that information assets within their control are classified, labeled and handled in a manner commensurate with their value, legal and US Government requirements, sensitivity, and criticality to the organization and in accordance with documented standards and guidelines.

**Ownership of Information Assets:** Company retains legal ownership of all data, including files and messages, stored or transmitted on its computer and network systems and reserves the right to monitor and/or access this information without prior notice whenever there is a genuine business need.

Asset owners must ensure that information is identified, marked, stored, transmitted, and disposed of in a manner commensurate with its classification.

## CMMC and Federal Contract Cybersecurity Requirements

Where a Company contract includes a cybersecurity clause, Company complies with the requirements of that clause, including any subcontractor flowdown.

### *CMMC Level Determination*

Before bidding on, accepting, or performing a contract that requires CMMC, Company determines the CMMC Level required by that contract — Level 1 (Federal Contract Information), Level 2 (CUI), or Level 3 (highest-sensitivity CUI) — and identifies the systems and personnel within scope. Scoping decisions are documented and approved by the CISO and reviewed when contract scope changes.

### *NIST SP 800-171 Implementation*

For systems handling CUI, Company implements the controls of the version of NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the Contracting Officer. Implementation is documented in a System Security Plan covering each in-scope system.

### *System Security Plan and POA&M*

Company maintains a current System Security Plan for each in-scope system and a Plan of Action and Milestones for any control not yet fully implemented. The CISO reviews the SSP and POA&M at least annually and after any material change.

### *SPRS Score and Annual Affirmation*

For each contract requiring CMMC, the CISO oversees an assessment of the in-scope systems and the submission of the resulting score into the Supplier Performance Risk System. The Affirming Official executes the annual affirmation in SPRS. Records of the assessment, score, and affirmation are retained per the Records Retention Policy.

### *FedRAMP for Cloud Services Handling CUI*

Cloud services that store, process, or transmit CUI must meet the FedRAMP Moderate baseline (or equivalent)

and provide Company with the artifacts needed to support Company's own NIST SP 800-171 implementation. The CISO maintains the inventory of approved cloud services for CUI handling and reviews proposed additions before use.

*Subcontractor and Supply-Chain Requirements*

Company flows applicable cybersecurity clauses down to subcontractors as required, and verifies subcontractor compliance — including SPRS scores and CMMC status — before award and at appropriate intervals during performance. Company does not award subcontracts requiring access to CUI to subcontractors who do not meet the applicable cybersecurity requirements.

## PERSONNEL SECURITY

### Awareness and Training

All personnel with access to Company information assets complete information security awareness training upon onboarding and at least annually thereafter. Personnel with access to CUI complete additional, role-tailored training. Phishing exercises are conducted at least annually and used to refine training. Records of training and exercise results are retained.

### Travel and International Operations

Personnel traveling internationally with Company devices must use travel-equipped or sanitized devices where required by the destination, the data on the device, or applicable export-control law. Travel involving export-controlled technical data or sanctioned destinations is governed by the Export & Import Compliance Policy ***(Resource 5m)*** and the Sanctions Compliance Policy ***(Resource 5n)*** in addition to this policy.

### Role Changes, Transitions, and Terminations

The CISO, Human Resources, and the Industrial Security function (where applicable) coordinate to ensure that access rights are adjusted promptly when personnel change roles, take leaves, or leave Company. Returning equipment, revoking credentials, and preserving records are completed within the timeframes set in the program procedures.

## PHYSICAL AND ENVIRONMENTAL SECURITY

Areas where information assets are sited are protected against unauthorized physical access, theft, fire, water, power loss, and other environmental hazards. Servers, network equipment, backup media, and any media containing CUI are secured in controlled-access spaces. Physical access logs are retained as required by the program procedures and applicable contracts.

### Communications and Operations Management

Standards and Operating Procedures: Company management must assign responsibilities and implement appropriate standards and operating procedures for the management and operation of all information processing facilities.

Standards and operating procedures must be documented, maintained, and made available to all authorized users who need them to perform their job functions. The standards and procedures should define the manner in which the key principles, guidelines and requirements contained in this policy should be implemented.

**Change Control:** Changes to production information processing facilities and systems must be controlled utilizing documentation, planning, scheduling, approval and testing processes.

**Operational Security Controls:** Operational processes must be developed, implemented and maintained to ensure that critical technical and organizational security controls remain effective over time including, but not limited to: access control, account and password management, separation of development, test and operational environments; protection against malicious code, protection/encryption of removable media, network security and clock synchronization, secure use, storage and disposal of equipment and removable media; secure messaging, session timeouts, application security, mobile computing and teleworking, cryptographic controls, web-based security, and **logging, monitoring and fault detection of Company's information assets.**

**Access Control and Identity:** Access to Company information assets is granted on a least-privilege, need-to-know basis and is reviewed periodically. Multifactor authentication is required for remote access, privileged access, and access to systems handling CUI. Privileged accounts are separated from standard user accounts, monitored, and reviewed at least quarterly. Access is removed promptly upon role change, termination, or completion of the contracted engagement.

## Development & Maintenance

Defining Information Security Requirements: All security requirements must be identified at the requirements phase of projects and must be justified, approved and documented as part of the overall business case for an information system.

**Security Controls:** Appropriate security controls must be designed into all systems and applications, to ensure correct information processing and to protect the confidentiality, integrity and availability of the data processed, transmitted and stored by those systems and applications.

**Vulnerability Management:** Technical vulnerability management must be in place in an effective, systematic, repeatable and measurable manner. Timely information about technical vulnerabilities of information systems being used within Company must be obtained, the Company exposure to such vulnerabilities must be evaluated and appropriate measures must be taken to address the associated identified risk.

## Incident Management

**Reporting Information Security Events and Weaknesses:** Formal event reporting and escalation procedures must be in place for identified information security events and weaknesses associated with information systems.

Company maintains a documented incident response plan that covers detection, containment, eradication, recovery, and post-incident review. The plan designates roles, escalation paths, and external-reporting obligations.

**Incident Response and Handling:** Responsibility and methodologies for incident handling and response must be defined, those with incident handling responsibilities must be adequately trained, and a process to identify and apply lessons learned from security incidents must be implemented.

**72-Hour DIBNet Reporting:** A cyber incident affecting a Covered Contractor Information System or covered defense information is reported to the Department of Defense Cyber Crime Center (DC3) via DIBNet within 72 hours of discovery, as required by DFARS 252.204-7012.

*REGULATORY WATCH — Forthcoming CIRCIA Reporting: The Cybersecurity and Infrastructure Security Agency is finalizing rules under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) that, when effective, will require covered entities — expected to include many defense industrial base contractors — to report substantial cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.*

**Other Mandatory and Customer Notifications:** The CISO, in coordination with the Legal function, identifies and executes any other mandatory or contract-specified notifications — including breach notifications to customers, government counterparties, and individuals whose personal information is affected. Cyber incidents involving classified information, CUI, or covered defense information are also reported through the Case Management & Investigations Policy ***(Resource 5c)*** for purposes of internal escalation, mandatory disclosure analysis under FAR 52.203-13, and audit-committee oversight.

### Business Continuity, Backup, And Recovery

Company maintains the backup, recovery, and continuity capabilities needed to restore the confidentiality, integrity, and availability of in-scope information after an incident or disruption. Restoration procedures are tested at least annually. The continuity plan addresses cyber-disruption scenarios in addition to physical-disruption scenarios.

## COMPLIANCE

Company must comply with all statutory, regulatory, and contractual security requirements applicable to the design, operation, use, export, and management of information and information systems as well as the protection of personal information, intellectual property rights and organizational records.

Information Systems Audits: Company must develop processes to ensure that information systems and security controls receive periodic independent reviews and/or when significant changes to security implementations occur. Reviews must be conducted by individuals independent of the area under review (e.g. an internal audit function, an independent manager or a third-party organization specializing in such reviews). Individuals carrying out these reviews should have the appropriate skills and experience to perform effective information security reviews.

### Discipline And Reporting Concerns

Suspected violations of this policy are reported through the channels in the Code of Conduct ***(Resource 5a)***. Confirmed violations are addressed under the Code of Conduct and the Ethics & Compliance Program Policy ***(Resource 5b)***. Cybersecurity incidents involving classified information, CUI, or Covered Defense Information are escalation triggers under the Case Management & Investigations Policy ***(Resource 5c)***.

**CROSS-REFERENCES**

***the Code of Conduct (Resource 5a)***
***the Ethics & Compliance Program Policy (Resource 5b)***
***Case Management & Investigations Policy (Resource 5c)***
***Export & Import Compliance Policy (Resource 5m)***
***Sanctions Compliance Policy (Resource 5n)***
***Industrial Security Program Policy (Resource 5o)***
***Confidential Information Policy (Resource 5q)***
***IT Acceptable Use & Online Conduct Policy (Resource 5r)***
***AI / Responsible Technology Use Policy (Resource 5s)***
***Records Retention Policy (Resource 5l)***

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5Q: CONFIDENTIAL INFORMATION POLICY

## OVERVIEW

Protecting Confidential information is a business, ethical, and legal requirement. Unauthorized disclosure or misuse of Confidential information can result in lost business, lawsuits or even bankruptcy of the business. Consequently, this policy is intended to identify information that is considered Confidential information and provide guidelines and outline employee responsibilities for the protection and use of Confidential information.

This policy applies to all directors, officers, employees, contractors, consultants, and other personnel who handle Company Confidential Information or third-party confidential information Company is obligated to protect, regardless of work location, device, or stage of employment, including, to the extent permitted by law, after employment ends.

## KEY TERMS

**Confidential Information** – Non-public information that employees have access to in the course of their work and that Company is obligated, by law, by contract, or by reasonable business judgment, to protect from unauthorized disclosure or use. Categories include:

- Business and customer information, including contracts, account details, pricing, proposals, and plans for new products or services.
- Financial, strategic, and operational information, including budgets, forecasts, M&A activity, market research, and procurement strategy.
- Technical information, including specifications, designs, source code, technical data, and know-how.
- Personnel records and HR data about other employees (such as performance evaluations, discipline, medical records, background-check results, and other employee data) — additional rules in the Data Privacy & Protection Policy.
- Information about investigations, audits, litigation, or administrative inquiries, whether internal or external.
- Information labeled by Company, by a customer, or by a government as Company Proprietary, Customer Confidential, Sensitive, Restricted, Controlled Unclassified Information (CUI), or Classified.
- Third-party confidential information that Company holds under a non-disclosure agreement, contract, or fiduciary duty.

**Trade Secret** — A subset of Confidential Information that derives independent economic value from not being generally known and that Company takes reasonable measures to keep secret, as defined by the Defend Trade Secrets Act and applicable state law.

**Misuse** — Any access, use, disclosure, transmission, copying, alteration, deletion, or disposal of Confidential Information that is inconsistent with this policy, the Code of Conduct, or the terms under which Company received the information. Misuse can be intentional or the result of negligence or inadvertence.

## Handling and Protection

You must:

- Access and use Confidential Information only when you have a legitimate business need and the appropriate authorization, and only for the purpose for which you were given access.
- Disclose it only to people, inside or outside Company, who are authorized to receive it and have a need to know.
- Take reasonable measures to safeguard trade secrets and keep them secret, as the primary legal mechanism for maintaining trade secret protection.
- Apply the handling controls — encryption, access restrictions, secure storage, and approved disposal — required by the Information Security & Cybersecurity Policy, and mark or label material so others know how it must be handled.
- Discuss Confidential Information only where unauthorized people cannot overhear, including on calls, in airports, and in shared workspaces.
- Not share login credentials or access codes with anyone, and not access information that is not relevant to your assigned work.
- Not alter, destroy, or fabricate information without authorization, or take any action that would obstruct an audit, investigation, or legal hold (see the Records Retention Policy).
- Not use Confidential Information for personal benefit, for the benefit of a competitor, or for any other unauthorized purpose.

## Receiving Third-Party Confidential Information

We are also responsible for the confidential information that customers, suppliers, business partners, and former employers of our personnel entrust to us. You must:

- Accept third-party confidential information only under a written confidentiality, non-disclosure, or other appropriate agreement reviewed by Legal or Contracts, or under an existing customer, supplier, or government contract that addresses the information.
- Use it only for the purpose for which it was provided, and apply at least the same protections you would apply to Company Confidential Information.
- Not solicit, accept, or use confidential information that an individual is not authorized to share, including the confidential information of any current or former employer of a Company employee, contractor, or consultant.

If you receive third-party confidential information you were not authorized to receive (for example, a misdirected document or email), stop reading and notify Legal immediately.

## Defend Trade Secrets Act — Whistleblower Immunity Notice

Nothing in this Policy, any Company agreement, or any Company instruction limits an individual's rights under the Defend Trade Secrets Act, other applicable whistleblower protections, or concerted activity protected by the National Labor Relations Act. Employees, contractors, and consultants may disclose trade secrets or Confidential Information in confidence to a government official or attorney for the purpose of reporting or investigating a suspected violation of law, or in a sealed court or agency filing as permitted by law. Company prohibits retaliation for lawful reporting and will not interpret its confidentiality requirements to restrict protected whistleblower activity. See also the Non-Retaliation & Whistleblower Protection Policy.

## Training and Governance

All employees receive training on this policy at hire and annually thereafter; personnel with access to trade-secret, classified, CUI, or other heightened-protection categories receive additional role-based training. The General Counsel owns this policy. Day-to-day implementation is shared by Human Resources (agreements, departures, training), Information Security (handling controls, access, incident response), and the business owners of each information category. Internal Audit periodically tests compliance on a risk-prioritized basis.

**CROSS-REFERENCES**

*Code of Conduct (Sensitive Information) (Resource 5a)*

*Ethics & Compliance Program Policy (Resource 5b)*

*Case Management & Investigations Policy (Resource 5c)*

*Non-Retaliation & Whistleblower Protection Policy (Resource 5d)*

*Conflicts of Interest Policy (Resource 5e)*

*Information Security & Cybersecurity Policy (Resource 5p)*

*Industrial Security Program Policy (Resource 5o)*

*Insider Information Policy (Resource 5ac)*

*Mandatory Disclosures Policy (Resource 5j)*

*Data Privacy & Protection Policy (Resource 5t)*

*IT Acceptable Use & Online Conduct Policy (Resource 5r)*

*Records Retention Policy (Resource 5l)*

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5R: IT ACCEPTABLE USE & ONLINE CONDUCT POLICY

## OVERVIEW

Company information technology resources are provided for Company business. How employees use those resources — and how they speak online about Company, our customers, and our work — affects information security, customer trust, regulatory compliance, and Company's reputation. This policy sets the rules for using Company IT resources and for online conduct that is connected to Company business.

This policy applies to all Users, on any device used for Company business — Company-issued, personal, or third-party — and on any network, including remote and home offices. It applies whether activity is on duty or off duty if it touches Company IT Resources, Company Information, or Company's name, customers, or work.

## KEY TERMS

**IT Resources** — Company-owned, Company-leased, or Company-managed information technology used to process, transmit, or store Company information. Includes computers, mobile devices, servers, storage, networks, email, collaboration and messaging platforms, cloud services, removable media, software, and the data they handle.

**User** — Any employee, officer, director, contractor, consultant, intern, or third party authorized to access Company IT Resources.

**Generative AI Tool** — A software service that produces text, code, images, audio, video, or other content from a prompt or other input. Includes commercial chatbots, code assistants, image and video generators, and AI features built into other software.

## POLICY

You should have no expectation of privacy when using Company IT Resources. Company may, consistent with applicable law, monitor, access, audit, retrieve, copy, disclose, and delete information stored on or transmitted through Company IT Resources, including email, messaging, internet activity, and files. Personal information processed by Company is also addressed in the Data Privacy & Protection Policy.

***Make sure you:***

- *Use Company IT Resources only for purposes consistent with Company policies and applicable law.*
- *Do not perform any activity that violates law, contract, or policy, including activity that harasses, threatens, defames, or discriminates against others.*
- *Do not attempt to circumvent authentication, security tools, encryption, or monitoring; do not disable, modify, or bypass security, anti-malware, or patching controls.*
- *Do not download, install, or use unauthorized hardware or software, including unauthorized cloud services, browser extensions, or AI tools.*

## User Credentials and Access

You are responsible for activity performed under your credentials. You must:

- Protect your passwords, tokens, and multi-factor authenticators; do not share them with anyone, including IT or your manager.
- Use the credential standards set by IT (length, complexity, multi-factor authentication, rotation) and the password manager Company has approved.
- Lock or sign out of devices when unattended.
- Not use another person's credentials, allow another person to use yours, or access information you are not authorized to access.
- If you have privileged or administrator access, use it only for the work that requires it, and certify U.S. person status when access relates to ITAR-controlled information.

## Devices, Removable Media, and Networks

Company Information and Company IT Resources must be protected wherever they are accessed — in the office, at home, on the road, and on any device or network.

- Company Information must be stored, transmitted, and accessed only through Company-approved devices, systems, cloud services, removable media, and secure network channels.
- Personal devices, personal email, personal storage, and personal cloud accounts may not be used for Company business unless expressly authorized and subject to required Company controls.
- Employees must keep Company-issued devices encrypted, updated, and configured as directed by IT; must not disable security tools or device-management software; and must use approved secure access methods, such as Company VPN, when connecting from home, public, or other untrusted networks.
- Third-party hardware, services, or network connections require IT approval before use. Employees traveling internationally with Company devices must follow applicable Trade Compliance, CUI, export-control, loaner-device, screening, and reporting requirements.
- All Company IT Resources must be returned at the end of employment or engagement and may be disposed of only through IT.

## Internet Use

When using Company IT Resources to access the internet, you must not:

- Visit sites or download content that is unlawful, that is inconsistent with the Code of Conduct (for example, sexually explicit, hateful, or harassing material), or that could expose Company systems to malware.
- Use Company IT Resources for gambling, unauthorized peer-to-peer file sharing, or any activity that infringes another person's intellectual property.
- Engage in lobbying, political fundraising, or campaign activity using Company IT Resources except as expressly approved by the Legal Department or Government Relations (see the Government Relations Policy).

## Use of Generative AI Tools

Use only AI tools — including generative AI services and AI features embedded in other software — that Company has approved for the type of work and the type of information involved. The Company AI program, including the approved-tools list, governance, and risk classification, is set by the AI / Responsible Technology Use Policy.

## Email, Messaging, and Collaboration Tools

Treat email and messages on Company systems as Company business records. They may be subject to legal hold, discovery, audit, and customer or government request. You must:

- Use Company-approved email, collaboration, and messaging tools for substantive Company business; do not use personal email or personal messaging accounts for Company business.
- Keep auto-delete and disappearing-message features turned off on Company-managed channels used for Company business, and not use consumer ephemeral-messaging applications for substantive Company business (see the Records Retention Policy and the Confidential Information Policy).
- Communicate with the same care you would use in a written memo: no language that is threatening, defamatory, obscene, harassing, discriminatory, or otherwise inconsistent with the Code of Conduct.
- Not auto-forward Company email to personal accounts or to non-Company systems.
- Not send chain mail, mass solicitations, marketing, or political fundraising from Company accounts; do not use Company accounts to register for unrelated personal services.

## Online Conduct and Social Media

Social media — including blogs, forums, video and image platforms, professional networks, and any other public online channel — is part of how our work is seen. When you participate online in a way that connects to Company, our customers, or our work, the rules below apply, on Company systems and on personal accounts.

***Make sure you:***

- *Do not represent yourself as speaking for Company unless you are authorized to do so; if you identify yourself as a Company employee, make clear that your views are your own.*
- *Do not post Company Confidential Information, customer information, export-controlled or classified information, Controlled Unclassified Information, personal information about co-workers, or trade secrets (see the Confidential Information Policy and the Data Privacy & Protection Policy).*
- *Do not post AI-generated images, audio, or video that could reasonably be mistaken for genuine content involving Company, our customers, our employees, or our products.*
- *Do not post material that is unlawful, harassing, threatening, or that targets a co-worker, customer, supplier, or competitor in a way that violates the Code of Conduct.*
- *Refer media inquiries, customer-facing statements, and any request for an official Company position to the Communications Department; do not use Company channels to make official statements unless authorized.*
- *If you participate in discussions about Company financial performance, securities, contracts, litigation, or pending bids, follow the Insider Information Policy and the Code of Conduct, and do not disclose material non-public information.*

## Reporting Security Incidents and Violations

Report immediately to your manager, IT, Information Security, or the Helpline at 888.888.8888:

- Lost or stolen Company devices, badges, or credentials.
- Suspected phishing, malware, intrusion, or unauthorized access to Company IT Resources or Company Information.
- Suspected unauthorized disclosure of Company Information online, including on social media or through generative AI tools.
- Any suspected violation of this policy.

Reports may be made anonymously where permitted by law. Company does not tolerate retaliation against anyone who reports in good faith (see the Non-Retaliation & Whistleblower Protection Policy).

## Training and Governance

All Users complete IT acceptable-use and security-awareness training at hire and at least annually thereafter; users with privileged access, social-media or communications duties, generative-AI use cases, or access to classified information or CUI receive additional role-based training. The Chief Information Security Officer owns this policy. IT, Information Security, Human Resources, Legal, Communications, and the Facility Security Officer share day-to-day implementation. The policy is reviewed at least annually and updated as technology, regulatory expectations (including DOJ Evaluation of Corporate Compliance Programs (ECCP) guidance and National Labor Relations Board (NLRB) doctrine), and Company business change.

**CROSS-REFERENCES**

*Code of Conduct (Sensitive Information; Public Communications; Social Media) (Resource 5a)*

*Ethics & Compliance Program Policy (Resource 5b)*

*Case Management & Investigations Policy (Resource 5c)*

*Non-Retaliation & Whistleblower Protection Policy (Resource 5d)*

*Conflicts of Interest Policy (Resource 5e)*

*Anti-Corruption & Business Courtesies Policy (Resource 5f)*

*Mandatory Disclosures Policy (Resource 5j)*

*Records Retention Policy (Resource 5l)*

*Export & Import Compliance Policy (Resource 5m)*

*Sanctions Compliance Policy (Resource 5n)*

*Industrial Security Program Policy (Resource 5o)*

*Information Security & Cybersecurity Policy (Resource 5p)*

*Confidential Information Policy (Resource 5q)*

*Data Privacy & Protection Policy (Resource 5t)*

*AI / Responsible Technology Use Policy (Resource 5s)*

*Insider Information Policy (Resource 5ac)*

*Government Relations Policy (Resource 5ab)*

## VIOLATIONS

Failure to comply with this policy may result in disciplinary action up to and including termination.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5S: AI POLICY

## OVERVIEW

This policy sets Company's expectations for the use, development, and procurement of artificial intelligence (AI). It applies to AI tools Company uses internally, and to AI capabilities Company builds, integrates, or delivers under a customer contract.

The legal and regulatory environment around AI — particularly for federal contractors — is moving quickly. This policy stays at the level of durable principles and core legal obligations. Where a specific executive order, regulation, agency directive, contract clause, or customer requirement is more specific or more restrictive, that requirement controls.

Day-to-day employee use of AI tools is also addressed in the IT Acceptable Use & Online Conduct Policy ***(Resource 5r)***. Information security and incident handling are addressed in the Information Security & Cybersecurity Policy ***(Resource 5p)***.

## KEY TERMS

**Artificial Intelligence (AI)** — Software that uses machine learning, large language models, generative models, or similar techniques to produce predictions, classifications, recommendations, or content based on data. Includes commercial AI products Company uses, and any AI capability Company builds, integrates, or delivers.

**AI Owner** — The individual Company designates as accountable for AI-related risks, controls, and policies at Company. In a smaller organization, the AI Owner may also serve in another existing leadership role (for example, Chief Information Security Officer).

## POLICY

**Accountability.** Company designates an AI Owner accountable for this policy. The AI Owner maintains an up-to-date understanding of where AI is used, developed, or delivered at Company, and ensures the controls in this policy are applied before a significant new AI tool or capability is put into production use.

**Lawful and accountable use.** AI does not change Company's legal, contractual, or ethical obligations. Company and its people remain responsible for the accuracy, lawfulness, and consequences of AI-assisted work — the same as for work done without AI.

**Human oversight.** A person reviews AI output before it is relied on for any decision that has a material effect on an employee, a customer, a supplier, safety, or compliance. Human oversight is meaningful, not a formality: the reviewer has the authority and the information needed to override the AI output. AI output is treated as a draft, a recommendation, or decision-support — not as a final work product — unless a specific tool and use case has been approved for automated operation.

**Approved tools and protected information.** Only Company-approved AI tools may be used for Company business. The following information may not be entered into any AI tool — internal or external — that has not been specifically approved for that information:

- Company Confidential or proprietary information
- Customer or third-party confidential information
- Personal data of identifiable individuals
- Controlled Unclassified Information (CUI), classified information, or export-controlled technical data (see ***Resource 5m***, Export and Import Compliance))
- Source-selection-sensitive information (see FAR Part 3)
- Information subject to attorney-client privilege or otherwise protected from disclosure

If you are uncertain whether a tool is approved for the information you want to use, ask the AI Owner or IT before using it.

**Vendor and third-party AI.** When Company buys AI capabilities from a vendor, uses an AI-enabled software-as-a-service product, or relies on an AI feature embedded in a third-party tool, due diligence appropriate to the risk is performed before the tool is approved. Diligence covers, at minimum: whether the vendor uses Company or customer data to train its models; where data is stored and processed; the vendor's security posture and relevant certifications; and the vendor's contract terms on confidentiality, intellectual property, and termination. Vendor relationships involving AI are also managed under the Third-Party Due Diligence Policy ***(Resource 5h)*** and the Information Security & Cybersecurity Policy ***(Resource 5p)***.

**AI-specific security threats.** AI tools and capabilities Company uses, develops, or delivers are evaluated for AI-specific threats — including prompt injection, training-data poisoning, model extraction, and adversarial manipulation — as part of approval and ongoing oversight. All other cybersecurity requirements are governed by the Information Security & Cybersecurity Policy ***(Resource 5p)***.

**Intellectual property and training data.** AI tools used for Company business are evaluated for what they do with the data Company puts into them. Company does not upload third-party copyrighted material, customer data, or Company trade secrets into any AI tool whose terms permit the provider to use that input to train its models or to make it available to other customers. Where a tool offers a setting that prevents training on Company input, that setting is enabled. Ownership and licensing of AI-generated output are addressed in the underlying tool agreement and, where Company delivers AI-assisted work product to a customer, in the customer contract. AI-generated or AI-assisted code is reviewed for security, licensing, and open-source obligations before it is incorporated into Company products or customer deliverables.

**AI in employment decisions.** AI used to support employment decisions — including recruiting, hiring, promotion, discipline, or performance management — is subject to the Equal Employment Opportunity Policy ***(Resource 5v)*** and any applicable state or local laws governing automated employment decision tools. A material employment decision is not made on the basis of AI output alone.

**Accuracy and disclosure of AI-generated content.** AI-generated content used in Company's external communications, customer deliverables, regulatory filings, or representations to a court is reviewed for accuracy before it leaves Company. Where disclosure of AI use is required by contract, court rule, customer policy, or applicable law, Company makes that disclosure. Company does not use AI to generate content intended to deceive a customer, regulator,

court, or counterparty — apart from approved exercises such as authorized security red-teaming or training, with appropriate controls. Records of AI use in regulated or contractual submissions are retained as required by the Records Retention Policy ***(Resource 5l)***.

**Federal contract and customer requirements.** When Company uses or delivers AI under a federal contract, the customer's authorization, accreditation, security plan, and any contract-specific AI provisions control where they are more specific or more restrictive than this policy. Company complies with applicable executive orders, agency directives, and procurement requirements that govern AI in federal contracts. Any Company work involving autonomous or semi-autonomous weapon systems is, in addition, subject to the customer's required review and approval process and to DoD Directive 3000.09.

**Reporting and incident response.** Suspected violations of this policy, and any AI-related event that contributes to a security incident, a customer-affecting error, or a possible compliance failure, are reported and handled under the Information Security & Cybersecurity Policy ***(Resource 5p)*** and the Case Management & Investigations Policy ***(Resource 5c)***, including any incident reporting required by contract. Anyone raising a good-faith AI concern is protected under the Non-Retaliation & Whistleblower Protection Policy ***(Resource 5d)***.

**CROSS-REFERENCES**

***Code of Conduct (Resource 5a)***

***Ethics & Compliance Program Policy (Resource 5b)***

***Case Management & Investigations Policy (Resource 5c)***

***Non-Retaliation & Whistleblower Protection Policy (Resource 5d)***

***Third-Party Due Diligence Policy (Resource 5h)***

***Records Retention Policy (Resource 5l)***

***Export & Import Compliance Policy (Resource 5m)***

***Information Security & Cybersecurity Policy (Resource 5p)***

***IT Acceptable Use & Online Conduct Policy (Resource 5r)***

***Equal Employment Opportunity Policy (Resource 5v)***

*REGULATORY WATCH — Federal AI requirements are active and shifting. Federal AI obligations for contractors are being set largely through executive orders and agency directives rather than a single comprehensive statute, and they may change. As of June 2026, there is no mandatory federal licensing, preclearance, or permitting requirement to develop, release, or use AI models; current federal efforts emphasize voluntary public-private frameworks for frontier models and AI-enabled cybersecurity. Companies should track the executive orders, agency directives, and contract clauses that govern AI, and comply with any that are more specific or more restrictive than this policy.*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5T: DATA PRIVACY & PROTECTION POLICY

## OVERVIEW

The purpose of this policy is to confirm Company's commitment to handle personal information about identifiable individuals — including employees, applicants, customers, and other third parties — in compliance with applicable U.S. federal and state privacy laws, contractual privacy obligations, and applicable foreign privacy laws to the extent they apply to Company.

This policy applies to all Company employees and to any third party that processes personal information on Company's behalf.

## KEY TERMS

**Personal Information** — Information that identifies, relates to, describes, or could reasonably be linked with a particular individual or household, as more specifically defined under applicable privacy law.

**Sensitive Personal Information** — A subset of Personal Information that, under applicable law, warrants heightened protection — including, depending on jurisdiction, government identifiers, financial account information, precise geolocation, biometric or genetic information, health information, racial or ethnic origin, religious beliefs, sexual orientation, immigration status, and personal information of children.

**Processing** — Any operation performed on Personal Information, including collecting, storing, using, transmitting, disclosing, or destroying.

## POLICY

Company collects, uses, retains, and discloses Personal Information only as necessary to operate its business, perform its contracts, and comply with law. Company does not sell Personal Information.

Company implements administrative, technical, and physical safeguards designed to protect Personal Information from unauthorized access, disclosure, alteration, and destruction, consistent with the safeguards required by the Information Security & Cybersecurity Policy.

Where Company is subject to comprehensive state consumer privacy laws, Company honors applicable individual rights (including the rights to know, delete, correct, and opt out, where applicable) and provides any required notices to the extent practicable.

Where Company is subject to a foreign privacy regime by virtue of its operations or counterparties (including the EU and UK General Data Protection Regulations and similar laws), Company addresses the additional obligations of that regime under the direction of Legal.

Personal Information involved in a security incident is handled in accordance with the Information Security & Cybersecurity Policy and applicable breach-notification laws, including, for incidents involving covered defense information, the 72-hour reporting obligation under DFARS 252.204-7012.

## GOVERNANCE

The General Counsel (or a designated Privacy Officer) owns this policy, with support from Information Security, Human Resources, and Legal. The Privacy Officer maintains a record of Company's processing activities, oversees responses to data-subject requests, reviews vendor and supplier privacy practices, and reports periodically to executive leadership on the privacy program. The policy is reviewed at least annually and updated as applicable laws and business activities change.

## TRAINING

All employees complete privacy awareness training at hire and at least annually. Personnel in roles with regular access to Personal Information — including Human Resources, Information Technology, marketing, customer service, and procurement — receive role-specific training on lawful handling of Personal Information, response procedures for data-subject requests, and escalation requirements for privacy incidents. Training content is reviewed annually and updated to reflect changes in applicable laws and Company's processing activities.

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5U: PROCUREMENT INTEGRITY POLICY

## OVERVIEW

The purpose of this policy is to assure that goods and services are procured efficiently, ethically, and in compliance with applicable law and contract requirements; to promote full and open competition and the use of small businesses where practical; and to safeguard the integrity of Company's procurement system.

This policy applies to all Company employees and to its subsidiaries and affiliates worldwide, and serves as the minimum standard for procurement operations. It applies to every method by which Company commits to acquire goods or services, including consulting and other professional-services arrangements.

## POLICY

This policy is intended to provide consistent methods to achieve objectives, clarify expectations, reinforce values and behaviors, and mitigate risk to Company.

Procurement function is required to take the appropriate steps to meet these requirements and shall ensure that supplier selection procedures fully support this policy.

**A. Value:** Obtain the best value for goods and services purchased while maintaining the highest ethical standards in dealing with suppliers. Value reflects a balance of technical and operational requirements, price, quality, service, delivery, total cost of ownership, and risk — including compliance and supply-chain risk — to provide the best overall benefit to Company.

**B. Compliance:** All procurement transactions must be conducted in compliance with applicable customer requirements, laws and regulations, and Company policies and procedures. Requirements include, but are not limited to:

- Use full and open competition where possible.
- Select small businesses where possible, including Small, Small Disadvantaged, Women-Owned, HUBZone, Veteran-Owned, and Service-Disabled Veteran-Owned businesses, consistent with applicable contract obligations.
- Protect customer and Company intellectual property and confidential information, including in non-contractual or pre-contractual contact with suppliers involving the transfer of proprietary design or process information, ITAR-controlled technical data, or EAR-controlled technology. (See Export & Import Compliance Policy.)
- Flow down required clauses and certifications to suppliers and subcontractors, in accordance with the prime contract and applicable regulations. This includes, where applicable: cybersecurity requirements; prohibitions on covered telecommunications and video-surveillance equipment and services; trade-agreement and domestic-preference clauses; anti-trafficking certifications; and other clauses identified by Contracts or Legal.
- Adhere to Contractor Purchasing System Review (CPSR) requirements as defined in FAR Subpart 44.3 where Company is subject to CPSR.
- Compliance with sanctions, export controls, third-party due diligence, anti-corruption, and forced-labor obligations is governed by the cross-referenced policies listed at the end of this document.

**C. Anti-Collusion:** Procurement personnel must protect the integrity of Company's source-selection and pricing decisions. Bid rigging, price fixing, market or customer allocation, and other collusion among suppliers — or between Company personnel and suppliers — are prohibited and may violate the Sherman Act and parallel state law.

**D. Consultants, Advisors, and Foreign-Influence Risk:** Before engaging consultants, advisors, or other professional-services providers for U.S. Government contract work, employees must coordinate with Contracts and Legal to assess foreign-influence, organizational conflict-of-interest, and procurement-integrity risks. Employees may not engage consultants for work if the consultant has a prohibited relationship with a covered foreign entity. Employees must obtain required representations, certifications, and supporting documentation before making any commitment.

**E. Supplier Qualification and Utilization:** All new suppliers, and existing suppliers where mandated by government or regulatory requirements, must satisfy minimum qualification requirements. Qualification includes risk-based due diligence (see Third-Party Due Diligence Policy), execution of a Non-Disclosure Agreement where appropriate, and acknowledgment of Company's Supplier Code of Conduct or equivalent supplier integrity expectations.

**F. Authority:** The authority to commit Company to legally binding procurement transactions resides solely with procurement personnel acting within their delegated authority, except for Procurement Card transactions, expense reimbursements, emergency orders required for critical operations, and other expressly authorized non-PO transactions.

**G. Methods:** Requests for purchases of goods or services must follow the process appropriate to the type of acquisition, based on spend authority and functional accountability, and must be promptly transacted so that liabilities and expenses are visible to Company. Acceptable methods include purchase orders, change orders, Procurement Cards, Supplier Schedule Order Agreements, Material Requirements Plan releases, Blanket Order Agreements, Blanket Purchase Orders, subcontracts, master service agreements, and consulting agreements.

**H. Contract Development:** For large or complex purchases, or purchases that include nonstandard terms or otherwise expose Company to material risk, procurement personnel will use formal contract agreements. The requestor is responsible for obtaining input from relevant stakeholders, which may include Finance, Tax, Human Resources, Risk Management, Legal, Trade Compliance, IT/Security, and any other function that has an interest in the contractual commitment.

**I. Records Retention:** All procurement-related documents must be retained in accordance with the Records Retention Policy and the applicable records-retention schedule.

## TRAINING

Procurement personnel and other employees who participate in or approve procurement decisions must complete training on this policy at hire and at least annually. Specialized training (e.g., CMMC flowdown, Section 889, anti-corruption, anti-collusion red flags) is provided based on role.

## GOVERNANCE

The Procurement function owns this policy and is responsible for procedures, supplier qualification, and program oversight, working with Contracts, Legal, Trade Compliance, IT/Security, and Internal Audit. Periodic risk-based reviews of supplier files, flowdowns, and authority approvals support compliance with this policy and the Contractor Purchasing System Review framework where applicable.

| CROSS-REFERENCES |
| --- |
| *Code of Conduct (Resource 5a)* |
| *Ethics & Compliance Program Policy (Resource 5b)* |
| *Government Contracting Integrity Policy (Resource 5i)* |
| *Third-Party Due Diligence Policy (Resource 5h)* |
| *Records Retention Policy (Resource 5l)* |
| *Export & Import Compliance Policy (Resource 5m)* |
| *Sanctions Compliance Policy (Resource 5n)* |
| *Information Security & Cybersecurity Policy (Resource 5p)* |
| *Human Trafficking & Forced Labor Prevention Policy (Resource 5aa)* |
| *Non-Retaliation & Whistleblower Protection Policy (Resource 5d)* |

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5V: EQUAL EMPLOYMENT OPPORTUNITY POLICY

## OVERVIEW

Company values its highly talented workforce as a strategic advantage and is committed to providing equal opportunity in employment for all people. This policy applies to all U.S. job applicants and employees of Company.

## POLICY

Company is committed to providing Equal Opportunity in Employment to all applicants and employees regardless of race, color, ethnicity, ancestry, religion, sex (including pregnancy, sexual orientation, and gender identity), national origin, age, physical or mental disability, military/veteran status, marital status, genetic information, or any other characteristic protected by law. This commitment must be followed in all aspects of employment and personnel practices including but not limited to: recruitment, hiring, placement, performance evaluation, upgrading or promotion, demotion, transfer, compensation, benefits, layoff and recall, training and development, social and recreational programs and application of all company policies, procedures, and benefits.

*NOTE: the following paragraph only applies where Company is subject to Section 503 and/or VEVRAA affirmative-action program requirements.*

Where Company is subject to applicable federal contractor affirmative action obligations, it maintains affirmative action programs for individuals with disabilities and protected veterans, as required by U.S. federal law.

Where FAR 52.222-90 applies, Company will not engage in racially discriminatory DEI activities in connection with performance of the covered contract, including disparate treatment based on race or ethnicity in recruitment, employment (including hiring and promotion), contracting (including vendor agreements), program participation, or the allocation or deployment of an entity's resources. The substance of FAR 52.222-90 must be flowed down to covered subcontracts at any tier. Suspected subcontractor conduct that may violate the clause must be escalated promptly to Legal and Contracts for review. Where Company knows, or reasonably should know, of subcontractor conduct that may violate the clause, Company will make any required report to the Contracting Officer and will take appropriate remedial action as directed by the Contracting Officer.

### Responsibilities

All employees, managers, and supervisors are responsible for actively supporting Company's commitment to Equal Employment by performing their duties and conducting their behavior in a non-discriminatory manner. Managers and supervisors are responsible for taking appropriate actions to prevent violations of this policy and to maintain a work environment that is free of unlawful discriminatory activities.

All employees are responsible for reporting any conduct that might constitute discrimination or retaliation to their supervisor, their Human Resources point of contact or ethics and compliance contact.

### Retaliation

Retaliation of any kind against employees for reporting harassment and/or discrimination or assisting in investigating such complaints is prohibited.

## VIOLATIONS

Violations of this policy will not be tolerated. Company will promptly investigate every issue that is brought to its attention in this area and will take appropriate disciplinary action, up to and including termination of employment.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5W: NON-HARASSMENT POLICY

## OVERVIEW

Company is committed to maintaining an environment that is free of all forms of harassment, disruptive behavior and abuse and in which all individuals are treated with dignity and respect. This policy applies to all employees of Company.

## KEY TERMS

**Harassment** — refers to verbal, physical, written or visual conduct or behavior which harasses, disrupts, or interferes with another's work performance, or creates an intimidating, hostile or offensive work environment.

**Sexual Harassment** — refers to unwelcome behavior of a sexual nature when (i) an employment decision affecting the employee is based upon the employee's acceptance or rejection of such conduct, or (ii) such conduct has the purpose or effect of substantially interfering with an individual's work performance such that it creates an intimidating, hostile, or offensive working environment.

## POLICY

This policy promotes a safe, respectful and productive workplace by defining prohibited behavior and responsibilities and establishing processes to prevent, report, investigate and resolve allegations of harassment.

### Non-Harassment

Company does not tolerate any acts of Harassment by or against its employees or Third-Parties. Employees may not engage in or display any form of Harassment. What one person treats as harmless may still be experienced as harassment by another. The test is not how it was meant or how it was received, but whether a reasonable person in the same situation would find the conduct hostile or offensive.

Although it is not possible to list every type of behavior that can be considered Harassment in violation of this policy, Harassment includes, but is not limited to:

- intimidating, threatening or hostile behavior;
- comments, gestures or actions regarding violent events or behavior;
- shoving, punching, groping, tripping, pinching, stalking, pushing, damaging another's personal tools or possessions;
- demeaning or offensive slurs, profanity and foul language;
- displays of demeaning reading materials or pictures, including electronic materials, drawings, or objects;
- inappropriate email communications;
- jokes or negative comments that demean or disparage others;

- spreading malicious rumors or comments;
- acts of vandalism, arson, or sabotage;
- behavior that reflects a lack of respect for an individual's race, color, ethnicity, ancestry, religion, sex (including pregnancy, sexual orientation, and gender identity), national origin, age, physical or mental disability, military/veteran status, marital status, genetic information, or any other characteristic protected by law

## No Sexual Harassment

Sexual harassment violates the law and is expressly prohibited under this policy and Company's Code of Conduct. Company does not tolerate any acts of Sexual Harassment by or against its employees or Third-Parties. Sexual harassment includes conduct by members of the same gender, and is not limited to:

- unwelcome sexual advances or requests for sexual favors;
- promising favorable treatment or threatening unfavorable treatment based on the employee's response to behavior of a sexual nature;
- sending, displaying, forwarding, or posting sexually suggestive pictures, videos, photos, drawings, images, letters, notes, text messages or email;
- making inquiries about an employee's sexual behavior;
- unwelcome touching that makes an employee feel uncomfortable such as massages, hugging, kissing or intentional brushing against another's body;
- repeated requests for dates or contact outside the workplace;
- behavior, remarks, jokes, gestures or innuendos of a sexual nature or that intimidate, ridicule, demean or belittle a person on the basis of their gender (regardless of whether the remarks are sexually provocative or suggestive of sexual acts);
- using sexual behavior to create an intimidating, hostile or offensive working environment.

## Reporting Harassment

Employees and Third Parties are requested to promptly report any witnessed potential Harassment behavior to the attention of management or those referenced in the Code of Conduct in order for Company to take appropriate action.

## Management Responsibilities

It is the responsibility of persons in supervisory or management positions to maintain a workplace free from any form of Harassment including Sexual Harassment and to bring this policy to the attention of all employees, to verify that all employment actions are administered in accordance with this policy, and to bring to the attention of their supervisor or manager, their Human Resources representative, an ethics and compliance representative, or a legal representative any violation of this policy of which they become aware.

## Violations of this Policy

Anyone violating this policy may be removed from the premises and is subject to disciplinary measures, up to and including termination.

Third-Party offenders may suffer the suspension or termination of their business relationship with Company. Violations of this policy may also result in personal legal and/or financial liability.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5X: WORKPLACE VIOLENCE PREVENTION POLICY

## OVERVIEW

Company is committed to providing a safe work environment for all employees and individuals who conduct business with our employees on company property. The purpose of this policy is to define the prohibited conduct by employees and to establish a process for reporting and responding to incidents or threats of violence.

This policy applies to every employee, officer, director, contingent worker, applicant, and intern of Company; to conduct by or against third parties (vendors, customers, visitors) in the conduct of Company business; and to any work setting — physical premises, customer or supplier sites, business travel, Company-sponsored events, virtual meetings, and electronic communications that touch the workplace or the working relationship. It applies regardless of whether the conduct occurs during working hours.

## KEY TERMS

**Workplace Violence** — Behavior involving the threat or infliction of physical or verbal harm to persons or property, including statements, expressions of intent, intimidation or conduct against persons or property that is sufficiently severe, offensive, or intimidating enough to make a reasonable individual fear for his/her personal safety or the safety of family, friends, or property.

**Threat** — a statement or communication, direct or indirect, that a reasonable person would interpret as an expression of intent to cause physical harm to a person or damage to property. Threats include conditional, veiled, and online threats.

### Prohibited Conduct

Prohibited conduct includes, but is not limited to:

- intentional, unwelcome physical contact — including hitting, shoving, punching, kicking, biting, tripping, pinching, pushing, groping, blocking, or impeding movement;
- intentionally causing, or attempting to cause, physical injury to another person;
- intimidating, threatening, or hostile behavior, including comments, gestures, or actions regarding violent events;
- threats — verbal, written, or electronic — to harm a person or that person's family, friends, associates, pets, or property, including threats made by phone, email, text, chat, social media, or graffiti;
- stalking, surveillance, or repeated unwanted contact that creates reasonable fear for safety;
- intentional destruction or threatened destruction of Company property or property of another, including acts of vandalism, arson, or sabotage;
- brandishing, displaying, or referencing a weapon in a manner intended to intimidate; and
- unauthorized possession or inappropriate use of firearms, weapons, or other dangerous devices on Company premises or during Company business.

Knowingly false reports of workplace violence are themselves a violation of this policy and the Code of Conduct.

### Reasonable Accommodation

Company considers reasonable accommodations — for example, schedule changes, location changes, or escorts to and from a vehicle — for employees who are victims of domestic violence, sexual assault, stalking, or threats; or who are otherwise reasonably concerned for their safety at work. Accommodation requests are managed through Human Resources and coordinated with Security. This policy is intended to operate consistently with federal, state, and local laws that provide additional rights for victims.

### Reporting Responsibilities

Company employees are required to notify a member of Company Management, Security, or Human Resources immediately of any incidents of Workplace Violence which they have witnessed, suffered, or have received credible information about, regardless of the position held by the individual engaging in the violent or threatening behavior. Company encourages all employees to proactively report suspicious and erratic behavior before violence occurs in the workplace.

Employees or managers should always call local law enforcement if, in his or her good judgment, such a call is appropriate. For Company operations in California, the Workplace Violence Prevention Plan required by California Labor Code § 6401.9 (SB 553) is incorporated by reference and supplements this policy.

## TRAINING

All employees receive workplace-violence-prevention training at hire and at least annually. Training covers how to recognize warning signs, how to report a concern, how Company responds, available resources, and the protections in place for those who report. Managers and supervisors receive additional training on responding to reports and supporting affected employees. Training is updated when there is a material change to applicable law or to Company's prevention plan, and is delivered to California-based personnel in a manner that satisfies SB 553.

## GOVERNANCE

Security owns this policy day-to-day, in coordination with Human Resources. The Chief Ethics & Compliance Officer (or designee) oversees integration with the broader ethics and compliance program and with case management. The General Counsel advises on threat assessment, restraining orders, law-enforcement coordination, and disclosure-related elements. Internal Audit periodically reviews the Violent Incident Log and case-file records for indicators of underreporting and reports findings to the Audit Committee or equivalent board-level body.

**CROSS-REFERENCES**

*This policy is related to the Code of Conduct (Resource 5a), the Case Management & Investigations Policy (Resource 5c), the Non-Retaliation & Whistleblower Protection Policy (Resource 5d), the Records Retention Policy (Resource 5l), the Industrial Security Program Policy (Resource 5o) and its Insider Threat Program, the Information Security & Cybersecurity Policy (Resource 5p), the IT Acceptable Use & Online Conduct Policy (Resource 5r), the Non-Harassment Policy (Resource 5w), the Drug-Free Workplace Policy (Resource 5y), and the Environmental, Health & Safety Policy (Resource 5z).*

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5Y: DRUG-FREE WORKPLACE POLICY

## OVERVIEW

The purpose of this policy is to establish Company's position on alcohol and illegal or unauthorized drug/controlled substance abuse in the workplace and to clarify our responsibilities to comply with relevant legal requirements of government jurisdictions.

This policy applies to all employees of Company worldwide in accordance with country specific and local laws and regulations. Employees covered by collective bargaining agreements, union or works council agreements are governed by the relevant provisions of those agreements.

## KEY TERMS

**Drug-Free Workplace / Drug-Free Work Force Requirements** – Require covered U.S. government contractors to maintain a drug-free workplace and, where DFARS 252.226-7003 applies, a drug-free work force program addressing unlawful controlled-substance activity, employee notice and awareness, employee assistance and referral resources, supervisory training, testing for employees in sensitive positions, and appropriate personnel or rehabilitation-related action for covered violations.

**Illegal Drug** – A substance whose use or possession is controlled by federal law but that is not being used or possessed under the supervision of a licensed health care professional.

**Use of Illegal Drugs or Alcohol** – A confirmed positive test result for illegal drug/alcohol use per this policy. In addition, it means the misuse of legal drugs (prescription and possibly over-the-counter) where there is not a valid prescription from a physician for the lawful use of a drug or if an over-the-counter drug or substance is abused.

## POLICY

Company is strongly committed to providing a safe and secure workplace for the benefit of our employees, their families and our customers. Consequently, Company will take reasonable steps to prevent drug and alcohol abuse or misuse in the workplace and to comply with the Drug-Free Workplace Act of 1988, applicable federal contract clauses, and any applicable security, safety-sensitive, customer-site, collective bargaining, state, local, or non-U.S. legal requirements.

### DoD Drug-Free Work Force Requirements

Where a contract includes DFARS 252.226-7003, Company will maintain a drug-free work force program that includes employee assistance resources, supervisory training, self-referral and supervisory-referral procedures, and controlled, carefully monitored testing for employees in sensitive positions. For this purpose, a sensitive position includes an employee with access to classified information and other positions Company determines involve national security, health or safety, or other functions requiring a high degree of trust and confidence. Employees found to use illegal drugs may not remain on duty or perform in a sensitive position unless Company determines, under established procedures, that the employee may safely and appropriately perform in that position.

## Drug Free Awareness Program

It is Company policy to:

- Promote the dangers of drug abuse in the workplace, including notification that it is unlawful to sell, manufacture, distribute, dispense, possess or use a controlled substance on company premises.
- Promote that it is company policy to maintain a drug-free workplace.
- Provide and promote the availability of company drug counseling, rehabilitation and employee assistance programs (including self-referral programs).
- Promote and develop procedures outlining the penalties, including those listed below, that will be imposed on employees for violation of Company drug-free workplace policy:
  - Any employee convicted during their employment with Company of the distribution or sale of illegal drugs on company premises or the possession of such drugs with intent to distribute or sell on company premises shall be immediately terminated from employment.
  - Any employee convicted during their employment with Company of a criminal drug possession or drug use offense, or any employee found to be possessing or using illegal drugs, shall be subject to disciplinary action, up to and including termination. If employee is not terminated, employee is required to attend a drug counseling and rehabilitation program and shall not be permitted to perform work on a government contract until they have successfully completed the program.
- Promote that as a condition of employment, each employee must agree to abide by the terms of the drug-free workplace policy, and notify their supervisor and Human Resources, of any criminal drug conviction for a violation occurring in the workplace no later than five days after such conviction or as described in the terms and conditions of established employment agreements.
- Promote that the company may, at its discretion, require the inspection of personal property and vehicles brought onto company premises by employees and visitors. The inspections may include briefcases, purses, bags, lunch boxes, desks, file cabinets, lockers and other personal effects and areas used by employees and visitors while on company premises. Bargaining unit employees may request that a union representative be present for any inspection. Refusal to permit company inspections may result in disciplinary action against an employee, including termination. If Company has reasonable grounds to suspect that an employee is violating this policy, Company may call in the appropriate law enforcement agency to perform the search.
- Promote and develop procedures for a carefully controlled employee drug testing program, consistent with safety and security requirements, performed by qualified personnel or a third party, that employees may challenge the results. The two (2) types of testing, as permitted by the governing laws of the work location, are as follows:
  - "For cause" testing shall be conducted at the company's discretion when there is a reasonable suspicion that an employee is using or possessing illegal drugs on company premises. The circumstances giving rise to reasonable suspicion of illegal drug use or possession may include, but are not limited to the following:
    - When an employee is observed possessing or using illegal drugs or alcohol on company premises (alcohol consumption may be permitted in conjunction with certain company-sponsored social events.)
    - When an employee exhibits observably impaired performance, or erratic or unusual behavior that appears to be the result of illegal drug use or alcohol abuse.

    - » When an employee is involved in a reportable accident involving any bodily injury or any economic loss to the Company, or when an employee is involved in a reportable safety-related incident.
    - » When the company receives information concerning illegal drug activity that is either provided by reliable and credible source(s) or is independently corroborated.
  - Certain employees may be subject to random drug testing where permitted by applicable law, contract, security requirement, or site rule. This includes employees with a prior positive test result under Company drug screening; employees in return-to-duty or follow-up status, including those returning to work after completing a drug assistance or rehabilitation program; employees in federally regulated testing programs; and employees in cleared, customer-site, or safety-sensitive positions, including safety-sensitive positions performing work on a covered government contract. "Safety Sensitive" positions are those that involve access to classified information, that involve significant public or employee safety, health, or security issues, or that involve significant trust or confidence.
- Deploy supervisory training and develop procedures for the detection and handling of drug use and violations in the workplace, specifically to include that supervisors who receive notification of an employee workplace drug conviction are to immediately notify Legal department and Security department; and if appropriate the U.S. Government Contracting personnel who must be notified within 10 days.

**Marijuana and State Law:** Marijuana and THC-containing products remain controlled substances under federal law unless excluded or otherwise authorized under federal law. State or local authorization does not permit marijuana use, possession, sale, manufacture, distribution, or impairment in the workplace, while performing Company business, on customer or government sites, or where prohibited by contract, security-clearance, safety-sensitive, site-access, or other legal requirements. Off-duty or medical-marijuana issues must be reviewed under applicable federal, state, and local law.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5Z: TEMPLATE ENVIRONMENTAL, HEALTH & SAFETY POLICY

## OVERVIEW

Company is committed to conducting business in a socially and environmentally responsible manner. This includes providing safe and healthy operations for its employees, its customers, and the public, assuring compliance with occupational safety & environmental requirements and preserving company assets.

## POLICY

Environmental, Health and Safety ("EHS") criteria and practices are dictated by various laws and regulations in the location in which Company operates. To establish consistent expectations for EHS performance, Company will:

- Meet all applicable environmental laws, regulations, and permit requirements.
- Comply with applicable laws and regulations relating to safety, health and environmental quality, including selection of personal protective equipment that properly fits each affected employee.
- Consider health effects and environmental impact before selecting production materials, before buying or leasing property, and when developing new products or processes.
- Design, operate and maintain facilities that minimize emissions and wastes, while maintaining a safe workplace.
- Solicit and respond to community concerns about environmental and health issues.
- Integrate safety, health and environmental goals into applicable business functions to include purchasing, design, testing, manufacturing practices, and product support.
- Ensure effective safety, health and environmental programs are continually validated and improved through disciplined risk evaluation and strategic planning.
- Recycle reusable materials and purchase products containing recycled materials to conserve energy and reduce waste.
- Periodically survey facilities for compliance with applicable laws and regulations.
- Work constructively with trade associations, government agencies, customers, and others to develop equitable laws, regulations or guidelines.
- Develop guidelines when Company determines additional protection beyond that provided by laws and regulations is appropriate.
- Any Company employee who violates environmental, health & safety laws and regulations or does not comply with the intent of the Company policies shall be subject to disciplinary action, up to and including termination of employment.

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5AA: HUMAN TRAFFICKING & FORCED LABOR PREVENTION POLICY

## OVERVIEW

This Policy sets out Company's commitment to prevent human trafficking and forced labor in our operations and our supply chain, and to comply with U.S. and applicable foreign anti-trafficking and forced-labor laws. It applies to all Company employees, officers, directors, contractors, contingent workers, and operations globally, and to suppliers, subcontractors, and other third parties acting on Company's behalf.

## KEY TERMS

The terms below are defined in the Federal Acquisition Regulation (FAR), Subpart 22.17 – Combating Trafficking in Persons:

**Commercial Sex Act** — any sex act for which anything of value is given to or received by any person.

**Debt Bondage** — the status or condition of a debtor arising from a pledge by the debtor of his/her personal services or of those of a person under his/her control as a security for debt, if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined.

**Forced Labor** — knowingly providing or obtaining the labor or services of a person (1) by threats of serious harm to, or physical restraint against, that person or another person; (2) by means of any scheme, plan or pattern intended to cause the person to believe that, if the person did not perform such labor or services, that person or another person would suffer serious harm or physical restraint; or (3) by means of the abuse or threatened abuse of law or the legal process.

**Involuntary Servitude** — includes a condition of servitude induced by means of (1) any scheme, plan or pattern intended to cause a person to believe that, if the person did not enter into or continue in such conditions, that person or another person would suffer serious harm or physical restraint; or (2) the abuse or threatened abuse of the legal process.

**Sex Trafficking** — the recruitment, harboring, transportation, provision or obtaining of a person for the purpose of a commercial sex act.

**Severe forms of trafficking in persons** — means (1) sex trafficking in which a commercial sex act is induced by force, fraud or coercion, or in which the person induced to perform such act has not attained 18 years of age; or (2) the recruitment, harboring, transportation, provision or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

## POLICY

It is Company's policy to demonstrate through its actions that human rights violations are avoidable and unacceptable. Company will not willingly or knowingly assist in any violation of human rights or benefit from any human rights

violation committed by another party. Human rights violations include, but are not limited to, the direct or indirect procurement or use of commercial sex acts, forced labor, child labor, debt bondage, involuntary servitude and sex trafficking.

## Supply Chain Due Diligence

Company maps and monitors its supply chain to identify and address forced-labor and trafficking risk. Supply chain due diligence is performed under the framework set out in the Third-Party Due Diligence Policy, which establishes the risk tiers, screening expectations, and escalation paths Company applies to third parties — including screening against the Uyghur Forced Labor Prevention Act (UFLPA) Entity List and treatment of goods subject to the Xinjiang rebuttable presumption.

Where Company sources goods that may have been mined, produced, or manufactured in whole or in part in a region or by an entity covered by the UFLPA rebuttable presumption, Company does not import or use those goods unless the supplier provides documentation sufficient to overcome the presumption to CBP's satisfaction.

Findings of forced-labor or trafficking risk are escalated to Legal for handling under the Case Management & Investigations Policy.

Company is committed to the freedom of association and the recognition of the right to collective bargaining provided by law and to complying with all applicable wage and hour laws and providing safe and secure working conditions for employees and others working on the company's behalf.

## Government Contracting Compliance Plan

For covered government contracts and subcontracts involving supplies acquired or services performed outside the United States, Company will maintain any written compliance plan and certifications required by FAR 52.222-50. The plan will include appropriate procedures to prevent, monitor, detect, and address prohibited trafficking-related activities; employee awareness and non-retaliation reporting mechanisms; compliant recruitment, wage, and housing practices where applicable; and coordination with Contracts and Legal.

*REGULATORY WATCH — EU Forced Labour Regulation*

*The EU Forced Labour Regulation (Regulation (EU) 2024/3015) prohibits placing on the EU market, and exporting from the EU, products made in whole or in part with forced labor. The Regulation applies regardless of company size and is enforceable beginning December 14, 2027. Companies with EU customers, EU operations, or supply chains touching the EU should expect product-level enforcement, importer liability, and product-tracing obligations under this Regulation, and should plan accordingly with Legal and Trade Compliance.*

## Reporting & Resolution

All persons — including Company employees, contractors, contingent workers, and suppliers— are expected to report any actual or suspected human rights violation to any of the resources listed in the Code of Conduct or the Global Human Trafficking Hotline (1–844–888–FREE or help@befree.org).

Individuals who report suspected human rights violations can do so confidentially and/or anonymously and will be protected from retaliation as outlined in Company's Code of Conduct and Non-Retaliation policy.

## TRAINING

Company provides anti-trafficking and forced-labor awareness training at hire and at least annually thereafter to employees whose roles touch global operations, sourcing, contracting, recruitment, or human resources. Other employees receive an awareness module as part of the Code of Conduct training cycle.

## GOVERNANCE

The Ethics & Compliance Officer is responsible for this Policy. Supply Chain, Contracts, Human Resources, and Legal are jointly responsible for implementation in their respective functions. Legal maintains the controlling guidance on UFLPA Entity List screening, rebuttable-presumption rebuttal documentation, and EU Forced Labour Regulation readiness.

**CROSS-REFERENCES**

*Code of Conduct (Resource 5a)*

*Third-Party Due Diligence Policy (Resource 5h)*

*Export & Import Compliance Policy (Resource 5m)*

*Case Management & Investigations Policy (Resource 5c) — investigation handling*

*Non-Retaliation & Whistleblower Protection Policy (Resource 5d) — protection for reporters*

*Mandatory Disclosures Policy (Resource 5j)— disclosure obligations on government contracts*

*Records Retention Policy (Resource 5l) — retention of compliance plans, certifications, and screening records*

DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 5AB: GOVERNMENT RELATIONS POLICY

## OVERVIEW

The purpose of this policy is to provide a structured process and governance model for engaging with Congress on issues considered essential to accomplishing the strategic goals and operational objectives of Company. This policy encompasses all business related contact, whether direct or indirect (via consultants, prime contractors or teammates) with Congress on issues of importance to Company.

## SCOPE

This policy applies to every employee, officer, director, and contingent worker of Company. It also reaches outside consultants, contract lobbyists, prime contractors, and teammates engaged on Company's behalf in any contact with federal, state, or local government, and to any employee seeking elected or appointed government office.

## POLICY

It is the policy of Company to pursue a program of congressional relations to ensure issues, programs and concerns of the Company are strategically prioritized, understood and supported on "Capitol Hill." Policies and procedures herein are intended to ensure Company has a focused Congressional strategy that ensures the greatest success as a company.

All contact with Congress shall be pre-approved by the Company Government Relations department. In the case of classified or compartmentalized programs, that coordination will be conducted with the Company VP, Congressional Relations but be implemented by personnel with the appropriate clearances who have also been designated as the company's multi-divisional representatives with the intelligence committees.

### Congressional Contact

While everyone has a right as a citizen to contact their elected representatives on issues of personal interest, contact with Congress and strategies for dealing with Congress on issues on behalf of Company shall only be accomplished through Government Relations department. In addition, all inquiries regarding a congressional activity or concern shall be forwarded to the Company Government Relations department.

Employees shall not hire outside consultants for the purposes of lobbying Congress unless explicitly approved by the Company Government Relations department.

### Outside Lobbyists and Consultants

Engaging outside lobbyists, consultants, public-affairs firms, grassroots organizations, or similar third parties to communicate with the federal government on Company's behalf requires prior written approval from Government Relations and Legal. Government Relations and Legal coordinate any required LDA, FARA, or other periodic registration and reporting obligations.

For DoD contracts and solicitations, Company will not retain or compensate any third party if the engagement would create an ineligibility risk, including where the third party lobbies for a Chinese military company identified on the Section 1260H list. Required diligence, representations, and screening are handled under the Third-Party Due Diligence Policy.

## Contractors and Teammates

Employees shall not request and/or commit a contractor or teammate to supporting Company activities on Capitol Hill unless expressly approved by the Company Government Relations department.

Requests by prime contractors or teammates for assistance with Capitol Hill shall be immediately forwarded to the VP, Congressional Relations. Our intention is to support such requests to the greatest extent possible.

## Campaign Contributions

Requests for campaign contributions to support a political candidate or sitting Member of Congress should be forwarded to the Company Government Relations department.

Individual employees may make personal contributions to candidates and political parties of their choice. Such individual or personal contributions are not reimbursable by the company and are not tax deductible.

## Political Action Committee

Company has a Political Action Committee to which employees are encouraged to voluntarily contribute.

## Facility Reductions and Community Notifications

Whenever circumstances require a reduction of at least 25 positions in facility headcount or substantial change in a company facility's community footprint, Human Resources department is required to notify Government Relations department of related details, including actions taken to cushion adverse employee impacts.

This information will be used to notify affected DoD, government agency, and House and Senate offices immediately prior to planned public announcements.

## Annual Authorization and Appropriations Process

During the annual Congressional authorization and appropriations process, Company comments regarding specific programs will be a part of the continuing business development efforts involving all other elements of the Federal Government's Planning, Programming, and Budgeting System (PPBS) process. Every effort shall be made to develop a strong rationale ("good story") as well as strong "customer support" for each program before contact with Congress.

The annual cycle is initiated with delivery of the President's Budget request in early February, and congressional members' inputs to the various oversight committees are generally required by the end of March. Preparation, prioritization and obtaining the highest level of executive branch customer support must therefore, be finalized by no later than December 1st of the prior year to maximize Company's potential for success in Congressional marketing.

Programs requiring congressional support should be forwarded through the Business Development department to be discussed with the Government Relations department by no later than the fall of the year PRIOR to budget submission. These discussions should coincide with evolution from the programming portion of the PPBS cycle into the Budgeting portion of the cycle as the budget gains visibility and issues become better understood.

Once a program is identified as a potential congressional interest item, the Business Development department will assign a point of contact (POC) to work directly with the Government Relations department to ensure maximum success.

Strategic prioritization of Company budgetary and program support requests for individual members of Congress is an absolute necessity. The Business Development department shall prioritize programs and communicate them to the Government Relations department.

## TRAINING

Government Relations-led training is required at hire for any role that involves federal customer engagement, business development, congressional contact, or supervision of outside lobbyists, and annually thereafter. Refresh training is delivered when a regulatory or policy change materially affects the obligations in this policy.

## GOVERNANCE

Government Relations owns this policy and the related procedures. Legal advises on lobbying registration, FARA, anti-lobbying-with-appropriated-funds (Byrd Amendment) compliance, and FAR 31.205-22 cost-allowability questions. Internal Audit reviews lobbying expenditures, LDA filings, and FY2025 NDAA consultant due diligence on a risk-based cycle.

**CROSS-REFERENCES**

*Code of Conduct (Resource 5a)*

*Government Contracting Integrity Policy (Resource 5i)*

*Mandatory Disclosures Policy (Resource 5j)*

*Third-Party Due Diligence Policy (Resource 5h)*

*Records Retention Policy (Resource 5l) —*
*for retention of LDA filings, lobbying contact logs, and FARA records*

## OVERVIEW

This policy establishes the requirements for compliance with federal securities laws applicable to insider information — also referred to as material non-public information (MNPI) — affecting the market in Company securities and in securities of other companies in which Company has an interest. It also addresses procurement-sensitive information protected under the Procurement Integrity Act, which is operationally addressed in the Government Contracting Integrity Policy and the Procurement Integrity Policy.

## KEY TERMS

**Material Non-Public Information (MNPI), also known as Insider Information** – Material, non-public information on the affairs, operations, or financial position of Company that may affect the price of securities of Company or otherwise might be of significance to a reasonable investor in determining whether to purchase, sell or hold securities of Company.

Examples of MNPI include changed earnings expectations, negotiations relating to possible acquisitions or divestitures, change of dividend terms, stock splits, arrangements preparatory to an exchange or tender offer, calls for redemption, and major new contracts.

**Source Selection Information** – Information prepared for use by a federal agency to evaluate a bid or proposal to enter into a federal procurement contract, where that information previously has not been made available to the public or disclosed publicly. It includes, for example, bid prices before public opening, proposed costs or prices, source selection and technical evaluation plans, evaluations and rankings of bids or proposals, competitive range determinations, and other information marked as "source selection information."

**Contractor Bid or Proposal Information** – Information submitted to a federal agency as part of, or in connection with, a bid or proposal to enter into a federal procurement contract, where that information previously has not been made available to the public or disclosed publicly. It includes, for example, cost or pricing data, indirect costs and direct labor rates, proprietary information about manufacturing processes, operations, or techniques marked by the contractor, and other information marked by the contractor as "contractor bid or proposal information."

## POLICY

Company employees, officers and directors shall comply fully and in good faith with all laws and regulations, related to the timing of transactions, the purchase or sale of such securities and with the rules for safeguarding and disclosing MNPI.

Employees should seek guidance from the Company General Counsel regarding their responsibilities under this policy.

### Regulation Fair Disclosure (Reg. FD)

The Securities and Exchange Commission has adopted Regulation Fair Disclosure (referred to as "Reg. FD") which prohibits the selective disclosure of MNPI about Company. The reason for this rule is that selective disclosure of MNPI undermines investor confidence and creates serious conflicts of interest by securities analysts.

Company is committed to maintaining an active, public dialogue with institutional shareholders, analysts and other members of the shareholder community. Company will provide full, fair, accurate, timely, transparent and

understandable disclosure of the company's historical performance and future prospects, in accordance with SEC rules and regulations and generally accepted accounting principles.

Accordingly, Company will not disclose MNPI that has not been previously disclosed to the public in one-on-one conversations with investors, during investor conferences or analyst calls not open to the public, or in any other non-public forum nor will Company update previously issued guidance in one-on-one conversations. However, in the event that Company inadvertently discloses MNPI on a selective basis, the Company General Counsel should be contacted immediately so that prompt corrective action consistent with Reg. FD can be taken.

## Trading Restrictions

Federal securities laws prohibit insiders of Company, which includes its employees, officers and members of its Board of Directors, from trading in the securities of Company on the basis of MNPI. Employees can have personal liability for providing information to anyone outside the company (your family, your friends or anyone else) if that person uses the information to trade in the stock of Company. It is a violation even if you or the person who receives the information does not actually make a profit or receive compensation.

All employees, including employee family members and relatives, that become aware of any MNPI (information that has not yet been made available to the general public by press release or otherwise), are strictly prohibited from buying or selling Company securities or directly or indirectly disclosing such information to any other person who may trade in securities of Company until the business day following the day in which Company makes such information available to the general public.

Trading of other company securities with which Company has initiated discussions or negotiations relating to acquisition, divestiture, or other important contractual relationships shall be ruled by the same considerations as the timing of transactions in Company stock.

## Blackout Policy

**Directors, Officers or Employees subject to trading prohibitions:** Employees that are identified as a director, officer or under Company's insider trading list are subject to periodic prohibitions on the trading of the Company's securities ("Blackout Periods"). In specific, these employees are required to obtain written clearance from the Company General Counsel before selling or purchasing Company equity securities except through the straight exercise of an option under a Company employee stock option plan, when stock is purchased and held for investment, or ongoing purchases through a continuing election under the Company's retirement/401K plans.

The following outlines the terms of the blackout policy, which applies to all transactions in Company securities including open market transactions and other purchases and sales, exercises of stock options (including cashless exercises, but subject to certain exceptions referred to below), gifts, trust transfers and other non-sale transfers. These restrictions also apply to employee's spouse, children and relatives who share employee's home and certain entities in which you or any of the mentioned family members have a financial interest (e.g., certain trusts, partnerships and corporations).

Quarterly Blackout Periods. The information contained in the Company quarterly earnings announcements may be considered material nonpublic information. To protect against potential insider trading based on access to such information, Company has established four Quarterly Blackout Periods during which covered insiders may not transact in Company securities. The trading window will close at least ten business days before each earnings release.

Blackouts prior to Board Meetings. In addition to the Quarterly Blackout Periods, transactions in Company securities are prohibited for the ten calendar days preceding meetings of the Board of Directors.

Special Blackouts. A special blackout may be implemented at other times, such as during the pendency of certain transactions or when some other extraordinary company event is pending. Designated employees shall receive written notice as to the details of a Special Blackout.

### Rule 10b5-1 Trading Plans

SEC Rule 10b5-1 provides an affirmative defense to insider-trading liability for transactions made under a qualifying written trading plan adopted when the insider is not aware of MNPI and entered into and operated in good faith. The SEC's 2022 amendments added cooling-off periods, required written representations/certifications in plans adopted or modified by directors and Section 16 officers, and limited overlapping and single-trade plans. Designated insiders must consult the General Counsel before adopting, modifying, or terminating any Rule 10b5-1 plan.

### Procurement Information

Source selection information and contractor bid or proposal information must be safeguarded with the same care that applies to MNPI. Do not seek, accept, use, or disclose another offeror's bid or proposal information, or any source selection information, unless authorized by the contracting officer. If you receive such information without authorization, stop, do not read further, and contact the Legal or Contracts Department immediately. Operational requirements for protecting and handling procurement-sensitive information are addressed in the Government Contracting Integrity Policy and the Procurement Integrity Policy.

**CROSS-REFERENCES**

*Code of Conduct — Insider Information and Procurement Integrity sections (Resource 5a)*

*Government Contracting Integrity Policy (Resource 5i)*

*Mandatory Disclosures Policy (Resource 5j)*

*Procurement Integrity Policy (Resource 5u)*

*Confidential Information Policy (Resource 5q)*

## GOVERNANCE

The General Counsel administers this policy, maintains the Company insider trading list, schedules and communicates blackout periods, and reviews proposed Rule 10b5-1 plans. Designated insiders and other employees with regular access to MNPI or to procurement-sensitive information receive periodic training on this policy as part of Company's broader ethics and compliance program.

DEFENSE INDUSTRY INITIATIVE

DII

ON BUSINESS ETHICS AND CONDUCT

## SMALL BUSINESS TOOLKIT

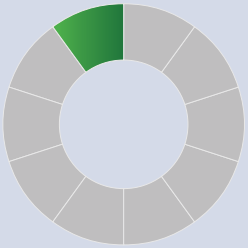
# AUDITING AND MONITORING

DEFENSE INDUSTRY INITIATIVE
DII
ON BUSINESS ETHICS AND CONDUCT

Small Business Toolkit

# RESOURCE 6: SELF-AUDITING YOUR ETHICS AND COMPLIANCE PROGRAM

**Purpose:** The purpose of a self-audit is to assess whether an Ethics and Compliance Program is effective. This audit procedure examines the effectiveness of an ethics and compliance program against the ten steps noted below. You can use these procedures for the nine-step process or for only those steps that you have implemented in your company.



## 1. Leadership Commitment

**Overview:** *The visible commitment of your company's leadership at all levels is imperative to the success of your program. Leaders set the tone and culture of an organization, including its attitude about ethics. It is imperative that employees see that leaders are committed to the highest ethical standards. It is important for a leader to understand how his or her company's ethics program works, and how his or her role as a leader fits into the program and contributes to building and maintaining an ethical culture.*

Leadership includes not just the senior executives but also those at middle management. Employee perceptions about the company's commitment to ethics and the company's commitment to non-retaliation for reporting a concern are greatly influenced by the behavior of middle management.

Here are some steps you can perform to assess the level of leadership commitment in your company:

**a.** Ensure that the following organizational structure and activities exist to demonstrate leadership commitment:

1. Does the leader of the Ethics organization report directly into the Board of Directors or Chief Executive Officer? If that is not possible, does the leader have direct access to the Board or CEO to ensure issues can be properly escalated, if needed?
2. Is there a formal statement signed by the CEO to formalize your company's commitment to the highest ethical conduct in all aspects of your business?
3. Is there an Ethics and Compliance Committee that can provide leadership and oversight to the ethics program and review status of ethics-program-related activities?
4. Does the leadership of the Ethics and Compliance Committee reflect leadership commitment by having a senior executive as Chairman of that Committee? (The committee can consist of senior leaders from the Law Department, Human Resources, Internal Audit, Business Management, Operations, Communications, Security, Information Technology, and any other organization with which you may partner.)
5. Does the company's compensation and bonus structure include criteria tied to ethics and compliance performance, and does the company have clawback provisions for compensation paid to individuals who engage in misconduct?

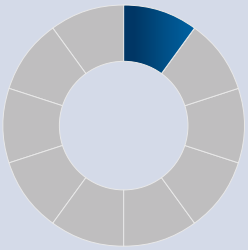
**b.** Select a random sample of your middle managers (e.g., department manager, site manager, district manager, area manager, regional manager) and ask about their role in implementing the Company's commitment to the highest ethical standards in all aspects of their responsibilities. They should say all or most of the following:

- Lead by example.
- Ensure that employees understand the company's ethics standards.
- Create a culture that encourages employees to comply with company policies and voice questions and concerns.
- Respond appropriately and immediately to concerns that are raised.
- Ensure that employees receive a copy of the Code of Conduct.

- Ensure that employees complete required training and certifications as required.
- Be cognizant of ethics exposures and take appropriate mitigating actions.

If the middle managers are not responding as noted above, that could indicate the message of ethical behavior has not flowed down to the middle-level managers who actually manage the company's business on a day-to-day basis. Therefore, you should recommend corrective actions such as additional training, communication, and coaching.

Prepare an opinion about leadership commitment based on the results of the above steps.



## 2. Company Values / Code of Conduct

**Overview:** *Your company values must be the foundation of your ethics and compliance program and should be communicated through your Code of Conduct ("Code"). The Code must also provide important business conduct information for your employees and others who represent your company. How do you know that your company has been effective in achieving these objectives?*

### The following are audit steps you can use to assess the effectiveness of the communication of your values and the Code of Conduct.

**a.** Do you provide your Code of Conduct to all of your employees, Directors and agents?

If so, examine evidence of acknowledgments of receiving the Code. This can be done by examining the acknowledgment cards, if submitted by the individuals who received the codes; or examining any electronic evidence of acknowledgment of the code if the code was distributed electronically. Examine at least 25% of such evidence selected at random.

**b.** What do you do to ensure that your employees understand the Code of Conduct and are familiar with its requirements?

Is there any training for employees to introduce them to the Code? If so, from the list of your company employees, select 25% of the names at random and examine evidence of their attendance at orientation training for the code. Such evidence, for example, can be signatures on sign-in-sheets noting employee name and employee number or other evidence as deemed appropriate.

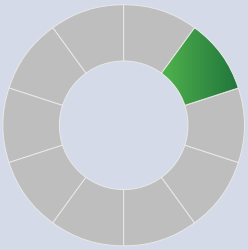
**c.** How do you know that the Code training provided to employees is effective in ensuring that the employees understand the Code and its requirements?

Select a random sample of employees (no more than 15 or no less than 10 per site) to interview, without the presence of their supervisors. The questionnaire should include the following:

1. Have they received the Company's Code?
2. Do they understand their role in complying with the standards established by the Code?
3. Do they believe the Company is serious about ethics and compliance? If not, why not?
4. What do they think are the Company's risks regarding ethics and compliance?

5. Do they know the name of their Ethics Officer or the person they can contact to report wrongdoing?

The answers to the above questions should be summarized to form an opinion regarding the effectiveness of the Code of Conduct training program.



## 3. Risk Assessment

**Overview:** *To build upon a foundation of ethics, many companies conduct a comprehensive risk assessment by looking closely at their business to determine areas of business ethics and legal risks on a periodic basis. The purpose of such assessment is to ensure that the ethics and compliance program is focusing on current business risks as a result of changes in organizations, business practices, and laws and regulations.*

### Some risk areas may include:

| | | | | |
|---|---|---|---|---|
| **Anti-Kickback/ Anti-Bribery** | **Proprietary Information** | **Cost Accounting** | **Supply Chain Integrity** | **Government Contracting Issues** |
| **Company Assets** | **Time Charging** | **Foreign Corrupt Practices Act** | **Antitrust** | **Safety Rules/OSHA** |
| **Environmental** | **Nondiscrimination** | **Procurement Integrity/TINA** | **Conflicts of Interest** | **Non-harassment** |
| **Cybersecurity and Data Protection** | **Business Courtesies/ Gratuities** | **Teaming** | **Export Control** | **AI and Emerging Technology** |

Compliance programs establish minimum acceptable conduct, whereas robust ethics and business conduct programs are the foundation upon which compliance programs and legal best practices are built. Compliance rules tend to cluster in discrete subject areas, and some areas may only concern a specific, targeted group of employees (e.g., export control issues, TINA, etc.). However, your compliance program may be integrated into your ethics and business conduct program, resulting in a cohesive, holistic Ethics and Compliance program. Here are the audit steps you can use to assess the effectiveness of your risk assessment programs:

a. What do you do to assess the risk of non-compliance with applicable laws and regulations and to assess the risk of fraudulent transactions by your employees and/or third parties?

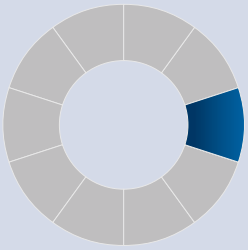
1. Is there a formal risk assessment process? If so, examine how the risk assessment is done to ensure that it is done objectively.

2. Did the risk assessment identify risks of fraud and/or non-compliance with laws and regulations? If so, are there plans for mitigating those risks? Such mitigation may include implementation of applicable policies, establishment or enhancement of internal controls, internal or external audits, segregation of duties, and training.

3. If there were risk mitigation plans, ensure that specific individuals have been identified to implement the risk mitigation plans. Seek opinions of subject matter experts (e.g., Law, Internal Audit, Controllership, IT, Corporate Security, Loss Prevention) regarding the adequacy of the risk mitigation plans.

4. Follow up on the action items after the planned implementation dates to ensure that the mitigating actions were implemented according to the plan.

Based on the above action items, provide an opinion regarding the adequacy and effectiveness of the risk assessment program in your company.

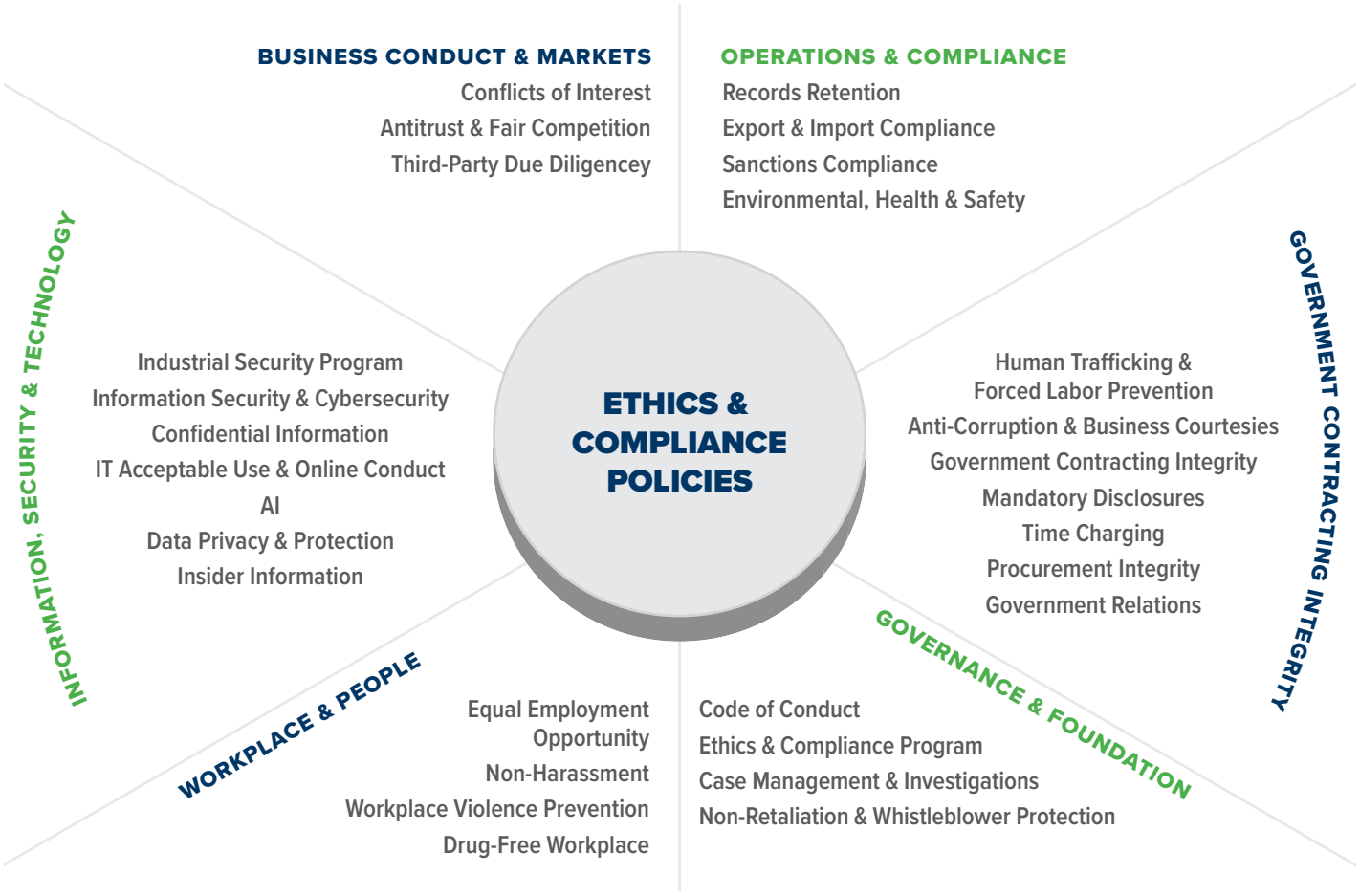


## 4. Ethics and Business Conduct Policies

**Overview:** *Your company's policies and procedures should include a statement from your CEO on ethics and business conduct. This formalizes your Company's commitment to the highest ethical conduct in all aspects of your business.*

The company's policies and procedures are the execution plans for the values and standards established in the Company's Code. Do you have policies and procedures addressing all areas of your Code to ensure that the employees understand their responsibilities to carry out the Company's commitments and to implement the standards established in the Code?

An effective Ethics and Compliance Program should include Policies and Procedures addressing the particular risks facing the company, such as:

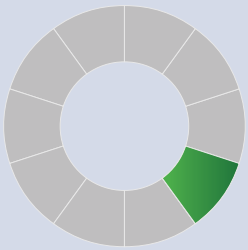


Examine your list of policies and see if all of the above risk areas are addressed. If not, recommend the establishment of such policies to facilitate compliance with relevant laws, regulations, and/or the Company's standards or guidelines. If all or some of the policies listed above exist, how do you know that the employees are aware of such policies and are knowledgeable about their roles in complying with the requirements of those policies?

In the employee interviews mentioned in audit step 1c above, ask the following questions for each of the policies relevant to your Code. The following is a suggested format for such questions:

1. I am going to read you a list of items and I'd like you to tell me how well you understand your own responsibilities in connection with each of them. It might be that you understand your responsibilities "Well," or you understand them "Somewhat," or you "Don't Really Understand Your Responsibilities," or that the item "Just Doesn't Apply To You." (Read each item and wait for the employee's response.) The questions relate to the employee's overall awareness on these issues based on their understanding of the Code and the Company's Policies and Procedures identified above in section 3.
2. If an employee says he/she is not aware of the Company's guidelines on a topic listed above, refer him/her to the specific section of the Code of Conduct.
3. Based on the results of the above interviews, prepare an opinion regarding employee awareness of your policies and procedures.

Recommend what actions, if any, need to be taken to address any deficiencies. For example, if the majority of interviewees answer "somewhat" or "don't know" to your questions about Human Rights and Conflicts of Interest, you should recommend that awareness of those policies be increased through additional training and/or communication.



## 5. Inquiry and Reporting Mechanisms

**Overview:** *It is important that your ethics and compliance program includes at least one mechanism in place for your employees, suppliers, customers, and others who do business with your company to ask questions or raise areas of concern.*

a. Do you have a process for employees to report their concerns about ethics or about violations of laws, regulations, and Company policies? If so, who is responsible for receiving employee calls or concerns? The best practice is to use a third party to receive such calls live on a toll-free line so that there is no concern about the complainant being identified.

b. If you have a Hotline number, how is it communicated to employees? Ensure that the following are done:

1. Posters with the toll-free hotline number are displayed prominently at locations where employees gather frequently (e.g., cafeteria and other common areas).

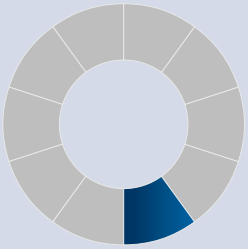
2. The name and contact information of the appropriate Ethics Officer or other appropriate person are noted to allow employees to report a concern in person if they wish to do so.
3. Ensure that the posters state that the concerns can be reported anonymously.
4. Ensure that the hotline poster states that there will be no retaliation for reporting a concern even if it turns out to be unsubstantiated.
5. Ensure that the posters are changed periodically in designs and colors so that they continue to remain noticeable.

c. Assess the effectiveness of the above reporting mechanism by asking the following questions during the interviews mentioned in 1c above:

1. Do they know that there is a hotline number they can use to report concerns?
2. Do they know where to find the hotline number?
3. Do they know that there will be no retaliation for reporting a concern if it turns out to be unsubstantiated?
4. Do they know the name and contact info of their Ethics Officer?

d. Do the company's confidentiality, severance, and employee agreements include carve-outs preserving employees' rights to report concerns to government regulators (including the SEC, EEOC, DOL, and similar agencies)?

e. Does the company periodically assess employees' willingness to report concerns (for example, through survey questions) and identify any factors that may chill reporting?



## 6. Investigation of Reported Concerns

**Overview:** *Once a concern is reported, how you investigate it determines whether employees will trust the program and continue to come forward. An effective investigation process is prompt, objective, consistently applied, and conducted by trained individuals who are independent of the matter under review. The following audit steps will help you assess whether your investigation process meets those standards.*

a. What is your process for investigating the concerns reported through your reporting mechanisms such as the company's hotline?

b. Is there a formal protocol for deciding who investigates what? Do you verify that the investigator is independent and objective and has had some training in conducting investigations?

c. Are the investigations documented in formal reports? If so, examine a sample or all of the reports completed during the past 12 months and determine if the investigations are done in accordance with the Company's protocol.

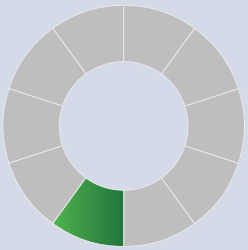
d. Is there a prioritization of concerns (e.g., A, B, C) received based on the severity of the issues raised? If so, was

there a timeline for completion of the investigation based on this categorization?

1. Were the investigations completed in accordance with the established timeline?
2. Were the investigations thorough enough to reach a conclusion regarding the validity of the concerns?
3. Was there any explanation for actions taken or not taken as a result of the concerns received?
4. Were the concerns acknowledged to assure the caller that their concerns were taken seriously and will be investigated timely and thoroughly?
5. Were the callers made aware of the results of the investigations?

e. Are confidentiality instructions to witnesses and complainants narrowly tailored to the specific investigation (for example, limited to the duration of the investigation and to specific categories of information), rather than blanket prohibitions on discussion?

Prepare an opinion about the adequacy and effectiveness of your Inquiry and Reporting Mechanisms based on the results of the above audit procedures.



## 7. Awareness Training

**Overview:** *In addition to publishing a Code, it is necessary to continue to communicate your company's commitment to ethics to your employees. Employee awareness can be achieved through something as formal as one hour of live ethics training each year or through a variety of ethics awareness initiatives that can be presented to employees periodically on a more informal basis, such as incorporating ethics discussions into regular staff meetings, safety meetings, or employee forums.*

One effective method of training is top-down, cascaded training that begins with the company's president or CEO training his or her staff. The training is then cascaded down through the entire company, with each leader training his or her direct reports so each employee hears the company's ethics message directly from his or her immediate supervisor.

Other examples of ethics training materials include videos, on-line training provided by training vendors, and live classroom training.

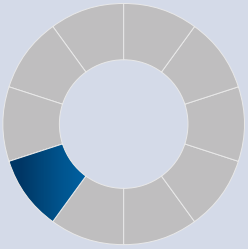
Do you have a program to train your employees to make them aware of Ethics and Compliance issues relevant to your Company? If yes:

a. How is this training delivered to employees? Is it an on-line program or live sessions? Is the delivery method adequate to reach all employees who must take the ethics and compliance courses?

b. How is one considered to have completed a course? Is there a quiz after a training course with a minimum score requirement?

c. If a tracking mechanism is used to see the completion status of required courses, what percent of the employees have completed their required courses? A best-practice ethics program will have 100% completion status.

Prepare an opinion regarding the adequacy of the Awareness Training program based on the results of the above audit steps.



## 8. Communication Program

**Overview:** *Developing a comprehensive communication plan for your ethics and compliance program allows you to manage the task of communicating your program's elements to your employees. A communication plan ensures that you are able to engage all audiences with specific messages using a variety of media.*

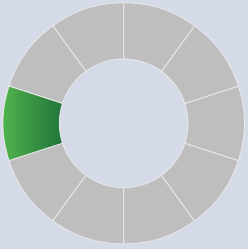
a. Does the communication of your company's commitment to ethical conduct include consistent messages delivered in engaging and diverse manners such as email, posters, company newsletters, company intranet, and other existing company communications?

b. Do all levels of leadership in your company use every available opportunity to verbalize a personal commitment to the company's ethical standards? Examine evidence of such communications (e.g., speeches, presentations, discussions on ethics topics at staff meetings, safety meetings, and All-Hands meetings).

c. Examine how often messages described above are delivered. Such messages should be frequent enough to be constant reminders for ethical behavior in all aspects of the Company's business.

d. Does the program address business communications conducted on personal devices and messaging applications (including ephemeral messaging applications)? Does the company have a policy directing the preservation of business-related communications on employees' personal devices?

The effectiveness of the above-mentioned communication initiatives will also be reflected in the employee interviews mentioned in step 1c above. Prepare an opinion on the adequacy of your Company's communication initiatives based on the results of the above audit steps and the employee interviews.



## 9. Program Assessment and Evaluation

**Overview:** *Part of maintaining an effective Ethics and Compliance Program is conducting regular program assessments and evaluations. Performing the audit procedures described in this document is one way to assess the effectiveness of your ethics and compliance program.*

You should inquire about the following question:

a. Was there any internal or external audit of your program?

b. Who conducted the audit and how was the audit team composed? Was there an appropriate mix of internal personnel, external consultants, and subject-matter experts (such as legal, accounting, or industry specialists), and were team members independent of the activities being audited?

Internal and external audits of your program addressing all areas of your program can help your company avoid noncompliance and should be conducted regularly. This may be particularly useful when there is a new business venture, downsizing or personnel changes have taken place, or complacency has become evident.

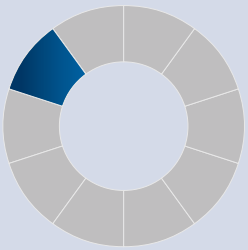
c. How often are the internal controls tested to ensure that they are adequate to prevent or detect fraud and/or non-compliance with laws and regulations?

d. Does the ethics and compliance function have appropriate access to company data (financial, HR, IT, third-party) needed to identify and assess compliance risks?

e. After completing the audit, did the company implement a follow-up review (typically three to six months later) to confirm that corrective actions were applied and that compliance improvements have been sustained?

Based on discussions with your controllers, ensure that internal controls are kept up to date and effective and that corrective action was taken when misconduct or potential for misconduct was identified.

You may also use employee surveys (separate from Human Resources surveys) and focus groups to measure the ethics culture of your company and spotlight areas for improvement in your program. Assessment surveys can also be done through external resources to ensure objectivity and independence in the expression of an opinion regarding the adequacy and effectiveness of your program in instilling ethical values, ethical leadership, and an overall ethical culture.



## 10. Discipline and Incentives

**Overview:** *An effective ethics and compliance program is reinforced through both consequences for misconduct and rewards for ethical behavior. Discipline should apply not only to those who engage in improper conduct, but also to supervisors and managers who fail to take reasonable steps to prevent or detect it. Incentives — including compensation, recognition, and advancement opportunities — should reward employees who demonstrate commitment to the program.*

a. Does the company have written standards for disciplinary action that apply to misconduct in connection with Government contracts? Confirm that discipline is available not only for the employee who engaged in improper conduct, but also for any supervisor or manager who failed to take reasonable steps to prevent or detect the conduct.

b. Is discipline applied consistently? Examine a sample of disciplinary actions taken over the past 12–24 months to confirm that similar misconduct results in similar consequences across levels of seniority and across business units.

c. Does the company's compensation structure reinforce compliance? Determine whether:

1. Eligibility for bonuses, raises, and other discretionary compensation is conditioned on meeting ethics and compliance expectations;

2. The company has clawback or recoupment provisions for compensation paid to individuals later found to have engaged in misconduct or to have supervised others who did; and
3. Ethics and compliance performance is a factor in promotion and succession decisions.

d. Does the company recognize and reward employees who demonstrate commitment to the ethics and compliance program — for example, through performance evaluations, formal recognition, or eligibility for advancement?

Prepare an opinion regarding the adequacy and effectiveness of the company's discipline and incentive practices based on the results of the above audit steps.

**Conclusion: Prepare an overall summary of your findings based on the results of the above audit steps and provide an opinion about the adequacy and effectiveness of your ethics and compliance program. Provide recommendations for corrective actions if needed. The recommended corrective actions should identify individuals responsible for implementing those actions with expected completion dates.**