PROFESSIONAL PRACTICE STATEMENT
Developing a Business Continuity Plan
ADOPTED: OCT. 2012

What is a professional practice statement?
Professional Practice Statements developed by the Association Forum are provided as a management tool for associations and individual association professionals, developed by experts in the industry, and recommended as a means to achieve excellence in managing associations and other nonprofit organizations.

BACKGROUND
A business continuity/disaster recovery plan is essential for organizational stability in an emergency. A well-developed business continuity plan can provide the association with a roadmap for maintaining revenue streams, continued operations and customer service during times of crisis.

POLICY STATEMENT
Every association should have a business continuity plan (“Plan”) covering key areas of its operations including but not limited to physical facilities, finance, technology, human resources, communication, public relations and risk management. The Plan should define a means for the association to resume operations without significant delay in the case of a local/city/state/ or national event, natural disaster or other unforeseeable events preventing normal business operations. The Plan should take into consideration the severity of the disaster, ranging from something as simple as an outage within the building (which may require a simple and quick resolution) to something more severe such as a natural disaster or terrorist attack (which may require a full business shut-down with functions moving to a disaster recovery site).

Overall, the Plan should define key business functions and plans for continuation of revenue-generating activities, and possible reduction of expenses until business conditions return to normal. It should include information about when and how the Plan will be activated, who declares a disaster, and who should be contacted. The Plan should include an inventory of key business functions, identify priorities and indicate the expected recovery time objective. (See Table 1)

The plan ideally should be reviewed and updated annually by representatives from all the association’s units that have responsibilities under the Plan. The Plan should be available to staff and multiple copies should be available so each unit has access to a written copy. At least one copy should be maintained off-site in a secure location and also available on an intranet, extranet or independent web site. In addition, tests should be performed on a regular basis, such as once a year, so those affected by a business interruption are familiar with their responsibilities. Senior volunteer leaders also should have a copy of the Plan so they are informed as to the association’s response protocols.

PHYSICAL FACILITIES
In the event of a business interruption it may be necessary to move or repair the association’s physical location(s). A successful Plan may include, depending on organizational needs and circumstances, the following:

- Designated chain-of-command within staff and volunteer leadership with clear responsibility for securing alternate space and/or fiscal authority to contract for repairs and establishing services at an alternate location.
- A list, with complete contact information, of key leadership, vendors, business partners, and emergency response agencies that would need to be advised regarding status of personnel and operations or contacted to obtain supplies and support. Develop a list of “back-up” providers.
- Procedures for remote operations. Remote operations would include all staff having access to the internet, IT infrastructure set up to allow for staff to be online at one time, access to e-mails and files, and customer service calls being forwarded.
- Procedures for closing the building, and shutting down and securing equipment in an orderly fashion that will assist in restoring operations later. Clearly identify the conditions that could necessitate a shutdown and who is authorized to conduct the shutdown.
- Clear understanding of the effects of a partial or full shutdown on other facility operations and how long it will take to shutdown and restart facility operations.
• Prioritized list of equipment that would need to be or could be moved if the facility became unusable.

• If appropriate, a secondary location in case facilities become unavailable. Choose a location that would be accessible in an emergency, considering communication capabilities (telephones, cell phone operability); computer/internet capability; and a size large enough to accommodate staff needed on-site to keep the association functioning and provide needed services.

• Security considerations relating to both the evacuated facility and a secondary location.

• Insurance coverage contacts and other information detailing the requirements in the event of a loss, the types of records and documentation that will be required to file claims and what records need to be protected.

• The recovery period after a disaster is key. Organizations that are in a temporary location will need to consider staffing, equipment, data collection, and other key operational issues over an extended period of time. See the Key Business Process Inventory (Table 1).

• Contact information for the U.S. Postal Service and other delivery services to provide information on where to redirect mail and other types of correspondence.

FINANCIAL

Financial integrity is crucial in any business emergency to protect assets, minimize loss and avoid disruption. Finances are key to ensuring the association’s long term viability. Consideration should be given to the following before a disaster occurs:

Ensure that all financial records are identified, backed-up and protected.

Alert banking, investment, insurance and other financial relationships to potential disruption in operations.

Arrange for secure remote computer access, if it may be needed for future use.

Ensure appropriate levels of reserves which will sustain the association in the case of an interruption in revenue-generating activities.

Create a clear plan for and prioritization of fixed and variable expenditures that can be modified in the event revenue-generation is altered. This should include how personnel issues would be handled.

Maintain proper levels of insurance to protect the association from risk.

TECHNOLOGY

In order to effectively deal with situations that would seriously affect business processes, the Information Technology (IT) department should develop a comprehensive plan for restoring all technology infrastructures (“IT Plan”). In the event of an interruption, the IT Plan should be used to guide the recovery and continuation of association business information systems. The IT Plan should be incorporated and housed with the associations overall business continuity plan. The IT Plan should include details of the back-up and restore systems.

Attached to this Statement is a detailed outline of objectives, recovery, and testing issues to be considered and incorporated into the IT Plan as a part of the overall business continuity plan.

HUMAN RESOURCES

An association should develop a good communication plan to communicate with employees which phases of the business continuity plan will be implemented and the role of each team member. Organizing a staff team of members to be the point person from each department will be helpful to facilitate communication.
Associations should also consider the possibility that employees’ personal lives may be disrupted and their ability to contribute may be affected. A good business continuity plan will take into account various staffing scenarios based on the impact to the association and its human resources. It may be critical to be able to process payroll from a location outside of your facilities if they cannot be occupied.

MARKETING, COMMUNICATION AND PUBLIC RELATIONS

In the case of business interruption it may be necessary to communicate with a variety of publics – including, but not limited to, board, staff, members, stakeholders, vendors, attorneys, insurance agents, media, and various local, regional and national authorities. The association should:

• Assign a person to the communication function with additional assistance as required by the scope of the problem.
• Provide information to staff and others directly impacted by the emergency, including safety instructions, and how to obtain medical, transportation, equipment, relocation, meals and/or other assistance.
• Provide information to key leadership and to the membership regarding the organization’s status and methods for communication.
• Maintain a list of all employees with home, cell phone and emergency contact information. Also maintain lists of methods of communicating with each of the other potential audiences with copies of all lists kept off-site and immediately available.
• Designate an authorized media spokesperson in the event the emergency attracts media attention or requires more detailed organizational information.
• Communicate concise information rapidly to all necessary parties as quickly as possible with instructions on any action needed to be taken. Include information on how to contact headquarters staff.
• Report progress promptly as the situation changes and normal business resumes.
• Consider creating a secure website for staff to obtain communications from association leadership.

DISCLAIMER

The Association Forum expressly disclaims any warranties or guarantees, expressed or implied, and shall not be liable for damages of any kind, in connection with the material, information, or procedures set forth in these Statements or for reliance on the contents of the Statements. In issuing these Statements, the Association Forum is not engaged in rendering legal, accounting, or other professional services. If such services are required, the services of a competent professional should be sought.

REFERENCE LIST

Article of ABCs of BC/DR Planning from the CSO (Chief Security Officer) http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf
Disaster Planning: http://www.sba.gov/content/disaster-planning
Disaster Planning Can Reduce Time to Recovery and Expense: http://preparemybusiness.org/planning

ATTACHMENT TO DEVELOPING A BUSINESS CONTINUITY PLAN - INFORMATION TECHNOLOGY PLAN

IT PLAN OBJECTIVES

The modern association depends on information systems for day-to-day business activities. Each department therefore depends on the hardware, software, networks and information technology personnel to perform their respective functions.

No IT Plan can be created that would anticipate all variables but the plan should contain steps to mitigate data and system loss as much as possible. Time is also a major consideration in limiting the disruption to the business. Primary objectives for IT should include:

1. Provide information about when and how the IT Plan will be activated.
2. Outline checklist and/or flow diagrams that indicate actions for restoring critical systems.
3. Provide information on personnel that will be required to carry out the plan and the computing expertise required (both internal and external to the association).
4. Identify equipment, software, vendors and other items necessary for recovery.

Within these objectives, key consideration should be given to the following variables;

1. Salvage operations at the disaster site (protective and reactive measures) and secondary location site(s).
2. Recovery process accountability (staff accountable for tasks necessary).
3. Purchase of new equipment (staff accountable and vendors necessary).
4. Recovery of both the physical platform equipment/networks and operating systems software.
5. Restoration of application data (user/departmental databases and files).
6. Move to restored permanent location (if necessary).

TECHNOLOGY RECOVERY

Information needs to be gathered before beginning recovery operations; this includes damage assessment data and first-hand reports from staff and first responders. This will help you assess which functionalities have been affected, how they were affected and how that impacts the recovery time objective. Use the key business process inventory as a primary guide; begin restoring critical systems using the priorities defined in the IT Plan. Items to consider include:
### TABLE 1 - KEY BUSINESS PROCESS INVENTORY

<table>
<thead>
<tr>
<th>Key Business Process</th>
<th>Recovery Time Objective</th>
<th>Desired Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>24 hours</td>
<td>Enable access to web site for communications and revenue continuation</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>24 hours</td>
<td>Enable communications with employees, leaders, members, constituents, vendors, media etc.</td>
</tr>
<tr>
<td>Email</td>
<td>24 hours</td>
<td>Enable email communications with employees, leaders, members, constituents, vendors, media etc.</td>
</tr>
<tr>
<td>Financial systems</td>
<td>3 days</td>
<td>Resumption of financial transactions to restore financial viability</td>
</tr>
<tr>
<td>Applications/Databases (includes AMS)</td>
<td>2 days</td>
<td>Resumption of member and customer interactions, either via web or telephone</td>
</tr>
<tr>
<td>Remote connectivity</td>
<td>24 hours</td>
<td>Association staff re-connection to perform functions</td>
</tr>
<tr>
<td>External systems/Third party technology providers</td>
<td>2 days</td>
<td>Accelerated recovery of systems such as externally provided credit card or payroll processing</td>
</tr>
<tr>
<td>Personal computers</td>
<td>4 days</td>
<td>Immediate work resumption from original or alternative location</td>
</tr>
<tr>
<td>Other office equipment</td>
<td>5 days</td>
<td>Resumption of normal functionality for items such as faxes, printers, copiers, etc.</td>
</tr>
</tbody>
</table>

### TESTING

Identifying the infrastructure requirements to begin operations after a disruption is only the beginning. Like the overall plan, the IT Plan should include a comprehensive testing component that would include defined outcomes to measure success. The test plan should be performed at least annually. An assessment of the plan and the success of recovery should be done to validate the assumptions and to determine any gaps in skills, systems and/or resources.