Disaster Recovery Plan for Information Technology Services	Document No.	ITS-7502-Web	Rev:	E
	Owner:	IT Infrastructure Services Enterprise Applications		
	Approved by:	Tosha Pham, Associate Vice President Information Technology Services		
	Issued:	2-24-11	Revised:	6-26-17
				Page 1 of 12

Table of Contents

1 Purpose

As part of the Cal State LA Emergency Preparedness Plan, Information Technology Services (ITS) develops, documents, tests and maintains the *ITS-7502 ITS Technical Disaster Recovery Plan*. The disaster recovery plan ensures the recovery of critical ITS University functions, systems and services when a disruption to University operations occurs after a disaster or emergency situation.

2 Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8085.0	**Policy**	**Business Continuity and Disaster Recovery**
EO 1014	Executive Order	Business Continuity Program

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3 Entities Affected by this Document

Disaster recovery and business continuity processes are the responsibility of all Information Technology Services employees.

4 Definitions

a. Business Continuity Plan (BCP): A document describing how an organization responds to an event to ensure critical business functions continue to be provided without unacceptable delay or change.

b. 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.

c. Disaster Recovery Plan (DRP): A technical document describing how an organization restores critical technology and business systems following an outage or disaster.

d. Emergency Operations Center (EOC): Under the direction of Public Safety, the center that coordinates emergency activities for the University.

e. ITS Command Center: A temporary on or off-campus location established by the ITS management team for central coordination during disaster recovery.

f. ITS Management Team: The disaster recovery team responsible for first-line response to any incident, for assessing and evaluating the incident to determine if the ITS Technical Disaster Recovery Plan should be enacted and providing communications and status updates to the University. The team is comprised of the associate vice president and four ITS directors who are responsible for leadership within their respective areas.

g. ITS Team Leaders: The disaster recovery team responsible for carrying out the tasks and provisions of the ITS Technical Disaster Recovery Plan including assigning tasks to staff, obtaining remote site data backups, contacting vendors, monitoring work progress and reporting the status to the ITS management team. The team is comprised of all ITS assistant directors, associate directors and managers.

5 Levels of Disasters and Emergencies

Cal State L.A. Public Safety has classified disasters and emergencies into three levels – minor, intermediate and major.

5.1 Minor State

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 include the temporary loss of voice communications; network connectivity; data center servers; portal access; access to cloud-based services; and the ITS Help Desk incident management system, switchboard or telephone service.

5.2 Intermediate State

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. ITS would activate a subset of the ITS disaster recovery plans.

Examples 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.

5.3 Major State

Major incidents have a low possibility of occurring, but the extent has significant impact. These incidents disrupt normal operation of all critical business processes and involve the inaccessibility or failure of most systems and equipment. ITS would immediately enact an emergency state and activate the ITS disaster recovery plans.

Examples include fires, floods, earthquakes and sabotage.

6 General Information

6.1 Responsibilities

This plan will be executed by the IT Infrastructure Services unit and, as appropriate, by the Enterprise Applications department.

6.2 Location of the Plans

a) The Information Technology Services office maintains a confidential hard copy of *ITS-9507 Management Disaster Preparedness Plan*, *ITS-7502 ITS Technical Disaster Recovery Plan* and *ITS-9506 Internal Business Continuity Plan*.

b) *ITS-7502 ITS Technical Disaster Recovery Plan* and *ITS-9506 Internal Business Continuity Plan* are available in electronic format on the ITS emergency document server, emergency laptops, SharePoint and multiple off-site locations for designated ITS managers and staff.

c) Modified versions that do not contain confidential information, *ITS-7502-Web Disaster Recovery Plan for ITS* and *ITS-9506-Web Business Continuity Plan for ITS,* are available on the IT Security and Compliance website under Guidelines, Standards and Laws > Business Continuity Management.

6.3 Access to this Plan

The technical disaster recovery plan contains protected information that **should not** be shared publicly. It is the responsibility of each ITS department to ensure that these plans be held, developed and reviewed by designated individuals only.

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

6.4 Review of this Plan

This plan will be reviewed annually, and updated and reissued if changes occur. Modifications and updates to this disaster recovery plan and related recovery procedures are made throughout the year, if warranted. Responsibility for conducting the annual review resides jointly with the associate vice president for Information Technology Services and the directors of IT Security and Compliance, IT Infrastructure Services, Enterprise Applications and Client Support Services.

6.5 Call Tree Assignments

The division's confidential emergency call list is maintained by the ITS office. Copies are available electronically to ITS managers on the ITS emergency server, their emergency laptops and cell phones, SharePoint Public Folders and multiple off-site locations. An electronic version of this emergency contact list is also electronically synced to all ITS managers' cell phones. Printed copies are available from the ITS office.

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

6 Disaster Recovery Planning

6.1 Risk Assessment

Loss of the University infrastructure and ITS-managed systems and servers is a critical disruption to campus operations but the loss of data on any ITS-managed systems is an unacceptable risk. ITS has taken a four-prong approach to minimize, if not eliminate, this risk and ensure that the infrastructure, systems and data can be restored in the most expeditious manner.

a) The office of Risk Management and Environmental, Health and Safety office maintains a University-wide insurance policy on all technology equipment. In the event a disaster destroys equipment housed in the data center or Administration building, or peripheral equipment supporting these areas, the insurance policy ensures that funding is available to replace damaged equipment.

b) ITS maintains a separate insurance policy with El Camino Resources that ensures the availability and rapid replacement of equipment at any site designated by the University.

c) ITS maintains a third-party contract to provide comprehensive system backups that can be retrieved for restoration on campus or can be restored anytime, anywhere through the use of cloud computing.

d) ITS is moving 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.

6.2 Alternate Sites and Backup Strategy

ITS has evaluated the use of alternate sites for disaster recovery and has determined that pre-established alternative sites create unacceptable risk for the University.

Technology disasters routinely occur on a small scale – a local power failure, equipment failure or a broken water pipe – that allows ITS to test its disaster recovery plan on an isolated basis. Major disaster preparation in California generally tends to surround earthquake preparedness in part fueled by a 2008 report by the U.S. Geological Survey that examined the effects of a 7.8 earthquake on the San Andreas Fault. As a follow-up to that report, a team of scientists, engineers and emergency planners simulated the effects of a megastorm (based on a 45-day series of storms) on the state. The resulting floods, landslides, power outages, and water and sewage damage would potentially require months to restore. The common denominator of these events is the probability that the alternate site would be affected by the disaster and recovery would at best be delayed or at worst impossible to execute.

6.2.1 Cloud Computing

6.2.1.1 System Backups

ITS has contracted with a third-party service provider to use their fully managed cloud computing backup service. This service provides the University the flexibility during a major disaster to restore to whatever available site is chosen, thus eliminating the cost of deploying and maintaining an alternate site. This solution reduces recovery risk by providing an automated data protection service that is recoverable any time, from anywhere. Some advantages over re-establishing services at an alternate site include:

- Fully automated offsite data protection that provides speed and reliability in backup and recovery operations with little or no ITS intervention.
- Continuous back-ups and mirrored data centers, which minimizes the possibility of missing data gaps between the last tape backup and the disaster.
- Reliable recovery through a web portal that is accessible anytime, anywhere.
- The burden of managing secondary storage is transferred to a third-party, technology-enabled service provider, and that eliminates the costs of deploying and maintaining a complex disaster recovery site.
- Data is encrypted at the source, in transit and in storage using 256-bit AES encryption, and data is mirrored and stored in a secure underground storage facility.
- Restoration backup data supports compliance and governance purposes where proving the authenticity of the data or preserving it for civil litigation cases and eDiscovery is critical.

6.2.1.2 Email Service

ITS utilizes Microsoft Office 365 for cloud-hosted email service. This solution reduces risk by providing email software as a service, which is replicated at multiple data centers within the United States. Email will not be affected by a campus incident, and should an external event affect any single cloud-hosted server or location, service will be immediately switched to another remote location.

6.2.1.3 Website Hosting

The University's main websites are hosted by a Drupal-based service, with very few webpages remaining on the local data center web servers. Websites that have already migrated to the cloud-based environment will not be affected by a campus incident. The Library remains on the local server and will continue to be local for the immediate future..

6.3 Restoration Priority

Recovery of all systems is critical, however, some systems must be restored in a specific sequential order and all systems cannot be restored simultaneously. Therefore, ITS has evaluated and prioritized the system recovery sequence for those systems in the data center and switchroom. 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.

- Priority 1 includes all the hardware, software, minor cable and wiring required to re-establish the campus network and telecommunications infrastructure. Restoration of major wiring in the buildings and between buildings is covered in the *Cal State L.A. Multihazard Emergency Plan 2010-2011*. Complete restoration can run between 7 hours and 90 days depending upon the extent of damage and whether the equipment is available or must be reordered.
- 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, One Card and the like. 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 3 includes the servers managed by the ITS division that support applications used by all University departments. Examples include departmental application servers, instructional servers, document storage servers and other non-enterprise servers. Complete restoration can run between 2 days and 48 days depending upon the system and whether the equipment is available or must be reordered.

The following prioritized system list is available to assist departments with preparation of their department business continuity plans by indicating the intervals during which they will need to use alternate methods of conducting routine business processes.

Priority 1	
System	**Estimated Time to Recovery**
Minor wiring repairs	14 days if cable and termination equipment is available 30 to 90 days if unavailable
Telephone PBX	30 days *Note: Alternative voice communications methods will be deployed to critical areas.*
Telephone Satellite System	1-2 hours for handhelds 32 days for hard-wired phones
Network Distribution and Access Layer Infrastructure	3 days if equipment is available 30 days if equipment is unavailable
Network Core, Internet	10 days
Legacy Infrastructure	6 plus days
Domain Controllers *****	12 hours if equipment is available 33 days if equipment is unavailable
Network Access Control servers (used to authenticate users to the network)	4 days if equipment is available
Identity Management Servers (used to support authentication services) *****	4 days if equipment is available
VMware Servers	3 days if equipment is available 33 days if equipment is unavailable
NSM Servers (firewall systems)	2 days if equipment is available 32 days if equipment is unavailable
Log Management System	7 hours if equipment is available 32 days if equipment is unavailable

***** These critical servers provide authentication services to systems requiring user authentication for access. If unavailable, users will be unable to access any systems that require user sign-on until Priority 1 restoration is completed.

Priority 2	
System	**Estimated Time to Recovery**
Email for Students, Faculty and Staff	Service is hosted in the cloud and will not be affected by a campus event. Access is dependent on availability of Priority 1 local Exchange servers and authentication servers.
Web Server – University-hosted (includes Library) Web Server – Cloud-hosted	2 days if equipment is available Up to 48 days if equipment is unavailable Service is hosted in the cloud and will not be affected by a campus event.
MyCalStateLA Portal	Service is hosted in the cloud and will not be affected by a campus event. Access is dependent on availability of Priority 1 authentication servers.
One Card	14 days
Voice Mail System	15 days
Call Accounting System	8 days
NetBackup Server	4 days if equipment is available 44 days if equipment is unavailable
DNS Server	2 days if equipment is available 31 days if equipment is unavailable
DHCP Server	2 days if equipment is available 31 days if equipment is unavailable
File Servers	7 days if equipment is available 38 days if equipment is unavailable
Front-end Servers for Student Administration and Human Resources Management	2 days if equipment is available 32 days if equipment is unavailable

Priority 3	
System	**Estimated Time to Recovery**
SharePoint Servers	2 days if equipment is available 32 to 48 days if equipment is unavailable
License Servers for desktop images	2 days if equipment is available 32-48 days if equipment is unavailable
List Serve Server	4 days if equipment is available 34 days if equipment is unavailable
Instructional Server	4 days if equipment is available 32 to 48 days if equipment is unavailable
UAS Payroll Server	4 days if equipment is available 32 days if equipment is unavailable
ITS Help Desk Incident Management System	Service is hosted remotely and will not be affected by a campus event. Access is dependent on availability of Priority 1 authentication servers.
Moodle Server	Service is hosted at CSU Fullerton and will not be affected by a campus event. Access is dependent on availability of Priority 1 authentication servers.
Application Servers	14 days if equipment is available 48 days if equipment is unavailable

Note: The estimated recovery times stated above are for the designated system only and do not represent the sequential dependency of system recovery or the estimated time to restore all systems to a full operational state.

6.4 Joint Vendor, Department and ITS Restorations

Some servers located in the data center require restoration assistance from the associated vendor and/or the responsible department. The following servers, all priority 3 restorations, are in this category.

Department Contact	Application
Academic Affairs	File/print
Administrative Technology	Reprographics
	StarRez (Housing)
	Monitoring
	File/print
	Print
	SecureDoc imaging system
Engineering, Computer Science and Technology	Instructional
	Instructional
Student Health Center	Health Center system
Institutional Advancement	Alumni Call Center
Library	Library system
	File/print
	Library system
Student Life	OnBase
	Career Center
	File/print

7 Contacts and Resources

a) For questions regarding hardware, infrastructure or this document, contact the director, IT Infrastructure Services or the assistant director, Network Operations Center, Servers and Technology Operations.

b) For questions regarding Enterprise Applications, contact the director, Enterprise Applications.

c) For questions regarding the University website, University portal and client support services, contact the director, IT Client Support Services

d) For questions regarding *ITS-9506-Web Business Continuity Plan for Information Technology Services*, contact the director, IT Security and Compliance: itsecurity@calstatela.edu.

8 Reference and Recovery Documents

All procedures, diagrams, schemas, contracts and other confidential documents necessary for technical disaster recovery are stored in multiple locations accessible anytime, anywhere by all ITS management team members and ITS team leaders. All recovery documents are routinely reviewed, updated and uploaded to the onsite and remote document storage facilities, and are synced to all ITS team members' emergency laptop computers.