SCIGON
Technology Consulting | Engineering | Products

Disaster Recovery Plan Policy/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

Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives SCIGON Solutions ("SCIGON") a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

Purpose

This policy and plan defines the disaster recovery plan that describes the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

Scope

This policy is directed to the Management Staff, which is accountable to ensure the plan is kept up-to-date.

Current Systems State

SCIGON does not store, process or otherwise handle personally identifiable information, Protected Health Information (PHI), or other sensitive data for any partner or customer. Personally identifiable information or Protected Health Information (PHI) of SCIGON personnel is stored in an encrypted format in systems to which only SCIGON's management team has access. Proprietary data and key operational documentation of SCIGON related to business operations is stored in an encrypted format using Cloud-based technologies (e.g. Intermedia SharePoint/Exchange, SugarSync, DropBox). Only SCIGON's management team has access to this key operational documentation.

Procedures

- In the event of a disaster, contact the Response Team Lead or backup contacts
- Response Team Lead General 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.
- Refer to procedures in the Business Continuity Plan / Emergency Procedures document

This and associated documents, at a minimum, should be reviewed an updated on an annual basis.

Compliance

Understanding of Procedures

Management Staff will periodically discuss the Policy/Procedures under this document to ensure understanding and agreement.

Exceptions

Any exception to the policy must be approved by Executive Staff in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Business Continuity Plan / Emergency Procedures

Definitions and Terms

Disaster Recovery Plan (DRP)

A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster