SCIGON
Technology Consulting | Engineering | Products

Business Continuity Plan / Emergency Procedures

Contents

Emergency Contacts/Emergency Response Team

Name	Roles	Emails	Office/Mobile
John Scifers	CEO/Chief Technologist/Response Team Lead	jscifers@scigon.com jscifers@gmail.com	847-453-8890 630-544-9798
Eugene Gonchar	COO/Response Team Lead Backup	egonchar@scigon.com egonchar@hotmail.com	847-453-8885 224-212-0505
Anna Kousgaard	Marketing/Communications Manager	akousgaard@scigon.com Annakousgaard1@gmail.com	847-951-2662
Julia Fosco	Office Manager/Communications Backup	jfosco@scigon.com Julia.fosco@gmail.com	877-554-5678 847-393-6341
Caitlin Nowlan	Administrative/Support	cnowlan@scigon.com cnowlan@gmail.com	847-453-4386 708-476-9368

Purpose

The purpose of this business continuity plan is to prepare SCIGON in the event of disaster caused by factors beyond our control (e.g., natural disasters, man-made events, cyber-attacks, etc.), and to restore operations to the widest extent possible in a minimum time frame. All SCIGON sites are expected to implement preventive measures whenever possible to minimize network failure and to recover as rapidly as possible when a failure occurs.

This plan identifies vulnerabilities and recommends necessary measures to prevent and or minimize impact to operations. It is a plan that encompasses all SCIGON system sites and operations facilities.

Scope

The scope of this plan is limited to the restoration of services impacting the normal day to day operation of SCIGON. This is a business continuity plan, meant to be implemented in the event of a disaster. It is not a daily problem resolution procedures document.

Plan Objectives

- Serves as a guide for the SCIGON management teams.
- References and points to the location of any data that resides outside this document.
- Provides procedures and resources needed to assist in recovery and restoration of “normal” business operations as quickly as possible.
- Identifies vendors and customers that must be notified in the event of a disaster that impacts SCIGON operations.
- Assists in minimizing confusion experienced during a crisis by providing a document to follow with testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.

- Documents storage, safeguarding and retrieval procedures for vital records.

Assumptions

- Key people (Managers/Team Leaders or Alternates) will be available following a disaster.
- A national disaster such, as nuclear war, is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.
- Each department will have its own plan to handle unique recovery procedures, critical resource information and procedures.

Disaster definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by SCIGON operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

Emergency Response Team

Individual responsibilities may be delineated in fuller detail elsewhere in this document. Primary point of contact in call cases shall be the Response Team Lead, followed by the Response Team Lead Backup. Individual responsibilities will be assigned by that Team Lead and/or Backup depending on the scenario and specific situational factors.

- Chief Technologist/Response Team Lead: Heads all emergency response, recovery and continuity activities.
- COO/Response Team Lead Backup: Backup to the Response Team Lead in case that individual is unavailable. Will head all emergency response, recovery and continuity activities in absence of Response Team Lead. Will otherwise coordinate with the Response Team Lead in executing response, recovery and continuity activities.
- Marketing/Communications Manager: Will handle communications to employees, consultants, customers, vendors, and other stakeholders. Will support activities of the Response Team Lead and Response Team Lead Backup in emergency response, recovery and continuity activities.

Team member ongoing responsibilities

- All the members should keep an updated calling list of their work team members' work, home, cell phone numbers both at home and at work.
- All team members should keep this binder for reference at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

Instructions for using the plan

Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location, or a replacement location and control is returned to the appropriate functional management.

General Emergency Procedure:

1. Notify all contacts referenced above of pending event, if time permits
2. If impending disaster can be tracked in advance, within 72 hours:
    a. confirm Cloud-based/offsite server availability and geographic redundancy required for business to continue.
        i. Exchange Email/Calendar/ActiveDirectory: Intermedia
        ii. Cloud-based storage of key business documentation
            1. Primary documentation: SharePoint (Intermedia) – accessible by all team members identified above
            2. Proprietary documentation: SugarSync and DropBox—accessible by Response Team Lead and Response Team Lead Backup
        iii. Project Solution backups: Microsoft Azure
        iv. Project Management, Communication and Collaboration Systems: Skype for Business, Trello, Slack
    b. Refresh local PC image backups and provide to Chief Technologist/Response Team Lead for storage offsite in a water/fireproof safe.

Response Team Lead Responsibilities

Acting or actual Response Team Lead shall take the following actions:

- Evaluate which recovery actions should be invoked and direct activities of personnel.
- Evaluate and assess damage assessment findings.
- Set restoration priority based on damage assessment.
- Provide senior management with ongoing status information.
- Acts as a communication channel to corporate teams and major customers.
- Work with vendors and personnel develop a rebuild/repair schedule.

Disaster declaration

The Emergency Management Team Lead is responsible for declaring a disaster and notifying personnel. This notification will activate the various recovery teams as outlined in this plan.

Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the Chief Technologist/Response Team Lead must be notified immediately in the following cases:

- One (1) or more systems and/or sites are down for five (5) or more hours
- Five (2) or more systems and/or sites are down concurrently for two (2) or more hours
- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur

External communications

Marketing/Communications Manager is designated as the principal contact for communicating with customers, employees and the media (radio, television, and print), regulatory agency, government agencies and other external organizations following a formal disaster declaration if applicable.

Marketing/Communications Manager and Office Manager are tertiary contacts in the event the Chief Technologist/Response Team Lead and Response Team Lead Backup cannot be reached. In such a situation, these personnel shall assume the responsibilities of the Response Team Lead as appropriate to their respective positions.

Emergency management standards

Data backup policy

Full and incremental backups preserve corporate information assets and are performed on a regular basis through secure Cloud data providers (currently SharePoint, Sugarsync, Dropbox, MS Azure)

Redundant copies of data are also located on physical hardware on site. Disc images of key local machines are also updated at the beginning of each year, with operational documents and other operational data and software, and are stored in a remote facility in a fire/waterproof safe.

Retention policy

Data/code backups are stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing hardware with key operational documents and other operational data and software.

Emergency management procedures

The following procedures are to be followed by personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

These procedures are furnished to *SCIGON* management personnel to take home for reference.

In the event of any situation where access to a building is denied, personnel should report to emergency contacts referenced above.

In the event of a natural disaster

In the event of a major catastrophe affecting a SCIGON facility, seek shelter and immediately notify the Chief Technologist/Response Team Lead

In the event of a fire

In the event of a fire or smoke in any of the facilities, the guidelines and procedures in this section are to be followed.

If fire or smoke is present in the facility, evaluate the situation and determine the severity, categorize the fire as *Major* or *Minor* and take the appropriate action as defined in this section. Call 911 as soon as possible if the situation warrants it.

- Assess the situation and determine if outside emergency assistance is needed; if this is the case, dial 911 immediately.
- Personnel are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.

- In the event of any emergency situation, system site security and personal safety are the major concern. Each department head should ensure their department has exited the building and a roll call should be done at a pre-determined meeting place.
- In the event of a major catastrophe affecting the facility, immediately notify the Chief Technologist/Response Team Lead.

In the event of a network services provider outage

In the event of a network service provider outage, the guidelines and procedures in this section are to be followed:

- Assess the situation and determine if outside emergency assistance is needed; if this is the case, dial 911 immediately.
- Notify the Chief Technologist/Response Team Lead
- Establish network continuity for key systems (Email, Internet, etc.) using mobile hotspots and/or mobile devices
- In the event that mobile hotspots and/or mobile devices prove impractical for the duration anticipated by network service provider, Chief Technologist/Response Team Lead will assign alternate locations for continuing business operations

In the event of a flood or water damage

- Assess the situation and determine if outside emergency assistance is needed; if this is the case, dial 911 immediately.
- Notify the Chief Technologist/Response Team Lead
- Immediately notify all other personnel in the facility of the situation and to be prepared to cease operations accordingly.
- If water is originating from above the equipment, power down the individual devices and cover with protective shrouds located in the facility.
- Water detected below the raised floor may have different causes:
    - If water is slowly dripping from an air conditioning unit and not endangering equipment, contact repair personnel immediately.
    - If water is of a major quantity and flooding beneath the floor (water main break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow supervisor's instructions.

On-duty personnel responsibilities

Upon observation or notification of a potentially serious situation during working hours at a system/facility, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the Chief Technologist/Response Team Lead.

Marketing/Communications Manager responsibilities

Marketing/Communications Manager shall consult Chief Technologist/Response Team Lead on appropriate communications with internal/external stakeholders, customers, partners, vendors and employees about business continuity issues. These communications will address the following scenarios:

- Inform team members
- Notifying account teams/customers
- Contacting vendors

Maintenance of Key Contact Information

Personnel referenced in the Contacts List at the beginning of this document all have access to key points of contact for employees, vendors and internal/external stakeholders through documents and data housed in SCIGON's email/communications systems (Exchange) and through Cloud-based redundant document repositories (SharePoint, Sugarsync, Dropbox)

Decide course of action

Response Team Lead/Response Team Lead Backup decides how to respond to the event. As appropriate, the following scenarios will be addressed:

- Conduct situation assessment
- Identifying facilities, vital records and equipment needed for resumption activities that could be operationally restored and retrieved.
- Contact insurance providers, as appropriate
- Execute business recovery (24 hours - full recovery):
    - Delegate responsibilities for personnel unavailable for resuming normal operations
    - Resume system and facility operations
    - Assuming all relevant operations have been recovered (potentially at an alternate site or sites), and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the recovery location.