## Overview

As part of the Emergency Preparedness Plan for California State University, Sacramento, Information Resources & Technology (IRT) develops, documents, tests and maintains the Disaster Recovery Plan (DRP). The plan consists of a public facing plan and an internal technical procedures document. The plan helps ensure the recovery of critical university functions, systems, and services when a disruption to university operations occurs after a disaster or emergency. IRT's role in business continuity is to launch our disaster recovery procedures and restore campus services based on business impact assessments. IRT partners with the campus to understand business impact, set recovery priorities, communicate essential information, and manage expectations.

## Definitions

1. **Disaster Recovery Plan:** Internal documents describing how an organization responds to a disaster or emergency to ensure that critical business functions will be restored based on priority and business impact.
2. **Disaster:** An event that disrupts mission-critical business processes and degrades their service levels to a point where the resulting financial and operational impact to an organization becomes unacceptable.
3. **Emergency Operations Center (EOC):** Under the direction of Public Safety, the center that coordinates emergency activities for the university.
4. **IRT Command Center:** A temporary on or off-campus location established by the IRT leadership team for central coordination during disaster recovery.
5. **IRT Leadership Team:** The disaster recovery team responsible for first-line response to any incident. This team assesses and evaluates the incident to determine if the plan should be enacted and provides ongoing communication and status updates to the university. The team is comprised of the Chief Information Officer, the Associate Chief Information Officer, three senior directors, the Information Security Officer, and six IRT directors, who are responsible for leadership within their respective areas.
6. **IRT Disaster Recovery Team Leaders:** The disaster recovery team is responsible for carrying out the tasks and provisions of the Disaster Recovery Plan, including assigning tasks to staff, obtaining remote site data backups, contacting vendors, monitoring work progress, and reporting the status to the IRT leadership team.

## Levels of Disasters and Emergencies

### *Minor Incident*

Minor incidents occur more frequently and the effects are often isolated to a small subset of critical business processes or areas. Business units that depend on these processes can continue to function for a certain duration of time, and the cause is usually the failure of a single component, system, or service.

Examples of this type of incident include the temporary loss of voice communications, phone service, network connectivity, data center servers, portal access, access to cloud-based services, and the IRT Help Desk incident management system.

### *Intermediate Incident*

Intermediate incidents occur less frequently but with greater impact than minor incidents. These incidents impact portions of the university, disrupt normal operations of some but not all critical business units, and generally result from major failures of multiple systems and equipment. At this level of incident, IRT would activate a subset of the plan.

Examples of this type of incident include malfunction of university administrative systems, water intrusion or leakage that displaces or disrupts data center systems and servers, loss of building communications closets, or electrical disruptions that require generated power for longer than 30 minutes.

### *Major Incident*

A major incident has a low probability of occurring, but the event has significant impact. These incidents disrupt normal operation of all critical business processes and involve the inaccessibility or failure of most systems and equipment. Public Safety, or another authorized unit or person, would immediately enact an emergency state and activate the Disaster Recovery Plan.

Examples of this type of incident include fires, floods, earthquakes, and sabotage.

## Plan Information

### *Responsibilities*

This plan will be executed by the IRT Operations and Network Services (ONS) team and, as needed, by Senior Director of Enterprise Systems & Campus Applications and the Information Security Officer.

### *Location of the Plan*

The IRT executive team maintains a confidential hard copy of the Disaster Recovery Plan.

This comprehensive plan is available in electronic format on the IRT internal document server, which is replicated at our disaster recovery (DR) site and in a remote location with designated access for IRT managers and staff.

The public plan will be available on the IRT website.

*Access to this Plan*

The Disaster Recovery Plan contains protected information that should not be shared publicly. It is the responsibility of each IRT sub-unit to ensure that this plan be accessed, developed, and reviewed by designated individuals only.

A version of this plan was modified for public use and does not contain protected information. The plan is available online to assist other divisions with preparation of department and division business continuity plans. The public plan provides the priority sequence for recovering systems, as well as the estimated recovery time for each system. This is valuable planning information for departments as they determine alternate methods of providing critical services immediately following an incident.

*Plan Review*

The Disaster Recovery Plan will be reviewed annually, updated as needed, and reissued if changes occur. Modifications and updates to this plan and related recovery procedures are made throughout the year, if warranted. Responsibility for conducting the annual review resides jointly with the Associate Chief Information Officer, Senior Director of Operations & Network Systems, Senior Director of Enterprise Systems & Campus Applications, and the Information Security Officer. The Chief Information Officer will review and approve plan updates.

## Plan Execution

*Communication*

IRT's confidential emergency call list is maintained by the administrative office. Electronic copies are available to all managers. Printed copies are available from the administrative office.

To ensure rapid communication of disaster recovery status, notifications are distributed in a call tree fashion – senior directors will communicate to directors, directors to their lead technical staff members, and lead technical staff to their respective technical support staff.

*Risk Mitigation*

Loss of the university infrastructure and IRT-managed systems and servers is a critical disruption to campus operations. The loss of data on any IRT-managed systems is an unacceptable risk.

IRT has taken measures to minimize, if not eliminate, this risk and ensure that the infrastructure, systems, and data can be restored in the most expeditious manner.

- Procurement and Contract Services maintains a university-wide insurance policy that will address catastrophic losses.
- IRT maintains a separate insurance policy with CCS that ensures the availability and rapid replacement of equipment at any site designated by the university.
- IRT maintains a third-party contract with Iron Mountain to provide system backups that can be retrieved for restoration on campus or can be restored anytime, anywhere through the use of cloud computing.
- IRT is backing up important university services from the data center to cloud-based services, thereby improving availability from remote locations and decreasing the potential loss of services due to campus-based incidents.

## Redundancy, Alternative Sites, and Backup Strategy

*Redundancy*

IRT's IT infrastructure has been designed with redundancy in several areas, including network feed, network fiber distribution, and power source. The double-star configuration, coupled with two campus connections to the CENIC network (North and South), and the onsite generator, allow a certain degree of independence for minor network and power outages.

*Alternative Sites*

The basic infrastructure on campus has been replicated at a designated disaster recovery (DR) site to achieve faster recovery time of critical systems. These systems include:

1. Critical Infrastructure Services:
    a. Network Connectivity, Internet Service
    b. Storage and Virtual server infrastructure
    c. Local storage U:\, N:\, P:\ file shares (Sacfiles shared departmental folders)
    d. AD, ADFS, CAS, Shibboleth, CAS
    e. Remote connectivity and VPN services for technical staff
    f. Data Backup/Restoration systems, i.e., CommVault

2. Critical Application Services:
    a. Database Services
        i. Oracle Catalog and Grid servers
        ii. MS SQL database servers
    b. Campus web server and portal, CMS, CFS and Student Center
    c. Access to Cloud Services:
        i. Office365 : OneDrive storage, SharePoint sites, Exchange e-mail services
        ii. LMS system: Canvas

*Backup Strategy*

Server and application backups are performed daily and stored at a remote site though a contract with a third-party vendor, Iron Mountain. The vendor picks up and stores the tapes on a weekly basis.

The greatest gap between last tape pick up and a disaster could be a 7-day window. This information has been shared with campus business units.

*Service Restoration*

Recovery of all systems is critical. However, restoration requires that some systems be restored in a specific sequential order. All systems cannot be restored simultaneously. Therefore, IRT has evaluated and prioritized the system recovery sequence for those systems based on the current infrastructure configuration.

The restoration priority is determined by the business impact on the university and the period of time that departments can sustain their own operations using the alternate methods described in their divisional business continuity plans.

The following prioritized system list is available to assist departments with preparation of their department business continuity plans. The systems include intervals of time where campus units will need to use alternate methods of conducting routine business processes.

**Priority 1:**

*Priority 1 includes all of the hardware, software, minor cable, and wiring required to re-establish the campus network and telecommunications infrastructure.*

| Priority 1 | |
|---|---|
| System | Estimated Time to Recovery |
| Internet access | 24 hours at DR site<br>40 days for new equipment |
| Storage & VMware Infrastructure | 24 hours using DR site<br>40 days for addition of new equipment |
| Authentication and authorization systems: AD, ADFS, CAS, Shibboleth | 24 hours using DR site<br>40 days for new equipment installation |
| Remote connectivity and VPN services for users | 24 Hours using DR site<br>40 days for addition of new equipment |
| Data Backup/Restoration systems, i.e., CommVault | 24 hours using DR site<br>40 days for addition of new equipment |

**Priority 2: Critical Application Services**

*Priority 2 includes the servers that support and secure the infrastructure, grant access to the infrastructure and services, and establish communications. Examples include identity management, web servers, and One Card. Complete restoration can run between 2 days and 60 days depending upon the system and whether the equipment is available or must be reordered.*

| Priority 2 | |
|---|---|
| System | Estimated Time to Recovery |
| Campus storage drives, personal, departmental, project drives: U:\, N:\, P:\ | 24 hours using DR site<br>40 days for new equipment installation |
| Database Services<br>Oracle Catalog and Grid servers<br>MS SQL database servers | 24 hours using DR site<br>40 days for new equipment installation |
| Campus web server and portal, CMS, CFS, and Student center | 24 hours using DR site<br>40 days for new equipment installation |
| Office365: OneDrive, SharePoint, Email for Students, Faculty, and Staff | Service is hosted in the cloud and will not be affected by a campus incident.<br>Access is dependent on availability of Priority 1 authentication and authorization systems. |

**Priority 3**

| Priority 3 | |
|---|---|
| System<br>Campus Application Servers | Estimated Time to Recovery<br>60 days for addition of new |

**Auxiliary Data Restorations**

| Auxiliaries | |
|---|---|
| System | Estimated Time to Recovery |
| UEI | 24 hours using DR site<br>40 days for new equipment installation |
| ASI | 24 hours using DR site<br>40 days for new equipment installation |
| UU/The Well | 24 hours using DR site<br>40 days for new equipment installation |

Contacts and Resources

a) For questions regarding hardware, infrastructure, or this document, contact the Senior Director of ONS.

b) For questions regarding Enterprise Applications, contact the Senior Director of Enterprise Systems & Campus Applications.

c) For questions regarding the University website, contact the Director of Web & Mobile Services.

d) For questions regarding the University LMS, contact the Director of Academic Technology Services.

**Reference and Recovery Documents**

All procedures, contracts, and other confidential documents necessary for technical disaster recovery are stored in multiple locations accessible anytime, anywhere by the IRT leadership team and team leaders.

All recovery documents are routinely reviewed, updated, and uploaded to the onsite and remote document storage facilities.