Disaster Recovery Plan (Excerpt)

Contents

Purpose

The following plan is designed to be a guide for recovery of normal operations at Onpoint Health Data following a disaster which affects the delivery of Information Technology services. This can be small disaster affecting a server or set of servers, or a large disaster affecting all data services.

Scope

The plan covers the recovery of supporting systems, applications, and data at Onpoint Health Data. Locations include the office in Portland, Maine and Amazon Web Services (AWS).

Recovery Strategy

The primary backup strategy involves daily snapshots of AWS virtual servers, which are then replicated to multiple AWS data centers in the same region. The recovery point objectives (RPO) and recovery time objectives (RTO) can be found in the Business Impact Analysis

AWS resources have been created with duplicates of all critical services across different availability zones. In the event of a disaster in one zone, systems will be automatically made available in the secondary zone.

Disaster Declaration

A disaster will be declared when an unplanned outage is *expected* to last for more than 48 hours. The decision will be made by the CEO within 8 hours of the start of the outage. The decision will be made in consultation with the ISO and the management team.

Communications

The ISO will notify senior staff through email and telephone or in person if possible. Senior staff will notify their employees. The CEO will be responsible for coordinating all communication with customers and local authorities.

Security

Access to ePHI, PII, and company confidential information must be done in accordance with its security settings throughout the disaster. Recovery procedures must ensure that data is restored with exact permissions. At no time shall access controls be removed or protections in place be reduced to facilitate access unless expressly approved by the ISO. RTO and RPO will take into account no lapse in security settings.

By policy, the use of ePHI by employees follows a similar principal: security settings on workstations and in alternate work locations must match the security policies for normal working hours.

Resumption of Services

In the event that production operations in the data center are interrupted, all mission critical system functions will be brought online from the secondary AWS data center by the IT Technical Operations team.

If operations in the Portland office location is interrupted, employees have the capability of working remotely. Business operations would not be impacted as all data and applications are either at the data center or in the cloud. Please refer to the Business Continuity Plan for more detailed response information.

Testing & Review

The ISO will coordinate annual plan testing and decide which of the following to test:

- Tabletop discussions that examine scenarios and recovery arrangements.
- Simulations that train personnel for crisis management roles.
- Disaster recovery procedures to ensure information systems can be restored effectively.
- Test of service provider and supplier services to ensure that they meet contractual requirements.
- Complete rehearsals that include personnel, equipment, facilities, and processes.

All changes and modifications to the DR/BC Plan shall be documented.

The ISO assigns responsibility for reviewing the DR/BC plan and testing.

Documentation

All Infrastructure and other documentation necessary for successful restoration can be found on the IT SharePoint site. Supporting Documentation includes:

- Business Impact Analysis
- Business Continuity Plan

Disaster Avoidance

The overriding objective is continuity of services. In order to minimize downtime that might result from natural disaster, operational error, negligence, or unintentional consequence, the information systems infrastructure design incorporates numerous preventative and recovery controls to keep systems running optimally and preventing unnecessary downtime. For example:

- Onpoint has elected to place all critical systems in a hosted data center.
  - The Data Center has multiple Internet connections.
  - The Data Center has redundant telecommunications in the form of IP based phones and cellular devices.
  - The Data Center has hot-failover generators connected to provide power during an extended outage.
  - The Data Center has advanced fire detection and suppression equipment.
  - Climate is controlled and monitored by redundant systems.
  - Data center access is controlled via key card and all access is logged and monitored via CCTV.

- All systems are backed up nightly.
- AWS resources have been created with duplicates of all critical services across different availability zones.

Business Impact Analysis

Onpoint conducts a Business Impact Analysis to ensure that the most important business systems and their supporting systems are given priority during the recovery process. This also sets expectations for business units and managers. The Business Impact Analysis is reviewed annually and sooner if needed to address system changes.

Systems are assigned a criticality and sensitivity rating of 1-5, with 5 being the most critical/sensitive. The sum of the two numbers provides the BIA rating. Any acceptable losses are noted here.

The detailed Business Impact Analysis can be found on the IT SharePoint site. The BIA risk score, RTO and RPO along with system dependencies were used to determine the following recovery priorities.

Recovery priorities:

Item #	Information System Name	Notes
Priority 0 – Required Infrastructure		
[redacted]		
Priority 1		
[redacted]		
Priority 2		
[redacted]		
Priority 3		
[redacted]		