Cyber Security Policy

Overview

Keeping up cybersecurity is essential for protecting The Royal Australian Chemical Institute (RACI and customer data. Without the proper measures and every employee taking up responsibility in securing their devices, services, and networks, data could become compromised and cause serious damage to the organisation and its reputation.

The RACI's partners and customers trust us to keep their data safe, and this policy has been instituted to help employees and volunteers understand their responsibilities and what is expected of them to keep our promise to our customers and partners.

Purpose

The purpose of this policy is to clearly lay out what is expected from employees, volunteers and contractors in helping secure the organisation's data, devices and network. By agreeing to and following this policy, you are helping ensure that the organisation is doing everything it can to keep sensitive and personal data protected and maintain our reputation as a secure operator.

"Personal information" has the meaning in the Privacy Act 1988 (Cth). References to "PII" in this policy are to be read as "personal information." "Confidential information" includes personal information and other non-public organisational information.

This Policy must be read with RACI's Privacy Policy and Data Retention & Destruction Policy. If there is a conflict, the Privacy Policy prevails, subject to law.

Scope

This policy applies to all employees, volunteers, temporary workers, contractors and agents acting on behalf of the RACI that use or have access to the organisation's devices, network, or any of RACI's data in digital form.

Policy

Protection of data

Confidential information

All employees, volunteers and contractors must take all reasonable precautions to protect confidential information they gather, store, manage or otherwise come into contact with as part of their roles and responsibilities, or otherwise, in the organisation.

Employees, volunteers and contractors shall not share any confidential information with any party outside of the organisation, or any person within the organisation who does not have access to the confidential information, without explicit permission from their line manager.

Confidential information includes, but is not limited to:

- Lists of customers and/or members (existing and prospective)
- Patents, formulas and new technologies
- Unpublished computer code
- Unpublished financial information
- Any other unpublished organisational or partner data
- Children's information or data
- Data relating to any education program

Personally identifiable information

All employees, volunteers and contractors must take all reasonable precautions to ensure that personally identifiable information is collected, stored, used, and shared in accordance with all applicable data protection regulations and requirements and rules set out by the organisation.

Personally identifiable information of employees, partners, customers or any other person must not be shared with any third parties without consent from the person who the data relates to, or a necessary reason to do so.

Personally identifiable information includes, but is not limited to:

- Full names of individuals
- Phone numbers of individuals
- Email addresses of individuals
- Postal addresses of individuals
- Payment card details of individuals
- School Details

Protection of devices

All employees, volunteers and contractors must take all reasonable steps to protect the physical and digital security of RACI's devices, and any device that they access the organisation's data or the network from.

All employees, volunteers and contractors must:

- Ensure that all devices under their control are protected with a secure password or other form of authentication, such as fingerprint or facial recognition

- Set all devices under their control to automatically lock themselves after no more than five minutes without activity have elapsed
- Never leave devices under their control unattended in public places
- Report any security issue relating to a device in their control to the organisation without undue delay
- Install all operating system, antivirus, and antimalware updates and patches as soon as reasonably possible
- Never allow any person not associated with the organisation to use or access a device under their control
- Never download any illegal or potentially malicious software
- Hand back any devices to the organisation once they are no longer needed.

Protection of networks

All employees, volunteers and contractors must take all reasonable steps to maintain the integrity of the organisation's network or networks, and ensure that no unauthorised party is able to gain access to the network or networks.

All employees, volunteers and contractors must:

- Only access the organisation network from a device owned by the organisation or one that they have been given explicit permission to access the organisation's network from by the organisation.
- Ensure that all devices that access the organisation's network are up to date on operating system and antivirus software updates
- Utilise a Virtual Private Network or any other software that have been provided to them by the organisation to help ensure the integrity of the organisation's network.

Use of cloud and third-party systems

Only use cloud or third-party services that have been assessed for compliance with the Privacy Policy's overseas disclosure requirements (Australian Privacy Principles - APP8). Consult RACI's external Managed Services Provider and CEO before onboarding new systems that may host personal information outside Australia.

Email security

Email must be used responsibly to ensure that the organisation's network, services or data do not become compromised due to insecure use. All employees, volunteers and contractors must take all reasonable steps to ensure that they reduce the risk of downloading malicious software or giving up personal or confidential information or access to organisation's systems due to insecure use of email.

All employees, volunteers and contractors must:

- Only send and receive organisation-related information and correspondence from their official organisation-provided email address
- Protect their organisation email address with a secure password and multi-factor authentication if available
- Never send or forward any confidential or personal information to any third-party email address unless (a) the disclosure complies with the Privacy Policy (i.e., with consent or under an APP exception), and (b) you have explicit permission from your line manager.
- Exercise caution and take reasonable precautions when receiving emails to reduce the risk of downloading a malicious attachment or clicking a link to a malicious website
- Never open attachments in email from unknown sources
- Never send passwords or other credentials over email.

Internet security

The internet must be used in a responsible manner and only as and when required for organisational purposes. Employees, volunteers and contractors are responsible for ensuring that their use of the internet does not expose RACI's devices, networks, or data to unauthorised access or damage from malicious software.

All employees must:

- Use an up-to-date, secure web browser when accessing the internet
- Run an up-to-date antivirus software on their devices and ensure that they have installed the latest operating system updates and patches
- Limit personal use of the internet on RACI's devices and the company network to a reasonable minimum
- Never access illegal or potentially malicious websites or content
- Never access pornographic, offensive or violent content
- Report any potential security incident to RACI's external Managed Services Provider without any undue delay.

Compliance

Compliance measurement

The RACI will verify compliance with this policy through any methods deemed appropriate, including but not limited to: business tool reports, internal and external audits and feedback to the policy owner.

Exceptions

Any exceptions to this policy must be approved by the CEO in advance and have a written record.

Non-compliance

Any employees, volunteer or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Security incidents & data breaches.

Report suspected security incidents immediately to RACI's external Managed Services Provider and the CEO. RACI will assess incidents under the Data Breach Response Procedure and the Notifiable Data Breaches scheme and notify affected individuals and the Office of the Australian Information Commissioner (OAIC) where required.

Approved by Board on	30 March 2026
Responsible Person	CEO
Scheduled Review	30 March 2028 (Once every two years, on date of Board approval)