Policy Title:	Business Continuation / Disaster Recovery
Source:	Department of Information Technology
Basis:	ISO 17799: 14.1.x Disaster Recovery/Business Continuation
Prepared by:	Aaron Krantz, Vice President of IT & Operations
Approved by:	Aaron Krantz
Effective Date:	August 3, 2015
Replaces:	Updates Previous

INTRODUCTION

It is paramount to the long-term viability of the University that the core business functions, supported by Information Systems resources, be available for day-to-day operations. The focus of this preliminary policy is to list the information systems under the control of the Department of Information Technology and to outline an initial plan to sustain their operation and access.

PURPOSE

The purpose of this policy is to:

- Identify Information Systems assets which are critical to operations.
- Establish a detailed mechanism by which the University can continue to meet defined Business Objectives in the event of a disruption of the availability of these resources.
- Identify the resources necessary to execute and conduct the mechanism of business continuation identified herein.

SCOPE

The scope of this policy includes information systems resources and assets identified as “mission critical” which are presently located at the main campus and supported directly by the Heritage University Information Technology Department.

STATEMENT OF POLICY

MISSION CRITICAL RESOURCES AND FUNCTIONS (supported directly by IT)

1. J1 Student Information System
2. MyHeritage, PowerFaids, JRM
3. Network Infrastructure

4. Active Directory
5. DNS services
6. Email systems
7. Telecommunications
8. Heritage University Web Site
9. File servers
10. Internet Connectivity
11. Fiber Infrastructure

BUSINESS CONTINUATION PLANNING

Core Elements

Servers and network attached disk storage arrays identified as supporting critical systems will be dispersed to locations across campus to minimize the potential that a catastrophe affecting a single building will create a loss of all systems. The second criteria for selecting systems for dispersal will be the capacity of the mechanical server to be virtualized so that it can function as a host for additional Virtual Server Machines.

There are two network operations centers(NOC), one in the Arts and Science Building and the other in the Information Technology building. Both spaces are located on the main campus, are controlled atmosphere locations and physically secured IT spaces.

There are two additional spaces located in Petrie Hall and Simkins that are designed to storing backup data. This is to keep backup data located physically seperated from the production data located in the NOC. These are atmosphere controlled locations with a physically secured IT space.

Rationale

Should an event take place that destroys or disrupts access to either of the two operation center sites (buildings) housing mission critical server systems, the surviving site(s) will not only sustain a number of mission critical systems, but these very systems, already equipped with virtualization software (VMware) will have the capacity to be immediately re-deployed to support the systems lost in the event. We are starting to incorporate the cloud as part of the Disaster Recovery plan.

Primary data backup systems, housed separately from either of the server centers, will provide the ability to immediately restore near-real-time data to the reconstituted systems.

PLAN FOR INDIVIDUAL ASSETS

ASSET: DNS Services

Background

In order to provide continued network access to IT server systems, name resolution via local DNS services must remain operational.

System Operability and Access Continuation

Locally authoritative DNS services are replicated amongst 3 servers that are geographically separated on campus; An auxiliary externally authoritative DNS is provided by State of WA K20.

ASSET: Active Directory Services

Background

Access to network resources cannot be gained without proper authentication to the Domain. ADS servers act as a store for the Domain Schema and provides network authentication (logon) services.

System Operability and Access Continuation

In order to continuously provide network authentication services (logons) a server configured with ADS and global catalog will be continuously maintained at two or more locations on campus. This provides a collateral benefit as the use of multiple AD servers load balances login services.

ASSETS: J1 System

Background

The J1 system constitutes the entire suite of Course Management system modules including financial management, HR, Admissions, Registrar, Financial Aid, Advancement. This system resides in the cloud and is maintained by Jenzabar.

System Operability and Access Continuation

J1 system is located in Dallas, TX at a IBM data center. In the event that destructive event at the main campus, J1 services would continue to be available after restoring the VPN connection to Jenzabar. Jenzabar maintains full backups in the event that something happens to the data center in Dallas TX. They have a secondary data center located on the east coast and would restore services at that location.

ASSET: Heritage University Web Site

Background

The University web site is an important point of contact for the public. In an emergency environment it not only acts as a source of information but its continued operation servers to re-assure students and the public that we are “alive and well”.

System Operability and Access Continuation

This server is hosted offsite in the cloud for business continuity and communication purposes.

ASSET: Internet Connectivity

Background

Internet connectivity is a vital utility that supports numerous services to students, staff and faculty. In an emergency environment it gives us the ability to provide communications to students, the public, and maintain connectivity with our remote sites.

System Operability and Access Continuation

To ensure continued internet connectivity, Heritage University has two separate internet service providers. The PNWG is a full 10Gbps internet connection that provides high speed internet access to students, faculty, and staff. K-20 is a 1Gbps internet pipe that serves as a secondary a high speed internet connection. The K-20 circuit is terminated in the IT building and the PNWG is terminated in Arts and Sciences for physical redundancy. As we rely on cloud services more and more, these two internet circuits are vital to future sustainability.

ASSET: Data Backup Equipment

Background

The IT dept. has implemented a disk-to-disk-to-cloud backup solution.

System Operability and Access Continuation

Various network attached storage arrays are located in separate buildings across campus. Servers are backed up daily to these dedicated data de-duplication devices. Once the backup has completed to the first NAS box, it is than automatically replicated to a second NAS box that is geographically separate from the first. Critical data is also then backed up to the cloud.

ASSET: Network Infrastructure and Telecommunications

Background

Data communications are established by the interconnection of buildings across campus using single mode fiber optic cable and a high-speed core data switch. Voice communications are a mix of digital phones and Voice over IP.

System Operability and Access Continuation

Current

The main campus data core switch is located in the Arts and Sciences building. It currently provides a mix of data transport speeds of 10GBs and 1GBs among buildings. A secondary core switch provides failover redundancy. Additionally, there are two telecommunications switches one located in the Arts and Sciences NOC and a second auxiliary unit in the IT building. In the event of a loss of either system, the other is capable of sustaining telephone communications in a limited capacity until equipment can be replaced or restored. Telephone systems have been virtualized and can be moved to alternative host servers.

ASSET: Email System

Background

Electronic mail has become a core element of enterprise communication. Communication in the time of disaster is a high value asset.

System Operability and Access Continuation

Current

We migrated our email services over to Microsoft O365 cloud in 2023. Email can be accessed from anywhere with an internet connection and staff/faculty mailboxes are backed up.

SUSTAINABILITY

Microsoft has a detailed service level agreement and data protection agreement to provide high availability. No significant interruptions of this system are anticipated however we do maintain daily backups of individual mailboxes.

REVISION HISTORY

Initial policy iteration: April 10, 2007
Revised: February 28, 2011
Revised: May 7, 2012
Revised May 3, 2015
Revised April 5, 2019
Revised June 1, 2024