ADMINISTRATIVE PROCEDURE

Disaster Recovery Plan

PURPOSE

This document establishes the procedures used to guide management and technical staff in the recovery of computing and network facilities operated by Nevada State University (NS) in the event that a disaster destroys all or part of the facilities.

DEFINITION AND SCOPE

Due to the uncertainty regarding the magnitude of any potential disaster on the campus, this plan will only address the recovery of systems under the direct control of NS Information & Technology Services (ITS) and that are critical for business continuity. This includes the following:

- Authentication, single-sign-on, and directory services
- On-premises enterprise applications
- Datacenter (data warehouse, integration servers, file/print services)
- Data networks and telecommunications (wired and wireless networks, telephony)
- Desktop equipment, labs, classrooms

A number of critical services are hosted externally for the university. The recovery of these systems themselves is beyond the scope of this document and the ability of ITS, but this plan will address restoration of connectivity and integration with these services. This includes the following:

- Customer Relationship Management (Anthology Radius)
- Email (Microsoft 365)
- File sharing (Dropbox)
- Finance & HR systems (Workday)
- Learning management system (Instructure Canvas)
- Portal (Unifyed)
- Student information system (PeopleSoft Campus Solutions)
- Website

This plan covers the following phases of technology related disaster recovery:

- Assessment
- Notification
- Response
- Recovery

PROCEDURES

Assumptions

This disaster response and recovery plan is based on the following assumptions:

- The safety of students, faculty, and staff are of primary importance and the safeguard of such will supersede concerns specific to hardware, software, or other recovery needs.

- Depending on the severity of the disaster, other departments/divisions on campus may be required to modify their operations to accommodate changes in system performance, technology availability, and physical location until a full recovery has been completed. Departments are encouraged to have contingency and business continuity plans for their operations, which may include operating without IT systems for an extended period of time.

- The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be determined by the specific Disaster Recovery Teams under the guidance and approval of the Incident Commander and Incident Command Team.

Teams and Responsibilities

Incident Commander (IC) - The Incident Commander leads all efforts during the initial assessment of the incident, in conjunction with the Incident Command Team (ICT). If a disaster is declared, the IC is responsible for overall coordination of all IT related recovery activities. For Nevada State University, the Incident Commander is the Associate Vice President of Information & Technology Services.

Incident Response Team (ICT) - The ICT is a group of IT individuals with combined knowledge and expertise in all aspects of the IT organization. It is the responsibility of the ICT to perform the initial assessment of the damage, to determine if a formal "disaster" declaration is required and to coordinate activities of the various IT Disaster Recovery Teams (DRTs).

Desktop, Lab, and Classroom Recovery Team

The Desktop, Lab, and Classroom Recovery Team is composed of personnel within ITS that support desktop hardware, client applications, classrooms, and labs. The primary function of this group is the restoration of NS's desktop systems, classrooms, and labs to usable condition. During the initial recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer. Nevada State University recommends all users store data files on the file servers, which are backed up nightly, to support data recovery.

Enterprise Systems Recovery Team

The Enterprise Systems Recovery Team is composed of personnel within ITS that support enterprise systems such as email, the learning management system, and student information system. The primary function of this group is the restoration of authentication services, availability, and integration for enterprise systems. This team will coordinate its activities with the Nevada System of Higher Education (NSHE) System Computing Services (SCS), which is responsible for hosting, managing, and supporting PeopleSoft and Workday as well as any vendor who provides hosting services for enterprise systems.

Infrastructure Services Recovery Team
The Infrastructure Services Recovery Team is composed of personnel within ITS that support the university's datacenter and network infrastructure, including Active Directory, DHCP, DNS, file servers, network printing, server virtualization, and wired/wireless Internet connectivity. The primary function of this working group is the restoration of network and server infrastructure to their most recent pre-disaster configuration in cases where data and operational loss is significant. Additionally, this group is responsible for the activation of the secondary datacenter depending on the severity of the disaster. Due to the prerequisite nature of network and server connectivity, this team's role is to restore these systems to a condition where other teams can work on their recovery efforts.

Telecommunications Recovery Team
The Telecommunications Recovery Team is composed of personnel within ITS that support the university's telephone system. The primary function of this working group is the restoration of voice services to the most recent pre-disaster configuration in cases where operational loss is significant.

Data Backup & Recovery Information

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. System backups are governed by the NS Backup & Recovery Policy. Nevada State University does not have systems in place to backup and restore information/data located on individual desktop systems throughout the campus. Only the servers located in the datacenter are backed up; as such, only data resident on these systems will be able to be recovered. In the event that a disaster occurs on the campus which destroys personal computers, the information located on these computers will be extremely difficult or impossible to recover. ITS recommends and encourages the use of cloud-hosted (Dropbox) or network-based (Y: or X:) storage to house all important files. The recovery of data not backed up to these locations are not covered under this plan.

Disaster Recovery Processes and Procedures

Response Initiation
In the event of a disaster that impacts IT services at Nevada State University, initiation of this plan shall commence unless there is severe structural damage to the facility where personal safety is in question or where analysis must be completed to assure the building is acceptable for access. This would include, but is not limited to:

- Damage from a natural disaster such as a flood or earthquake
- Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contamination where the situation must be contained prior to building occupancy
- Flooding or other situations which may pose the risk of electrical shock or other life-threatening situations

Initial Assessment and Notification

The Incident Commander (IC) will gather the Incident Command Team (ICT) to assess the situation and determine the extent of the incident, impacted services, business impact, and users affected. Based on this information, the IC will provide the NS Executive Team with a high-level briefing of the situation.

Incident Command Team Response

Following the initial assessment and notification and throughout the recovery effort, the Incident Command Team shall:

- Identify which areas of the IT infrastructure are affected and contact members of the specific Disaster Recovery Teams.
- Secure all IT facilities involved in the incident to prevent personnel injury and minimize additional hardware/software damage.
- Supervise, coordinate, communicate, and prioritize all recovery activities with all other internal / external agencies.
- Oversee the consolidated IT Disaster Recovery plan and monitor execution.
- Hold regular Disaster Recovery Team meetings/briefings with team leads and designees.
- Appoint and replace members of the individual recovery teams who are absent, disabled, ill, or otherwise unable to participate in the process.
- Provide regular updates to the Executive Team on the status of the recovery effort.
- Approve and acquire recovery resources identified by individual recovery teams.
- Interface with other activities and authorities directly involved in the disaster recovery (University Police, Emergency Management, Fire, etc.)
- Make final determination and assessment as to recovery status, and determine when IT services can resume at a sufficient level.

Disaster Recovery Team Response

The Disaster Recovery Teams are organized to respond to disasters of various type, size, and location. Any or all of these teams may be mobilized depending on the parameters of the disaster. It is the responsibility of the ICT to determine which Disaster Recover Teams to mobilize following the declaration of a disaster.

Each team will utilize their respective procedures, disaster recovery information, technical expertise, and recovery tools to expeditiously and accurately return their systems to operational status. While recovery by multiple teams may be able to occur in parallel, the datacenter and network infrastructure will normally be assigned the highest priority, as full operational recovery of most other systems cannot occur until these areas are operational.

Datacenter Recovery Team Response

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery of datacenter.
3. If the alternate datacenter site is required, execute all necessary steps to notify appropriate personnel and secure backup facility.
4. Identify other individuals required to assist in recovery of datacenter, and report this information to the IC for action.
5. Develop overall recovery plan and schedule, focusing on highest priority servers for specific applications first.

6. Coordinate hardware and software replacements with vendors.
7. Recall backup/recovery data from on campus or off-campus storage, as required to return damaged systems to full performance.
8. Oversee recovery of datacenter based on established priorities.
9. Coordinate datacenter recovery with other recovery efforts on campus.
10. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
11. Verify and certify restoration of the datacenter to pre-disaster functionality.

Desktop, Lab, and Classroom Recovery Team Response

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage at all areas affected, and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of desktop services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure/desktop services first.
5. Coordinate hardware and software replacement with vendors.
6. Oversee recovery of desktop computing services (workstations, printers, etc.) based on established priorities.
7. Coordinate computer recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the desktops to pre-disaster functionality.

Enterprise Systems Recovery Team Response

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery to enterprise systems.
3. Identify other individuals required to assist in recovery of these applications, and report this information to the IC for action.
4. Restore degraded system function inform user community of the restrictions on usage and/or availability.
5. Coordinate recovery with hosting providers as required.
6. Coordinate enterprise systems recovery with other recovery efforts.
7. Execute plan to restore enterprise system services to full function.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of enterprise systems services to pre-disaster functionality.

Infrastructure Services Recovery Team Response

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first.
5. Coordinate hardware and software replacement with vendors

6. Oversee recovery of messaging, telecommunications and infrastructure services based on established priorities.
7. Coordinate messaging, network and web systems recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Messaging, Network and web infrastructure to pre-disaster functionality.

Telecommunications Recovery Team Response

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of these services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first.
5. Coordinate hardware/software replacement with vendor as required.
6. Oversee recovery of voice and infrastructure services based on established priorities.
7. Coordinate the voice and infrastructure services recovery with other recovery efforts.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the voice network to pre-disaster functionality.

Application/System Recovery Priorities

The following is a guideline as to how IT application/system recovery shall be prioritized:

1. Wired network and routing
2. DNS/DHCP services
3. Internet connectivity
4. Datacenter and virtual server environment
5. Authentication and directory services
6. Enterprise Applications
    a. Email
    b. Learning management system
    c. PeopleSoft
    d. Workday
    e. Portal
    f. File sharing
    g. Customer relationship management
7. Web services
8. Data integration services
9. Telecommunications
10. Desktop computing
11. Wireless network

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nevadastate.edu

DEFINITIONS

Backup/Recovery Files - Copies of all software and data located on the central servers, which are used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Disaster Recovery Team - The DRT is a team of individuals with the knowledge and training to recover from a disaster. This includes the desktop, lab, and classroom; enterprise systems; infrastructure services; and telecommunications recovery teams.

Disaster - Any IT incident which is determined to have potential impacts on the business continuity and ongoing operations of Nevada State University.

Crisis Management Team - The CMT is the first to respond to an incident, to secure and contain the situation. The CMT may consist of university personnel, firefighters, police, security, and other specialized individuals.

Incident - Any non-routine event which has the potential of disrupting IT services to Nevada State University. An incident can be a fire, wind storm, significant hardware failure, flood, virus, Trojan horse, etc.

Web Services - All services related to Nevada State University's Internet and intranet web activities and presence. The primary web service provided by the university is the homepage at https://nevadastate.edu and our portal at https://my.nevadastate.edu.

RELATED INFORMATION

HISTORY

Revised 11/17/23