IS-13 DISASTER RECOVERY POLICY

**13. Disaster Recovery Policy**

The <COMPANY NAME> Contingency Plan establishes procedures to recover <COMPANY NAME> following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the <COMPANY NAME> Security Officer and Privacy Officer.

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
   1. Notification/Activation phase\* to detect and assess damage and to activate the plan;
   2. Recovery phase\* to restore temporary IT operations and recover damage done to the original system;
   3. Reconstitution phase\* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out <COMPANY NAME> processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to <COMPANY NAME> systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering <COMPANY NAME> systems during prolonged periods of interruption to normal operations.
5. Ensure coordination with other <COMPANY NAME> staff who will participate in the contingency planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

This <COMPANY NAME> Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

This <COMPANY NAME> Contingency Plan is created under the legislative requirements set forth in the Federal Information Security Management Act (FISMA) of 2002 and the guidelines established by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, titled "Contingency Planning Guide for Information Technology Systems" dated June 2002.

The <COMPANY NAME> Contingency Plan also complies with the following federal and departmental policies:

* The Computer Security Act of 1987;
* OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000;
* Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999;
* Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998;
* PDD 63, Critical Infrastructure Protection, May 1998;
* Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999;
* Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, internal malicious activities.

<COMPANY NAME> defines two categories of systems from a disaster recovery perspective.

1. \*Critical Systems\*. These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. \*Non-critical Systems\*. These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

**13.2 Planning**

### Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The primary strategy chosen is for a fully mirrored recovery site. This strategy entails the maintenance of a fully mirrored system that will enable instantaneous switching between the live system and the backup system.

|  |  |
| --- | --- |
| KEY BUSINESS PROCESS | BACKUP STRATEGY |
| SaaS Web App Operations | Fully mirrored recovery site  ● Full backups – daily  ● Differential backups – hourly  ● Transaction log backups – every 10 minutes  ● Backups pushed to XXX after completing on the local system  ● Backups are retained and expire through XXX  Object Lifecycle management:  ○ Moved from XXX to XXX after 30 days  ○ Delete from XXX after 365 days |
| Website | Fully mirrored recovery site |
| Email | External vendor |
| Finance | Off-site data storage facility |
| Contracts | Off-site data storage facility |
| Product Sales | Off-site data storage facility |
| Human Resources | Off-site data storage facility |

### **13.2.1 Threat and Risk Assessment and Management**

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

The <Company Name> IT Risk Assessment documents a full detailed assessment of threats.

**13.3 Responsibilities**

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

1. The \*\*Ops Team\*\* is responsible for recovery of the <COMPANY NAME> hosted environment, network devices, and all servers. Members of the team include personnel who are also responsible for the daily operations and maintenance of <COMPANY NAME>. The team leader is the CTO and directs the Dev Ops Team.
2. The \*\*Web Services Team\*\* is responsible for assuring all application servers, web services, and platform add-ons are working. It is also responsible for testing redeployments and assessing damage to the environment. The team leader is the CTO and directs the Web Services Team.

Members of the Ops and Web Services teams must maintain local copies of the contact information from [§13.2](#13.2-line-of-succession). Additionally, the CTO must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

**13.4 Testing and Maintenance**

The CTO shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

**13.4.1 Tabletop Testing**

Tabletop Testing is conducted in accordance with the the [CMS Risk Management Handbook, Volume 2 - <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VII_4-5_Contingency_Plan_Exercise.pdf>). The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

\* Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

**13.4.2 Technical Testing**

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

* Process from backup system at the alternate site;
* Restore system using backups; and
* Switch compute and storage resources to alternate processing site.

**13.5 Disaster Recovery Procedures**

**13.5.1 Notification and Activation Phase**

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to <COMPANY NAME>. Based on the assessment of the Event, sometimes according to the <COMPANY NAME> Incident Response Policy, the Contingency Plan may be activated by the CTO.

The notification sequence is listed below:

1. The first responder is to notify the CTO. All known information must be relayed to the CTO.
2. The CTO is to contact the rest of the team and inform them of the event. The CTO is to to begin assessment procedures.
3. The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to follow the steps below.
   1. Damage Assessment Procedures:
   2. The CTO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.
   3. Alternate Assessment Procedures:
   4. Upon notification, the CTO is to follow the procedures for damage assessment with combined Dev Ops and Web Services Teams.
4. The <COMPANY NAME> Contingency Plan is to be activated if one or more of the following criteria are met:
   1. <COMPANY NAME> systems will be unavailable for more than 48 hours.
   2. Hosting facility is damaged and will be unavailable for more than 24 hours.
   3. Other criteria, as appropriate and as defined by <COMPANY NAME>.
5. If the plan is to be activated, the CTO is to notify and inform team members of the details of the event and if relocation is required.
6. Upon notification from the CTO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
7. The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
8. The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
9. Notification can be message, email, or phone.

**13.5.2 Recovery Phase**

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the <COMPANY NAME> infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild <COMPANY NAME> infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected.
2. Assess damage to the environment.
3. Begin replication of new environment using automated and tested scripts. At this point it is determined whether to recover in Rackspace, AWS, Azure, or another cloud environment.
4. Test new environment using pre-written tests.
5. Test logging, security, and alerting functionality.
6. Assure systems are appropriately patched and up to date.
7. Deploy environment to production.
8. Update DNS to new environment.

**13.5.3 Reconstitution Phase**

This section discusses activities necessary for restoring <COMPANY NAME> operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, <COMPANY NAME> operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration

* Begin replication of new environment using automated and tested scripts, currently Chef and Salt. - Dev Ops
* Test new environment using pre-written tests. - Web Services
* Test logging, security, and alerting functionality. - Dev Ops
* Deploy environment to production - Web Services
* Assure systems are appropriately patched and up to date. - Dev Ops
* Update DNS to new environment. - Dev Ops

2. Plan Deactivation

* If the <COMPANY NAME> environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the <COMPANY NAME> Media Disposal Policy.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 12.c - Developing and Implementing Continuity Plans Including Information Security

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(7)(i) - Contingency Plan

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |