POLICY AND PROCEDURE

Policy Name: System Disaster Recovery	**Effective Date: 07/04/2016**
Policy Number: 4005	**Revision Date: 10/26/2018**
Department: IT	**Author: Daniel Mos**

POLICY: UnifyHR follows a strict system disaster recovery protocol in case of natural or human-induced disaster.

PURPOSE: This policy outlines UnifyHR's system disaster recovery protocol that protects UnifyHR's technology infrastructure and systems from a natural or human-induced disaster.

PROCEDURES:

Azure Cloud and Geo-Redundant Storage

The system disaster recovery process relies heavily on many built-in features of the Microsoft Azure cloud. UnifyHR utilizes storage in the Microsoft Azure cloud that is automatically updated in multiple geographic regions in the United States. This is the primary mechanism used in our disaster recovery process. Also, the ability to quickly create server instances in the Azure cloud that are derived from images of the UnifyHR system servers is also utilized.

Disaster Recovery Site

In case the entire production environment goes down, we have a separate disaster recovery location hosted in Microsoft Azure that utilizes geo-redundant storage. This location is in a region distinct from the production environment. This location contains all the functionality of the production environment. The software is maintained to be the current version that exists in the production environment. This site can be activated quickly.

Testing

The disaster recovery site is fully tested on an annual basis. This test is documented.

Roles and Responsibilities

The information technology team is responsible to initiate the disaster recovery process. Multiple team members are responsible for incident response, with one specific team member being designated as on-call at any given time. Once disaster recovery has been activated, all available personal on the disaster recovery team will be engaged to assist with the process.

Incident Response and Plan Activation

The plan may be activated by any member on the disaster Recovery team. The activation occurs after automated system monitoring or UnifyHR personal has notified the team of a service interruption. The disaster recovery process remains in place until normal system functionality has been fully restored, as deemed by operational and information technology leadership.

Uptime Monitoring

The system is continually monitored by an azure server located in a geographic area that is separate from the core system servers. Email alerts are sent to our staff if the system servers cannot be reached or the database appears to be non-functional. The staff will determine if the disaster recovery process needs to be initiated.

Server Recovery

All servers used in the system are created from images that are stored in multiple physical locations. If a server in a data center goes down due to a disaster, the server is re-created in a different geographic location within Azure. Also, the servers themselves are replicated and load balanced across distinct geographic locations. If one data center is subjected to a disaster, the servers residing in the distinct geographic region will still be active.

If the entire production environment goes down, we will fail over to the disaster recovery site. IT staff will redirect the production URLs to point to the disaster recovery site.

Database Recovery

The system database files are written to geo-redundant storage in real time. In the event of a disaster at one Azure location, a backup database server (created using the server recovery process) will be activated to access the system data. The data is also backed up once a day to geo-redundant storage. Two weeks of backup data sets are maintained. This backup data may be restored and utilized in the event of a corruption of the current real-time data. If a database server is down, or the primary data center, the backup database server will be activated within 24 hours.

If the entire production environment goes down, the disaster recovery site will be activated, and the database located in that network will be used.

This policy shall be reviewed for language and application on an annual basis following its last revision and shall be reviewed every year thereafter.

Revision History

Version	Date	Author	Summary of Changes
1.0	12/15/2015	Daniel Mos	Original
1.1	07/05/2017	Daniel Mos	Updates for Improvements/Changes in Process
1.1	07/27/2018	Daniel Mos	Reviewed – No Changes
1.2	10/25/2018	Jennifer Shaub	Added Purpose and Policy Statements
1.2	08/01/2019	Daniel Mos	Reviewed – No Changes

Approvals

Version	Date	Approver	Summary of Changes
1.0	07/04/2016	Chris Heinefield Craig Firestone	Original
1.1	07/05/2017	Chris Heinefield Allen Gehrki	Updates for Improvements/Changes in Process
1.1	07/27/2018	Chris Heinefield	Reviewed – No Changes
1.2	10/26/2018	Daniel Mos	Added Purpose and Policy Statements
1.2	08/01/2019	Daniel Mos	Reviewed – No Changes