ITS Technical Disaster Recovery Plan				
	Document No	ITS-7502	Rev	H
	Owner	IT Infrastructure Services Enterprise Applications		
	Approved by	Tosha Pham, CIO / Associate Vice President, ITS		
	Issued	2-24-11	Revised	9-29-21
				Page 1 of 101

Table of Contents

1. Purpose 2
2. Related California State University Policies and Standards 2
3. Entities Affected by These Guidelines 2
4. Definitions 2
5. General Information 3
   - 5.1 Responsibilities 3
   - 5.2 Location of the Plans 3
   - 5.3 Access to this Plan 3
   - 5.4 Review of this Plan 4
   - 5.5 Call Tree Assignments 4
6. Disaster Recovery Planning 5
   - 6.1 Risk Assessment 5
   - 6.2 Alternate Physical Sites and Backup Strategy 5
     - 6.2.1 Cloud Computing 6
   - 6.3 Restoration Priority 7
   - 6.4 Joint Vendor, Department and ITS Restorations 11
7. Tasks and Procedures 12
   - 7.1 Immediate Response 12
     - 7.1.1 Receipt of Disaster Notification 12
     - 7.1.2 Proceed with Critical Notifications 12
     - 7.1.3 Activate Team and Relocate to Recovery Center 13
   - 7.2 Environmental Restoration 15
     - 7.2.1 Prepare Recovery Location 15
   - 7.3 Functional Restoration 16
     - 7.3.1 Prioritize Critical ITS Systems 16
     - 7.3.2 Voice Communications Restoration 18
     - 7.3.3 Data Communications Restoration 30
     - 7.3.4 Operating Systems Restoration 40
     - 7.3.5 Network Systems Restoration 48
     - 7.3.6 Web Systems Restoration 79
     - 7.3.7 Applications Restoration 81
   - 7.4 Verify Functionality 93
   - 7.5 Recovery of ITS Services 94
   - 7.6 Return to Home Site 95
     - 7.6.1 Prepare to Return to Home Site 95
     - 7.6.2 Organize Backup Material for Home Site 96
     - 7.6.3 Test and Return the Data Center to the Home Site 96
8. Contacts and Resources 97
9. Reference and Recovery Documents 97

1. Purpose

As part of the Cal State LA Emergency Preparedness Plan, Information Technology Services (ITS) develops, documents, tests and maintains this *ITS-7502 ITS Technical Disaster Recovery Plan*. The disaster recovery plan ensures the recovery of critical ITS campus functions, systems and services when a disruption to campus operations occurs after a disaster or emergency. This document is used to record key information within ITS in order to ensure the ability to recover from a disruption.

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
ICSUAM 08085.00	**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 These Guidelines

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 campus.

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 campus. The team is comprised of the CIO / associate vice president and five 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, assistant directors and managers.

5. General Information

5.1 Responsibilities

This plan will be executed by the ITS Management Team.

5.2 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 management server, emergency laptops, SharePoint and multiple off-line copies 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.

5.3 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.

ITS publishes *ITS-7502-Web Disaster Recovery Plan for Information Technology Services*, which has been modified for web publication and does not contain any confidential or proprietary information. It 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.

5.4 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 CIO / associate vice president for Information Technology Services and directors of IT Security and Compliance, IT Infrastructure Services, Enterprise Applications, and Client Support Services.

5.5 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 Document Management server, their emergency laptops and cell phones, SharePoint 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.

5.6 Emergency Communications Plan

Emergency Communications

An emergency communications plan creates procedures and establishes resources for distributing information appropriately in a timely, accurate, responsible, and sensitive manner to students, faculty, staff, stakeholders, and the general public during a crisis situation. Actions will depend on the type of crisis and the level of response needed.

1. Event coordination
    a. Forming a communications recovery team.
    b. Developing a process to communicate with employees for safety and well-being and for making them aware of decisions and expectations.
    c. Developing a process to make sure all external stakeholders are aware of decisions and expectations as management deem appropriate.
    d. Managing customer and key vendor communications.

e. Preparing a media communications plan.
f. Ensuring a communication system exists with redundancies for communication.

2. Internal and External Communicatoins
   a. ServiceNow
   b. Email
   c. Phone
   d. Conference Calls
   e. Plan
   f. Hourly Updates

6. Disaster Recovery Planning

6.1 Risk Assessment

Loss of the campus infrastructure, ITS-managed systems and/or 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 CCS Disaster Recovery Services. CCS Disaster Recovery Services 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 has moved and continues to move critical campus services from the data center to cloud-based services, thereby improving availability from remote locations and decreasing the time for potential loss of services due to campus-based incidents.

6.2 Alternate Physical Sites and Backup Strategy

ITS has evaluated the use of alternate physical 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 physical 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, 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 Endpoint Backups & Restore for business crucial users

ITS utilizes a cloud computing continuous backup and restore service for business crucial desktops and laptops. This service provides real time file backup and file restoration services for computers to ensure files are recoverable to replacement equipment as quickly as possible due to hardware failure, malware, system corruption, human error and disaster. This solution reduces recovery time by providing an automated data protection service that is recoverable any time, from anywhere, when internet connectivity is available.

6.2.1.3 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, but access is dependent upon availability of Priority 1 authentication servers. Should an external event affect any single cloud-hosted server or location, service will be immediately switched to another remote location.

6.2.1.4 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 but access to edit webpages is dependent upon availability of Priority 1 authentication servers.

6.3 Recovery Objectives & 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 switch room. The restoration priority is determined by the business impact on the campus 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, major cabling in and between buildings and minor cable and wiring required to re-establish the campus network and telecommunications infrastructure. Complete restoration can run between 7 hours and 90 days depending upon the extent of damage and whether the equipment and cabling is available or must be purchased.
- **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 servers, web servers, One Card and the like. Complete restoration of Priority 2 can run between 2 days and 60 days depending upon the system and whether the equipment is available or must be purchased.
- **Priority 3** includes the servers managed by the ITS division that support applications used by all campus departments. Examples include departmental application servers, instructional servers, document storage servers and other non-enterprise servers. Complete restoration of Priority 3 can

run between 2 days and 48 days depending upon the system and whether the equipment is available or must be purchased.

A comprehensive prioritized system list and the estimated time required for full recovery is stored on the ITS Emergency Document Management server, emergency laptops and SharePoint. A general prioritized system list is available online in *ITS-7502-Web Disaster Recovery Plan for Information Technology Services*, to assist campus 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**
Major building cable replacement	30 to 90 days Note: Requires collaboration between Facilities, Planning and Construction and external agencies to install replacement building cabling.
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 are outlined in *ITS-9506 Internal Business Continuity Plan*.
Telephone Satellite System	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 (includes AD and LDAP and MFA servers) *	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
IDP servers (used to run Shibboleth services for authentication)	4 days, if equipment is available

Priority 1	
System	**Estimated Time to Recovery**
Identity Management System (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
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
Palo Alto (firewall systems)	2 days if equipment is available 32 to 48 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	Email service is hosted in the cloud and authentication occurs against Azure Active Directory in the cloud so email will not be affected by a campus event.
Web Server – Campus-hosted	2 days if equipment is available Up to 48 days if equipment is unavailable
Web Server – Drupal-hosted	Service is hosted in the cloud, but access is dependent upon availability of Priority 1 authentication servers.
MyCalStateLA Portal (SharePoint)	Service is hosted in the cloud, but access is dependent upon availability of Priority 1 authentication servers.

Priority 2	
System	**Estimated Time to Recovery**
MFA Services (Duo)	Service is hosted in the cloud, but access is dependent upon 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
File Servers	7 days if equipment is available 38 days if equipment is unavailable
Help Desk Call Center (CxEngage)	1 day; Service is hosted in the cloud, but access is dependent on availability of a workstation and a headset for each agent in order to accept calls.
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 to 48 days if equipment is unavailable
Listserve Server	4 days if equipment is available 34 days if equipment is unavailable
IT Service Management (ITSM) ServiceNow System	Service is hosted remotely and will not be affected by a campus event.

Priority 3	
System	**Estimated Time to Recovery**
	Access is dependent on availability of Priority 1 authentication services.
Canvas Learning Management System	Service is hosted by Instructure and will not be affected by a campus event. Access is dependent on availability of Priority 1 authentication servers.
GETmobile	Service is hosted by Ready Education 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
	OnBase
Administrative Technology	Reprographics
	Monitoring
	File/print
	Print
	SecureDoc imaging system
Engineering, Computer Science and Technology	Instructional

Department Contact	Application
Student Health Center	Health Center system
University Advancement	Alumni Call Center
Library	Library system
	File/print

7. Tasks and Procedures

7.1 Immediate Response

7.1.1 Receipt of Disaster Notification

The ITS management team is responsible for the following actions.

Step	Task	Description	Completed By	Date / Time
1.	Receive notification of a major disaster declaration from the Public Safety **OR** Receive notification of a local disaster from affected ITS unit.	The ITS management team will contact ITS team leaders as soon as possible to communicate key information about the disaster declaration.		
2.	Receive recovery location from ITS or Public Safety.	The ITS management team will inform the ITS team leader about alternate site or recovery location information if the ITS office is physically damaged and cannot be used as the ITS Command Center.		

7.1.2 Proceed with Critical Notifications

The ITS team leaders are responsible for the following actions.

Step	Task	Description	Completed By	Date / Time
1.	Call VEEAM to obtain offsite vital records necessary for this team.	Call VEEAM and place a request for a bulk retrieval of offsite data via appliance.		

2.	Call CCS Disaster Recovery Services to notify them of the disaster and have equipment delivered.	Verify equipment needed and contract with CCS Disaster Recovery Services. Have CCS Disaster Recovery Services deliver equipment to the alternate recovery site.		
3.	Notify other key vendors.	Using the Vendor Contact List on the ITS Emergency Document Management server, contact any other vendors that need to deliver equipment, supplies or services to the alternate site.		

7.1.3 Activate Team and Relocate to Recovery Center

ITS team leaders are responsible for the following actions.

Step	Task	Description	Completed By	Date / Time
1.	Use the Fan-out Call Tree to call and activate the disaster recovery team.	Call the team, brief them on the incident and determine when and where the team should meet for a briefing if the ITS office is physically damaged and cannot be used as the ITS Command Center.		
2.	Conduct initial briefing for the team.	Once the team is assembled, brief them on the disaster and determine who is and is not available. Identify staffing and equipment resource needs.		
3.	Remind employees that they are NOT to make any media statements.	Staff should refer any media representatives to the campus Public Information Officer (PIO), the executive director for the Office of Communications and Public Affairs.		

Step	Task	Description	Completed By	Date / Time
4.	Aid in damage assessment, if required.	It may be necessary to participate in the initial damage assessment, if requested to do so by the campus Emergency Operations Center If requested to perform damage assessment, use ITS Data Center Diagram Spreadsheet and the ITS Data Center Diagram Visio documents on the ITS Emergency Document Management server.		
5.	Deploy appropriate employees to the alternate site.	Schedule staff for full coverage at the identified alternate site. If the alternate site is geographically distant, perform the following for each person who will travel: • Record the time the person will be ready to travel. • Arrange transportation to the departure point, if necessary. • Discuss any special requirements such as dietary restrictions, child/spouse/elder/animal care, medical treatment, etc. • Coordinate with the ITS Command Center to prepare a University travel allowance form and provide emergency funding, if necessary.		
6.	Document staff location during the disaster incident.	Report to the ITS management team on staff locations. Since staff may not be on campus when the disaster occurs, record the location and phone number where they can be reached for instructions.		

Step	Task	Description	Completed By	Date / Time
7.	Maintain record of team expenses	Instruct all employees to complete form *ITS-9804 Disaster Recovery Cash Expense Log* to record financial expenditures for purchases and expenses during the recovery time period. The ITS fiscal manager will be the designee responsible for collecting the employee expense documents.		
8.	Document employee hours worked or missed during disaster recovery.	Instruct all employees to use form *ITS-9805 Disaster Recovery Employee Hours Log* to record hours worked and jobs assigned during the disaster recovery.		
9.	Confirm recovery status and decisions with the ITS management team.	The team leader is to prepare *ITS-9807 Disaster Recovery Situation Status Report* indicating recovery plans and submit to the designated ITS management director.		

7.2 Environmental Restoration

Prepare the recovery location by ensuring appropriate facility setup.

7.2.1 Prepare Recovery Location

ITS team leaders are responsible for the following actions.

Step	Task	Description	Completed By	Date / Time
1.	Confirm alternate site requirements.	This is the site for system recovery. Confirm alternate site location requirements such as electrical, cooling, etc.		
2.	Verify security at alternate site.	Ensure that vital records, sensitive data, negotiable instruments, etc., will be adequately protected at the alternate site.		

Step	Task	Description	Completed By	Date / Time
3.	Receive and set up equipment from CCS Disaster Recovery Services.	Verify that necessary resource requirements will be delivered to the recovery location.		
4.	Receive offsite storage media and vital records from VEEAM.	Inventory and organize materials received from VEEAM.		
5.	Inform vendors of alternate business location.	Notify vendors of alternate business location. Reference the list of vendor information maintained for earlier disaster notification.		
6.	Order necessary documentation manuals.	Gather necessary documentation manuals from on-site, off-site and vendor inventory locations.		

7.3 Functional Restoration

7.3.1 Prioritize Critical ITS Systems

ITS team leaders are responsible for the following actions.

Step	Task	Description	Completed By	Date / Time
1.	Review and prioritize affected critical ITS systems.	Verify critical ITS functions as defined in the *Server Resource Sheet by Function*, located on the ITS Emergency Document Management server and SharePoint. Review recovery priorities with the ITS management team.		

2.	Evaluate ITS business operations to determine if the business continuity plan must also be initiated.	Verify the impact on Priority 1 (Critical and Urgent) ITS business processes as defined in *ITS-9506 Internal Business Continuity Plan*, located on the ITS Emergency Document Management server. Assign a secondary team of employees to business continuity tasks that will be undertaken concurrently with disaster recovery tasks.		
3.	Determine financial needs and obtain funding.	Evaluate additional resource needs and request funding from the ITS management team.		

7.3.2 Voice Communications Restoration

7.3.2.1 Telephone PBX System

Platform:	**Telephone PBX System**	**Location:**	**ADM 5**
Virtual / Physical:	**Physical**		
Description/Applications:			
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**30 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Quick ship and install		

Recovery Tasks			
Scenario:	**Loss of the primary switchroom or PBX**	**Recovery Location:**	**TBD based upon scope of the incident.**

Step	Task Detail	Est Time	Dependency	Team
If the PBX is Inoperable				
1.	Contact the PBX maintenance vendor, Black Box, to explain the disaster and open a trouble ticket. Describe the situation and provide our customer number 1477.		Existing telephone cabling must be intact.	ITS Telecom
2.	Contact AT&T to: 1. Request vendor implement a message with approved disaster information on campus pilot number 323-343-3000. Public Affairs must pre-approve the message. 2. Move the current T1 circuits from ADM 5A to the new PBX location or establish new voice circuits at the new PBX location.	1 day 7 to 10 days	Approval of disaster information message. Identification of alternate site. Receipt of new PBX, if required.	ITS Telecom

3.	If AT&T telecommunications services are unavailable, move the Sprint long distance overflow circuit from ADM 5A to the new PBX location.	7 to 10 days	Identification of alternate site. Receipt of new PBX, if required.	ITS Telecom
4.	Contact AT&T to build a new managed business line for the Child Care Center from the PBX to the new location that the center will identify.	7 to 10 days	Identification of alternate site. Receipt of new PBX, if required.	ITS Telecom
Emergency PBX Hardware and Communication Lines Installation				
1.	Contact Black Box to order a small PBX to bring up minimal phone service.	5 to 10 days	Existing telephone cabling must be intact. Receipt of auxiliary equipment. Prioritized list of name and location of individuals who will be provided minimal phone service.	ITS Telecom
2.	If recovering at a University building other than the Administration building, order needed auxiliary equipment: 110 blocks, cables, phones, wall jacks, etc.	5 to 10 days	None.	ITS Telecom
3.	Coordinate with Black Box technicians to connect the primary AT&T or the backup Sprint circuit(s) to the emergency PBX hardware.	10 to 14 days	Receipt of the new PBX.	ITS Telecom & Black Box
4.	Schedule the technician to punch down the wire pairs to critical extensions.	1 day	Receipt of the new PBX. Installation of auxiliary equipment.	ITS Telecom & Black Box
Emergency PBX Software Installation				
1.	Install PBX Software.	2 days	Receipt of the new PBX. Back up copy of the campus phone configurations.	ITS Telecom & Black Box
2.	Install the line cards, power and cable connections into the new PBX.	2 days	Receipt of the new PBX.	ITS Telecom & Black Box

3.	Configure the PBX for individual extensions (TNB – terminal numbers).	2 days	Installation of the new PBX. Prioritized list of name and location of individuals who will be provided minimal phone service.	ITS Telecom & Black Box

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Black Box	PBX hardware, software and associated components of the PBX including 110 blocks, cables, phones, wall jacks, etc.	Remotely stored backup copy of PBX configuration.
AT&T	T1 circuits for long distance calls and local call service.	
Sprint	T1 backup circuit for long distance calls.	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of a disaster?)
Circuit Listing	Comprehensive list of all the incoming/outgoing call circuits.	Contact information and circuit IDs are on the ITS Emergency Document Management server, emergency laptops and SharePoint.
PBX Monthly Backup	Campus phone configurations, features and access rights.	In ADM 5A and the data center safe.

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

PBX lines	Main campus number	323-343-3000 and roll-over numbers 3001 to 3010	AT&T
Circuit	T1 circuit for long distance calls.	13 PRIs	AT&T
Circuit	T1 backup circuit for long distance calls.		Sprint
Special Notes			

7.3.2.2 Critical Personnel Phone Restoration

Platform:	**Satellite Telephone System**	**Location:**	**Administration Building roof and ADM 5**
Virtual / Physical:	**Physical**		
Description/Applications:	**Two backup phone solutions are in place for critical personnel. 1) Designated PBX phones that have a line with access to dial tone through a satellite antenna on the ADM building roof, and 2) four satellite phones provisioned through Public Safety.** **If there is a problem with local phone service, there are a few hardwired phones that will provide local and long distance calling but they are dependent upon the PBX to function.** **If the PBX is inoperable, there are a few handhelds immediately capable of establishing a satellite connection.** **The satellite antenna is located on the Administration Building roof.**		

RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**32 days for hardwired satellite phones**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Quick ship and install		

Recovery Tasks

Scenario:	**Loss of local phone service with and without the PBX availability.**	**Recovery Location:**	**Not applicable**

Step	Task Detail	Est Time	Dependency	Team
If the Local Telephone Service Provider is Inoperable				
1.	The antenna on the Administration Building roof is connected to the PBX, which allows the following eight users immediate hardwired access to PBX phones with satellite service: • President • Office of the President • Provost and vice president for Academic Affairs • Vice provost for Diversity and Engaged Learning • Vice president for Student Life • Vice president for University Advancement • Vice president for Administration • CIO / associate vice president for Information Technology Services	2 min	None	ITS Telecom
2.	Notify the above departments of the local service outage and estimated recovery time, if known.	15 min	None	ITS Help Desk

If the PBX is Inoperable				
1.	There are four mobile emergency satellite phones provisioned by Public Safety on hot standby that do not require the Administration Building roof antenna. These can be used from any outside location but require that the batteries are working. The following users have satellite phones: • President • Provost and vice president for Academic Affairs • Vice president for Administration	2 min		ITS Telecom

	• Police Chief			
2.	If the satellite antenna or hardware needs to be replaced, call Remote Satellite Systems.	3 days		ITS Telecom

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Remote Satellite Systems	Antenna and phone repair or replacement.	Contact information is on the ITS Emergency Document Management server emergency server, emergency laptops and SharePoint.

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Satellite Phone Implementation	Satellite logistical information and instructions.	Visio file in SharePoint.

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Satellite Phone		88-16-22-41-89-58	Remote Satellite Systems

Special Notes

7.3.2.3 Voice Mail Restoration

Platform:	**Voice mail System and Call Pilot Software**	**Location:**	**Administration Building**
Virtual / Physical:	**Physical**		
Description/Applications:	**Campus voice mail services**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**15 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Quick ship and install		

Recovery Tasks

Scenario:	**Loss of the Administration building**	**Recovery Location:**	**TBD based upon scope of the incident.**

Step	Task Detail	Est Time	Dependency	Team
1.	Inform Black Box of the disaster and using the emergency procurement process, order a new system that supports 1000 users and 96 ports. Note: The current model is no longer available.	10 days	Identification and availability of an alternate site, if necessary.	ITS Telecom and Black Box
2.	In the event that only the voice mail system is inoperable, a Black Box technician will route voicemail numbers to an available port with a recording indicating voicemail is down	30 min	None	ITS Telecom and Black Box
3.	Receive new system and install in the new location.	4 hours	Availability of alternate site. Receipt and installation of the new PBX.	ITS Telecom and Black Box
4.	Retrieve backup configuration and software and restore the voice mail system.	1 day	Availability of backup configuration.	ITS and Black Box

5.	If backup is not available, manually add all mail boxes into the new system in order of priority using the hard copy or system print out.	1 day for Priority 1 users 7 days for full completion	Availability of hard copy of configurations.	ITS Telecom and Black Box

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Black Box	Hardware and software for voice mail server	Remotely stored backup of voice mail configuration.

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Voice mail server configuration	Comprehensive list of assigned mailboxes and features.	Black Box
Call Pilot software	System operating software.	Black Box

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.2.4 Call Accounting Restoration

Platform:	**Call Accounting System**	**Location:**	**Administration Building**
Virtual / Physical:	**Physical**		
Description/Applications:	**Phone call accounting services. Devices that record raw call data from the PBX and the software application that prepares the data for department usage chargebacks and billing reports.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**8 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Quick ship and install		

Recovery Tasks

Scenario:	**Loss of the primary switchroom or PBX**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Notify Black Box of the disaster. Order the replacement call collection device and a replacement copy of the Infortel Select application software. Note: If available, order two call collection devices for redundancy. If not available, the second device can be ordered following full operational recovery.	5 days	None.	ITS Telecom and Black Box
2.	Order a replacement server from CCS Disaster Recovery Services, the hardware vendor.	2 days	Availability of servers from the vendor site.	Server Team
3.	Install the operating system on the replacement server.	1 day	Receipt of the server.	Server Team
4.	Notify Black Box to install the Infortel Select application software.	1 day	Installation of the server.	ITS Telecom and Black Box
5.	Install the call collection device(s) and connect to PBX and the call accounting server	1 day	Installation of the PBX.	ITS Telecom and Black Box

			Installation of the server.	
6.	Restore the system from the backups.	1 hour		ITS Telecom and Black Box

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
CCS Disaster Recovery Services	Server hardware	
Black Box	Call collection devices and Infortel Select software for the billing server.	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Infortel Select server configuration backup	Backup copy of extension, employee, department and billing information.	Currently on VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.2.5 Help Desk Call Center

Platform:	**CxExchange**	**Location:**	**Cloud**
Virtual / Physical:	**Virtual**		
Description/Applications:	**A cloud based ACD solution for the Help Desk**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**Hours**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Self administration – redirect calls to Help Desk agents to any working number.		

Recovery Tasks

Scenario:	**Loss of the primary switchroom or PBX**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Log in to CxExchange Platform web administration page and change the phone numbers to any working number where an agent can pick up calls.	hours	None.	Client Support Services

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Serenova (part of LifeSize)	Software support	1-800-793-0549, 1, 2 (critical outage)

7.3.3 Data Communications Restoration

7.3.3.1 Rebuild Network Distribution and Access Layer Infrastructure

Platform:	**Network Distribution and Access Layer Infrastructure Rebuild**	**Location:**	**For all distribution and access level locations.**
Virtual / Physical:	**Physical**		
Description/Applications:	**This document is a guide for how to replace distribution and access layer functionality in any location, ranging from locations servicing SDF facilities to the data center.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**3 days or up to 1 month if purchasing equipment.** **Also dependent on location infrastructure.**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Identify all equipment that needs to be replaced. (Reference Network Equipment Spreadsheet by location or Network Diagram for an equipment list.)	1 hour		Network Services Team
2.	Assess availability of equipment in inventory or other unused or undamaged buildings to use in rebuild of new closet.	1 day		Network Services Team

3.	If equipment is not available in house, purchase comparable or identical equipment with equivalent port capacity.	up to 1 month		Network Services Team
4.	Obtain backup configurations if possible from configuration management tool if available or work from an existing configuration of a comparable device.	2 hours		Network Services Team
5.	Verify that there is appropriate power, port wiring and fiber connectivity.	1 day		Network Services Team
6.	Mount hardware, power it on and configure the hardware.	1 day		Network Services Team
7.	Verify connectivity and communication with neighboring devices.	Included in step 6		Network Services Team
8.	If there are access ports, implement proper security controls and application access, and verify proper VLAN assignment.	1 day		Network Services Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
AT&T or any vendor that has the appropriate equipment.	Hardware Vendor	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Network Equipment Spreadsheet		SharePoint and Avail
Backup Configurations	Configurations of router and switches	Configurations are on the emergency laptops.

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Special Notes			

7.3.3.2 Network Core – Internet Recovery

Platform:	**Network Core, Internet Recovery**	**Location:**	**Library North and ADM 5**
Virtual / Physical:	**Physical**		
Description/Applications:	**Campus access to the Internet**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**10 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	In the event of a disaster of the Library North and Administration buildings, Internet connectivity will be maintained through the redundant link in the alternate building.		

Recovery Tasks

Scenario:	**Loss of the primary Internet connection**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
Note: This is assuming that this infrastructure will be rebuilt at an alternate location.				
1.	Identify undamaged building BDF's that require core connectivity and run aerial fiber to connect them to the operational core until damaged infrastructure can be rebuilt.	3 days		Network Services Team
2.	Identify necessary equipment that needs to be replaced. There is redundant equipment and infrastructure between the Administration Building and the data center (reference Network Equipment Spreadsheet by location and the Network Diagram).	1 day		Network Services Team
3.	Assess availability of equipment in inventory or other unused or undamaged buildings to use.	1 day		Network Services Team

4.	If equipment is not available in house, purchase comparable or identical equipment with equivalent port capacity. -Cisco 4503 is owned by CENIC. Contact them for replacement.	up to 1 month		Network Services Team
5.	Obtain backup configurations, if possible, from configuration management tool if available or work from an existing configuration of a comparable device. NOTE: -Cisco 4503 configuration is implemented by CENIC -Procera PacketLogic configuration is identical to the redundant device in the data center. -Palo Alto Firewall configuration is identical to the redundant firewall in the data center.	1 day		Network Services Team
6.	Determine space required for network equipment. Ensure there is appropriate power, port wiring and fiber connectivity.	1 day		Network Services Team
7.	Mount hardware, power it on and configure the hardware.	3 days		Network Services Team
8.	Re-evaluate distribution of BDF connectivity and re-establish connectivity based on original design when possible.	included in step above		Network Services Team
9.	Verify connectivity and communication with neighboring devices.			Network Services Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
CENIC	Cisco Hardware / Software	

Vital Records		
Name	**Description**	**Storage Location (Where would you retrieve this from at time of disaster?)**
Network Equipment Spreadsheet		SharePoint site
Network Diagram		SharePoint site

Telecomm			
Type of Telecom Resource (Fax, Phone, Circuit)	**Description**	**Phone Number**	**Provider**

Special Notes

7.3.3.3 Clearpass

Platform:	**Clearpass**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Appliance that is used to grant a user access to network services based on the users' windows login.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**34 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild and restore		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Retrieve spare units from hardware and maintenance support inventory.	1 month		Network Services Team & Hardware and Maintenance Support
2.	Retrieve backup configuration from storage server and install updated software.	4 hours		Network Services Team
3.	If the configuration backup is not available, then configure the device from scratch.	3 days		Network Services Team
4.	Verify IP communication between Clearpass appliance and switches that it communicates with regarding user authentication.	1 day		Network Services Team
5.	Test user authentication.	included in step above		Network Services Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Configuration Backup		Configuration is on Zebra, which is also in the data center.

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.3.4 ACS – Access Control Server

Platform:	**Access Control Server (cla-acs5, cla-acs6, cla-acs7, cla-acs8)**	**Location:**	**Library North ADM 5A**
Virtual / Physical:	**Physical**		
Description/Applications:	**Accessing, authentication and accounting CISCO appliances.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**32 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild and restore		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Order new servers.	4 to 6 weeks		Server Team
2.	Obtain and install appropriate Windows Operating System software. Get IP address information from address list. Critical: Verify OS and patch level.	4 hours		Server Team
3.	Install most current version of Cisco ACS Application.	2 hours		Network Services Team
4.	If previous configuration is available, restore from the backup configuration.			Network Services Team
5.	If configuration not available, prioritize which systems need authentication and configure ACS for those systems.			Network Services Team
6.	Test to ensure that access is functioning.	30 minutes		Network Services Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Cisco	ACS Software Application	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
ACS Application Software		Download from Cisco

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.4 Operating Systems Restoration

This section will be referenced in subsequent sections for operating systems restoration procedures.

7.3.4.1 OS RedHat Restore

Platform:	**RedHat OS Recovery**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Procedures to restore a RedHat Operating System**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild and restore		

Recovery Tasks			
Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	**Task Detail**	**Est Time**	**Dependency**	**Team**
	Base RedHat Installation Tasks			
1.	Order comparable equipment from HP.	4 to 6 weeks		Server Team
2.	Obtain operating system software from RedHat.	1 hour		Server Team
3.	Install RedHat Operating System using appropriate IP Addressing	1 hour		Server Team
4.	Install VEEAM Client.	1 hour		Server Team
5.	Test basic network connectivity.	30 minutes		Server Team
6.	Restart system.	20 minutes		Server Team
7.	Restore OS over existing OS from VEEAM backup.	1 hour		Server Team

8.	Validate services such as file/print, web services and database services.	1 hour		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
RedHat	OS Vendor	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
RedHat Operating System		www.redhat.com using ISO CD image

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.4.2 Win2008 Operating System

Platform:	Windows 2008 Operating System	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	Procedures to restore a Win2008 Operating System		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild and restore		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
Base Win2008 Installation Tasks				
1.	Order comparable equipment.	4 weeks		Server Team
2.	Obtain operating system software.	30 minutes	License Key	Server Team
3.	Install Win 2008 with appropriate service - use appropriate IP addressing.	4 hours	IP Addressing and File System / Partition Configuration	Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Install backup client (VEEAM) as appropriate.	1 hour		Server Team

8.	Restart system.	30 minutes		Server Team
9.	Restore OS over existing from offsite backup.	2 to 8 hours		Server Team
10.	Validate services such as file/print, WINS, home directory, etc. (see hardware chart for specific server services).		Server Resource Sheet by Function and ind.Server Configs	Server Team
Note: If you can recover a PDC with an existing BDC, then for Win2008 or Win2012 OS systems:				
11.	Move FSMO roles to BDC to make it a master.	2 hours		Server Team
12.	Perform DC promote to promote machine as one of DC.	2 hours		Server Team
13.	Then transfer roles back to PDC.	2 hours		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	VEEAM Backup Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Win2008 OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter
VEEAM Client	Install VEEAM Client Software	ITS Office
Operating System Install Procedure		SharePoint

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Special Notes			

7.3.4.3 OS Win2012 Restore

Platform:	**WIN2012 OS Recovery**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Procedures to restore a Win2012 Operating System**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Rebuild and restore		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
Base Win2012 Installation Tasks				
1.	Order comparable equipment.	4 weeks		Server Team
2.	Obtain operating system software.	30 minutes	License Key	Server Team
3.	Install Win 2012 with appropriate service pack - use appropriate IP Addressing.	4 hours	IP Addressing and File System / Partition Configuration	Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Install backup client (VEEAM) as appropriate.	1 hour		Server Team

8.	Restart system.	30 minutes		Server Team
9.	Restore OS over existing from VEEAM.	2 to 8 hours		Server Team
10.	Validate services such as file/print, WINS, home dir, etc. (see hardware chart for specific server services).		Server Resource Sheet by Function and ind. Server Configs	Server Team
Note: If can recover a PDC with an existing BDC, then for Win2008 or Win2012 OS systems:				
11.	Move FSMO roles to BDC to create a master.			Server Team
12.	Perform DC promote to promote machine as one of DC.			Server Team
13.	Transfer roles back to PDC.			Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	Data backup source	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Win2012 OS Install Software and License	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter/ (Ryan Chan or Jeff Cheam)
VEEAM software	Install VEEAM Client	ITS Office and Horace Ting
Operating System Install Procedure		SharePoint

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Special Notes			

7.3.5 Network Systems Restoration

7.3.5.1 DNS Restoration

Platform:	**DNS Recovery (BlueCat appliance)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Domain Name Services**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**1 day plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Redundant locations		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase appliances for DNS service.	4 weeks		Server Team
2.	Install appropriate OS.	2 hours		Server Team
3.	Install VEEAM Client.	30 minutes		Server Team
4.	Restore DNS server from the VEEAM client.			Server Team
5.	If there is a problem with the VEEAM, there is also a copy of the DNS servers off campus in Chancellors Office (NS1.csu.net or NS2.csu.net).			Server Team

6.	Check under /var/named.			Server Team
7.	Check service bind/named.			Server Team
OR				
8.	*If there is no way to restore the primary DNS servers:* Promote CLA-ns1 located in the ST Annex building to primary.			Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter/
VEEAM Client software	Install VEEAM Client	ITS office and VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.2 DHCP Restoration

Platform:	**DHCP Recovery (BlueCat appliance)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Dynamic IP Address assignment server**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**8 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Redundant locations		

Recovery Tasks

Scenario:	**Loss of the primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase server for DHCP.	4 weeks		Server Team
2.	Obtain appropriate operating system software.	30 minutes		Server Team
3.	Install appropriate OS - use appropriate IP addresses.	4 hours		Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Install backup VEEAM client.	1 hour		Server Team
8.	Restart system.	30 minutes		Server Team

9.	Validate DHCP Services.	1 hour		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter/
VEEAM Client software	Install VEEAM Client	ITS Office and VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.3 Domain Controller Restoration

Platform:	**Domain Controllers**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Domain Controller Servers:** **Aladdin, Avatar, csula-dc1, csula-dc2, kh-dc3, kh-dc4, nis-dc1, nis-dc2, nis-dc3, nis-dc4, pine-dc1, pine-dc2, root-dc3, root-dc4,**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**12 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase servers for Domain controllers.	4 weeks		Server Team
2.	Obtain appropriate operating system software.	30 minutes		Server Team
3.	Install appropriate OS - use appropriate IP addresses.	4 hours		Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Install backup client (VEEAM).	1 hour		Server Team
8.	Restart system.	30 minutes		Server Team

OPTION 1				
9	If none of the Domain Controllers on that particular domain exists, Restore OS over existing OS from offsite tape.	4 hours		Server Team
OPTION 2				
1.	*If ITS can recover a PDC with an existing BDC, then for Win2008 or Win2012 OS systems:*			
2.	Move FSMO roles to BDC to make it a master.			Server Team
3.	Perform DC promote to promote machine as one of DC.			Server Team
4.	Then transfer roles back to PDC.			Server Team
5.	Validate services such as file/print, WINS, home dir, etc. (see hardware chart for specific server services).			Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter (Ryan Chan or Jeff Cheam)
VEEAM Client software	Install VEEAM Client	ITS Office and VEEAM, Horace Ting

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Special Notes			

7.3.5.4 IDP Servers Restoration

Platform:	**IDP Servers**	**Location:**	**Library North**
Virtual / Physical:	**Physical and Virtual**		
Description/Applications:	**IDP Servers:** **IDP3, IDP4, IDP14**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**12 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks			
Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
10.	Purchase servers for IDP servers.	4 weeks		Server Team
11.	Obtain appropriate operating system software (Red Hat 6).	30 minutes		Server Team
12.	Install appropriate OS - use appropriate IP addresses.	4 hours		Server Team
13.	Install virus scan software.	1 hour		Server Team
14.	Install patches.	1 hour		Server Team
15.	Test basic network connectivity.	30 minutes		Server Team
16.	Install backup client (VEEAM).	1 hour		Server Team
17.	Restart system.	30 minutes		Server Team

18.	If none of the IDP servers exist, restore OS over existing OS from offsite tape.	4 hours		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Red Hat	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter (Ryan Chan or Jeff Cheam)
VEEAM Client software	Install VEEAM Client	ITS Office and VEEAM, Horace Ting

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.5 Identity Management and MIM Server Restoration

Platform:	**Domain Controllers**	**Location:**	**Library North**
Virtual / Physical:	**Physical & Virtual**		
Description/Applications:	**Identity Management & MIM Servers:** **Monet, Okeeffe, Picasso, Vangogh1, Vangogh2, Matisse, Dali, Giotto, Davinici-1, Davinici-2**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**14 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Quick ship and VEEAM restore		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase servers for IDM & MIM servers.	4 weeks		Server Team
2.	Obtain appropriate operating system software.	30 minutes		Server Team
3.	Install appropriate OS - use appropriate IP addresses.	4 hours		Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Install backup client (VEEAM).	1 hour		Server Team
8.	Restart system.	30 minutes		Server Team

9.	Restore application files from VEEAM.	4 hours per server		Server Team
10.	Restart system.	30 minutes		Server Team
11.	Validate server operation, inter-server connectivity, network security.	30 minutes		Server Team
12.	Test functionality.	30 minutes		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
OS Install Software	OS Software with service pack	Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter (Ryan Chan or Jeff Cheam)
VEEAM Client Software	Download software for VEEAM Client	ITS Office and VEEAM, Horace Ting

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.6 VMWare Server Version Restoration

Platform:	**VMWare Server Version**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	***VMHost-ESX* (Aristocats)** ***VMHost-ESXi* (Sarabi1, Sarabi2, Sarabi3, Sarabi4, Testarossa)** ***VMHost-VM1* (VM1, VM2, VMS1, VMS2, VMS3, VMS4, VMS5, VMS6)** ***VMHost-VM2* (Bell, Tinker)**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**3 days plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	**Task Detail**	**Est Time**	**Dependency**	**Team**
1.	Purchase servers from HP.	4 weeks		Server Team
2.	Install OS (UBUNTU or RedHat).	4 hours		Server Team
3.	Install VMWare Server (server software).			Server Team
4.	Configure the VM Network.			Server Team
5.	Restore the guest virtual machines.			Server Team
	OR Rebuild the guest instances:			
1.	Website on VM1 host – backup of website is on Henry Liao's PC and notebook.			Server Team

2.	Blackberry on VMS5 – reinstall the application on a VM guest.			Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
VMWare	VMWare Software	www.vmware.com – All server team members maintain associate account for access to licenses.
RedHat	OS Software	
Hewlett Packard	Server Hardware	
Hewlett Packard	SAN Hardware	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Henry Liao's PC and notebook	Has a backup of the website on VM1	Henry's notebook offsite
Virtual Server Recovery Procedure	to be created	

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.7 Network Security Manager (NSM) Restoration

Platform:	**NSM (cla-nsm1, cla-nsm2)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Network Security Manager – these servers manage the server farm firewalls.** **If one manager goes down, the other manager will take over (Active/Passive).**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**2 days after equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks				
Scenario:	**Loss of primary data center**	**Recovery Location:**		
Step	**Task Detail**	**Est Time**	**Dependency**	**Team**
Note: NSM server (Qty2) – cla-nsm1, cla-nsm2: nsm1 is in the Administration building and nsm2 is in the data center.				
1.	Order equipment from HP – one server is critical, others to be added as needed.	4 to 6 weeks		Server Team
2.	Download RedHat OS from internet and onsite copy of OS in offices.	1 hour		Server Team
3.	Receive equipment and install.			Server Team
4.	Install OS RedHat.	1 day		Server Team
5.	Install VEEAM Client software.	30 minutes	Internet Access	Server Team
6.	Recover configuration files from VEEAM.	1 day		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
RedHat	OS Software	www.redhat.com
Hewlett Packard	Server Hardware	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Server List	To identify servers	SharePoint

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.8 Syslog Restoration

Platform:	**Syslog Recovery (Zebra)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Collects system / application/ security logs from multiple locations.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of Primary Data Center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase server for Syslog server.	4 weeks		Server Team
2.	Obtain appropriate operating system software.	30 minutes		Server Team
3.	Install appropriate OS - use appropriate IP addresses.	4 hours		Server Team
4.	Install virus scan software.	1 hour		Server Team
5.	Install patches.	1 hour		Server Team
6.	Test basic network connectivity.	30 minutes		Server Team
7.	Validate SYSLOG services.	30 minutes		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
SourceForge	Open Source Application – Syslog-ng	
CCS Disaster Recovery Services	Hardware Vendor	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Syslog-ng Procedures		

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.5.9 SharePoint Restoration

Platform:	**SharePoint (Atlantis)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**IIS Web Server for sharing of documents.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**16 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
	Atlantis server (Qty1) –			
1.	Order equipment from HP.	4 to 6 weeks		Server Team
2.	Receive equipment and install.			Server Team
3.	Install OS from CD.	1 hour		Server Team
4.	Enable IIS services.	included in step above		Server Team
5.	Install the same NET framework version.	30 minutes		Server Team
6.	Install SQL2005.	2 hours		Server Team
7.	Install MOSS (Microsoft Office SharePoint Service).	4 hours		Server Team

8.	Install VEEAM Client software.	30 minutes	Internet Access	Server Team
9.	Execute the SharePoint software.			Server Team
10.	Use the application option to restore from the backup.	4 hours		Server Team
11.	Fully test the SharePoint websites to validate the restore.	4 hours		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS	
Microsoft	SharePoint Software	
Microsoft	SQL Software	
Veritas	Netbackup Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Server List	To identify servers	SharePoint
OS Disk Image		Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter (Ryan Chan or Jeff Cheam)
VEEAM software		VEEAM
SQL2016/17 Disk Image		Microsoft Volume Licensing Service Center - https://www.microsoft.com/licensing/servicecenter (Ryan Chan or Jeff Cheam)

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider
Special Notes			

7.3.5.10 File Server Restoration

Platform:	**File Servers (frozen, frozen2, frozen3)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**File Server Restore Procedure** **Print services do not need to be recovered on the server.** **Assumption: IP address is on the printers, not in print queues**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 days plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase servers for file servers.	4 weeks		Server Team
2.	Install appropriate OS.	4 hrs		Server Team
3.	Install VEEAM Client.	2 hrs		Server Team
4.	Restore file server data from VEEAM Client software.	1 day		Server Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	OS Software	
Veritas	Netbackup Client Software	

Vital Records		
Name	**Description**	**Storage Location (Where would you retrieve this from at time of disaster?)**
VEEAM Client Software		VEEAM

Telecomm			
Type of Telecom Resource (Fax, Phone, Circuit)	**Description**	**Phone Number**	**Provider**

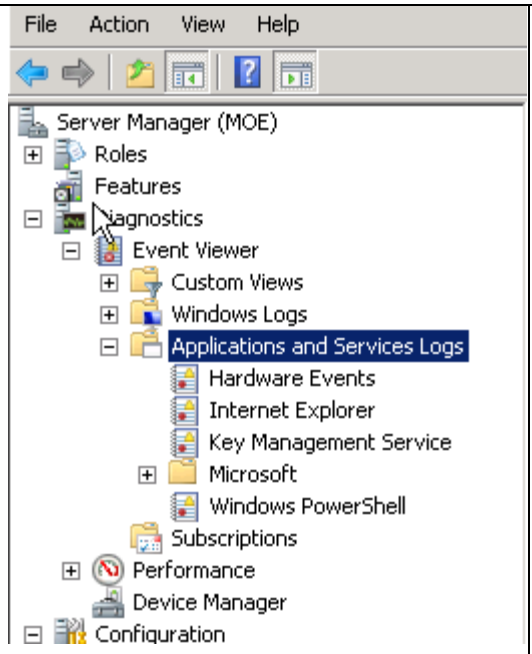
Special Notes

7.3.5.11 License Server Restoration

Platform:	**License Servers**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**MOE – Activating the Windows 7 and Windows 10 licenses for desktops that are disbursed throughout the campus.** **APU – Holding the licenses for, SPSS, AMOS, Mathematica, Maya, MatLab, Encase** **MOYA – Holding the license for Jaws, MAGic, Kurzweil, Key Server, Final Draft**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**7 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	Purchase and rebuild		

Recovery Tasks				
Scenario:	**Loss of primary data center**	**Recovery Location:**		
Step	**Task Detail**	**Est Time**	**Dependency**	**Team**
License Server (Qty1) – MOE Server (key mgmt server)				
If servers are not restored yet and the client's activation key is expired, the Server Team can use the multi-activation key on the PC itself. If the multi-activation key has hit the limit, request more from Microsoft. **This is for OS and Office products.**				
1.	Order equipment from HP.	4 to 6 weeks		Server Team

2.	Receive equipment and install.	included in step above		Server Team
3.	Download Win2012 OS from the internet (Microsoft website) or the onsite copy of OS in the Server Team offices.	1 hour		Server Team
4.	Install the activation key for windows (group B) thru the internet. If internet not available, call Microsoft to activate the key and follow their instructions.	30 minutes		Server & Desktop Teams
5.	Run the Command Line to verify the activation: Need KMS key for volume activation (i.e. KMS B) cscript c:\Windows\System32\slmgr.vbs /ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx cscript slmgr.vbs /dli (to query the KMS server and see its status) Under the Event Viewer, Application and Services Logs, Key Management Service	5 minutes		Server & Desktop Teams

	 cscript c:\windows\system32\slmgr.vbs /dlv cscript c:\windows\system32\slmgr.vbs /dlv bfe7a195-4f8f-4f0b-a622-cf13c7d16864			
6.	Download the module for Office 2016/2019 from Microsoft to the server.	1 hour		Server Team
7.	Install the activation key for Office 2016/2019 from the internet. KMS activation of Office 2016/2019: To activate the KMS host on the internet, run KeyManagementServiceHost.exe in the Microsoft Office 2016/2019 KMS Host License Pack	1 hour		Server and Desktop Teams

	Microsoft office 2016/2019 KMS Host License Pack (download this package) and a valid KMS host key is installed. If the internet not available, call Microsoft to activate the key and follow their instructions. To activate the KMS host on the telephone or manually, and to configure the KMS host, use the **slmgr.vbs** script.			
8.	Database of licenses would be rebuilt as the client connects to the system again.	1 day		Server & Desktop Teams
License Server (Qty1) - APU				
1.	Order the equipment from HP.	4 to 6 weeks		Server Team
2.	Receive the equipment and install.	included in step above		Server Team
3.	Download Win2012 OS from the internet and onsite copy of OS in offices.	1 hour		Server and Desktop Teams
4.	For all applications, contact the appropriate vendor (see resources below) to request a new license key.	1 hour		Desktop Team
5.	Install the license for applications on this server.			Desktop Team
License Server (Qty1) - MOYA				
1.	Order the equipment from HP.	4 to 6 weeks		Server Team
2.	Receive the equipment and install.	included in step above		Server Team
3.	Download Win2012 OS from the internet and onsite copy of OS in offices.	1 hour		Server Team
4.	For JAWS and MAGic, install license manager from the vendor's CD.	1 hour		Desktop Team

5.	For KeyServer application, download the application from the internet. Call SASSAFRAS vendor for license key.		File Server	Desktop Team
6.	Kurzweil application has a license key on a dongle. Use this instead of calling the vendor for recovery.			Desktop Team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Microsoft	Win2008 OS Win2012 OS Windows 7 Windows 10 Office 2016/2019	Download images and license keys from Microsoft site - https://www.microsoft.com/licensing/servicecenter/ (Ryan Chan and Jeff Cheam)
Apple	MAC OSes	Get OS from Apple App store
Freedom Scientific	JAWS Application License	Runs on Moya server
Freedom Scientific	MAGic Application License	Runs on Moya server
SPSS	SPSS Application License	Runs on APU server
SPSS	AMOS Application License	Runs on APU server
Kurzweil Education Systems	Kurzweil Application License	Activation from Kurzweil website – http://www.fireflybykurzwell.com
SASSAFRAS	Key Server Application License	Runs on Moya server
Wolfram	Mathematica Application License	Runs on APU server

Autodesk	AutoCAD/Maya Application License	Runs on MOE server
Mathworks	MATLAB Application License	Runs on APU server

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Server List	To identify servers	SharePoint
DSS images for Windows	DSS images for OAL,TEC, EC, faculty and staff	Image server(s), external drives and offsite
DSS images for Mac	DSS images for OAL,TEC, EC, faculty and staff	Image server(s), external drives and offsite
Activation key for Win 7 and Win 10 for Office Office 2016/2019		In Desktop Services office or offsite
License Information Adobe		In Desktop Services office or offsite
License Information JAWS		In Desktop Services office or offsite
License Information MAGic		In Desktop Services office or offsite
License Information SPSS		In Desktop Services office or offsite
JAWS and MAGic license manager CD	Needed for the install of the license keys on the server	Desktop Services office or offsite
Kurzweil	Need to activate at Kurzweil website	http://www.fireflybykurzwell.com
HP	Desktop and laptop hardware	Baseline Storage/IRG/HP/ITS Loaners

Apple	Desktop and laptop hardware	Baseline Storage/Apple/ITS Loaners

Telecomm			
Type of Telecom Resource (Fax, Phone, Circuit)	**Description**	**Phone Number**	**Provider**
Special Notes			

7.3.5.12 Tableau Server

Platform:	**Reporting Server**	**Location:**	**Library North**
Virtual / Physical:	**Virtual**		
Description/Applications:	**Business Intelligence**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):			

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase comparable hardware from HP.	4-6 weeks		Server team
2.	Install Windows OS.	2 hours		Server team
3.	Download and install Tableau Software.	2 hours		Server team
4.	Install VEEAM client.	30 minutes		Server team
5.	Restore server file systems.	1 hour		Server team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Hewlett Packard	Server hardware	Hewlett Packard
Tableau software	Software to automate the electronic processing of the transcript request	Tableau software

VEEAM	VEEAM Client Software	VEEAM
VMWare	Virtual server software	VMWare

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.6 Web Systems Restoration

7.3.6.1 Web Server Restoration

Platform:	**Web Server**	**Location:**	**Library North**
Virtual / Physical:	**Virtual**		
Description/Applications:	**Web Server: web.calstatela.edu**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**12 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks			
Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase servers for VM environment.	4 weeks		Server team
2.	Obtain appropriate operating system software (Red Hat 7.5).	30 minutes		Server team
3.	Install appropriate OS – user appropriate IP addresses.	4 hours		Server team
4.	Install virus scan software.	1 hour		Server team
5.	Install patches.	1 hour		Server team
6.	Test basic network connectivity.	30 minutes		Server team
7.	Install backup client (VEEAM Client software).	1 hour		Server team
8.	Restart system.	30 minutes		Server team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
CCS Disaster Recovery Services	Hardware Vendor	
RedHat	OS Software	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
RedHat OS recovery procedures		In this plan

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7 Applications Restoration

7.3.7.1 Robo Registrar

Platform:	**TranscriptsPlus**	**Location:**	**Library North**
Virtual / Physical:	**Virtual**		
Description/Applications:	**Transcript processing for the University. Credentials Solutions is the vendor.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):			

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase comparable hardware from HP.	4-6 weeks		Server team
2.	Install Windows OS.	2 hours		Server team
3.	Download and install RoboRegistrar software.	2 hours		Server team
4.	Install VEEAM Client software.	30 minutes		Server team
5.	Restore server file systems.	1 hour		Server team

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Hewlett Packard	Server Hardware	

RoboRegistrar Credential Solutions software	Software to automate the electronic processing of the transcript request	
VEEAM	VEEAM Cient Software	
VMWare	Virtual Server Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.2 Listserve Server Restoration

Platform:	**Listserve (TAZ)**	**Location:**	**Library North**
Virtual / Physical:			
Description/Applications:	**Target Group Communication for on-campus or off-campus. Survey and communication purposes.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**20 hours plus equipment order**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Purchase servers (TAZ Server).	4 weeks		Server Group
2.	Install appropriate OS and then patch.	4 hours		Server Group
3.	Install Listserve application.	4 hours		Server Group
4.	Install VEEAM Client software.	2 hours		Server Group
5.	Restore server from the VEEAM Client software.	8 hours		Server Group
6.	Call Lyris to activate license.	1 hour		Server Group

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
Lyris	Listserve Application	
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
Listserve Application	CD with application install	

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.3 Blackboard / One Card Restoration

Platform:	**Blackboard / One Card (BBTSCSU – is the only server listed on the inventory list for this app)**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Door access and debit card functionality** **There are several servers for this application: Three in the data center (database and Win primary and on appliance); others are throughout the University in Open Access Labs (for card key access and for printing and copying and charging from debit card). Control boxes in each building are vendor supported. Photo files associated with each person are in the database.** **1. ID cards for students (do not use Windows server).** **2. Debit card for students (uses all three pieces of equipment) – debit card is function of Pharos server.** **3. Door access (does not use Windows server).**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	**21 days**
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):	VEEAM		

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Call Blackboard and determine new hardware specs for all three devices. Order replacement servers from HP with O/S installed.	3 days	Campus network	Server Group
2.	Blackboard sends IT Infrastructure a tape or CD containing the application software.	1 day		Server Group

3.	Blackboard works with IT Infrastructure to ensure network connectivity.	4 hours	1	Server Group
4.	Once the tape is onsite, IT Infrastructure calls Blackboard to load the applications Optim and Pharos (print server software) and the database software. Then configure applications.	4 hours	3	Server Group
5.	Retrieve tape from offsite location.	2 hours	4	Server Group

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
VEEAM	VEEAM	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
VEEAM	VEEAM	VEEAM portal

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.4 SFTP Internal Server

Platform:	**Windows**	**Location:**	**Library North**
Virtual / Physical:	**Physical**		
Description/Applications:	**Club33** **Secure FTP system to securely transfer files from one system to another.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):			

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
1.	Order equipment from HP.	4 to 6 weeks		Server Group
2.	Receive equipment and install.	Included in step above		Server Group
3.	Install OS from CD.	1 hour		Server Group
4.	Install VEEAM Client software.	30 minutes	Internet Access	Server Group
5.	Recover app, configuration and data from VEEAM.	1 day		Server Group

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
VEEAM	VEEAM Client Software	VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.5 SFTP External Server

Platform:	**Windows**	**Location:**	**Library North**
Virtual / Physical:	**Virtual**		
Description/Applications:	**Entsys-SFTP2** **Secure FTP system to securely transfer files from Cal State LA to an external system.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):			

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
6.	Order comparable hardware from HP.	4 to 6 weeks		Server Group
7.	Receive equipment and install.	Included in step above		Server Group
8.	Install OS from CD.	1 hour		Server Group
9.	Install VEEAM Client software.	30 minutes	Internet Access	Server Group
10.	Recover app, configuration and data from VEEAM	1 day		Server Group

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
VEEAM	VEEAM Client Software	VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.6 Oracle Database

Platform:	**Linux**	**Location:**	**Library North**
Virtual / Physical:	**Physical and Virtual**		
Description/Applications:	**Orca1(Physical) and Orca2(Virtual)** **Oracle database systems currently supporting RDS; servers execute batch jobs used for Canvas, EAB, Vector, CSU Learn, and other important integrations.**		
RTO (recovery time objective – when will restoration take place):		**Est RTO:**	
RPO (recovery point objective – restore back to what point in time):		**Est RPO:**	
Recovery Strategy (Failover, Tape Restore, Quick ship etc.):			

Recovery Tasks

Scenario:	**Loss of primary data center**	**Recovery Location:**	

Step	Task Detail	Est Time	Dependency	Team
11.	Order equipment from HP.	4 to 6 weeks		Server Group
12.	Receive equipment and install.	Included in step above		Server Group
13.	Install OS from CD.	1 hour		Server Group
14.	Install VEEAM Client software.	30 minutes	Internet Access	Server Group
15.	Recover app, configuration and data from VEEAM.	1 day		Server Group

Resources

Vendors (Hardware, Software, Service Provider)

Name	Purpose	Resource Details
VEEAM	VEEAM Client Software	

Vital Records

Name	Description	Storage Location (Where would you retrieve this from at time of disaster?)
VEEAM	VEEAM Client Software	VEEAM

Telecomm

Type of Telecom Resource (Fax, Phone, Circuit)	Description	Phone Number	Provider

Special Notes

7.3.7.7 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. Since the vendor will determine disaster recovery procedures, this document does not describe the specific restoration steps for these systems. The following servers, all priority 3 restorations, are in this category.

Department Contact	Server Name	Application
Academic Affairs	AA-SDS	File/print
Administrative Technology	Avanti	Reprographics
	Environmental	Monitoring
	Holes1, Holes2	File/print
	Print-Pharos	Print
	Xythos1, Xythos2, Xythos3, Congas, Bumbaa, Mineo, Scan	SecureDoc imaging system
Engineering, Computer Science and Technology	Ess-ms1, ess-ms2, ess-ms3	Instructional
	Ess-msite	Instructional
Health Center	pnc-app, pnc-db, pnc-web (data center) and hc-data	Health Center system
University Advancement	Ccall01	Alumni Call Center
Library	Library E THSIS	Library system
	Library server	File/print
	Library X Mimas	Library system
Student Life	ccuser-smb-01	Career Center
	sa-smb-1	File/print
	All under AA-OB	OnBase
Enrollment Management Technology		

7.4 Verify Functionality

After restoring, verify environment and system functionality in the field.

Step	Task	Description	Completed By	Date and Time
1.	Verify PC capability.	Ensure that all personal computers are functioning correctly, and all critical LAN and modem connections are complete. Ensure appropriate application access.		
2.	Verify service provider connectivity.	Validate connectivity to CENIC and Unisys.		
3.	Verify operational readiness with all ITS departments.	Validate readiness of systems for users with all ITS departments.		

7.5 Recovery of ITS Services

The recovery procedures for the ITS Support Services are included in *ITS-9506 Internal Business Continuity Plan*.

Step	Task	Description	Completed By	Date and Time
1.	Assist the ITS Help Desk process recovery.	Assist the ITS Help Desk with technical recovery of their functions, if applicable.		
2.	Assist IT Security and Compliance process recovery.	Assist IT Security and Compliance with the technical recovery of their functions, if applicable.		
3.	Assist the ITS training unit process recovery.	Assist the ITS training unit with the technical recovery of their functions, if applicable.		

7.6 Return to Home Site

7.6.1 Prepare to Return to Home Site

Step	Task	Description	Completed By	Date and Time
1.	Meet with Facilities Services to plan return move.	Create and review a return home plan with Facilities Services. Confirm the location and time period for the final move. Set move date.		
2.	Identify environment requirements for restored or new data center.	Create a list of air, electrical and space requirements for a new data center, if applicable. Acquire vendors to perform the facility preparations.		
3.	Identify and install network communications.	Identify communications lines, fiber connections and telecommunications lines that require repair or installation. Order and install all communications hardware and software.		
4.	Plan the relocation or installation of technical resources.	Identify and coordinate the relocation or acquisition of required technical resources for the return move.		
5.	Verify the operational readiness with Facilities Services.	Report the status of the relocation plan to Facilities Services, ITS management team and the CIO / associate vice president for ITS. The CIO / associate vice president reports the status to campus management.		

7.6.2 Organize Backup Material for Home Site

Step	Task	Description	Completed By	Date and Time
1.	Review the configuration and address scheme.	Incorporate any changes that have occurred.		
2.	Identify files that need to be backed up for the home site.	Depending upon the similarity of configurations, full volume backups or file backups can be used.		
3.	Perform the appropriate backups for testing.	Backups will be from recovery site.		

7.6.3 Test and Return the Data Center to the Home Site

Step	Task	Description	Completed By	Date and Time
1.	Verify telecommunications and network connectivity.	Test connectivity to campus locations and service providers.		
2.	Perform system restorations at the home site with test backups.	Restore systems to any new hardware to test the conversion for move day. Follow systems recovery procedures outlined in this plan.		
3.	Plan the move day.	Prepare a relocation plan with Facilities Services and campus business areas.		
4.	Move from recovery site to the home site.	Follow the relocation plan. Validate operational activities once the return to the home site is completed.		
5.	List and track problems.	Use problem resolutions to update manuals, system or unit recovery procedures, or other disaster recovery documentation.		

6.	Update status with the ITS management team.			
7.	Prepare the post-recovery action report.	The ITS team leaders are responsible for completing *ITS-9809 Post-Disaster Recovery Action Report*.		

8. Contacts and Resources

a) For questions regarding this document, contact the director, IT Infrastructure or the assistant director, Network Operations Center, Servers and Technology Operations: itinfrastructure@calstatela.edu.

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

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

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

9. Reference and Recovery Documents

All procedures, diagrams, schemas, contracts and other 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. Documents are stored on the ITS emergency server, managers emergency laptops and cell phones, SharePoint Public Folders and multiple off-site locations.

ID/Control #	Title
Reference Documents	
NA	**Cal State L.A. Multi-Hazard Emergency Plan 2020-2021** Part I (calstatela.edu) This plan is designed to provide information to emergency response personnel and serves as an administrative guide outlining action steps for those offices and departments contributing essential services in emergency situations.
NA	**Pandemic Business Continuity Plan** pandemic_master_march_2020_0.pdf (calstatela.edu) The focus of this plan is to develop a level of preparedness and response to reduce the impact on University operations from a pandemic. General responsibilities and actions to be taken during each phase of any pandemic are articulated in this plan.

ID/Control #	Title
CCS Disaster Recovery Services Ltd. Contract	**CCS Disaster Recovery Services, Ltd.** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document outlines the steps to declare a disaster and initiate service and equipment restoration.

Campus EAI Disaster Recovery Plan	**Campus EAI Disaster Recovery Plan** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This document outlines the vendor's backup and restoration plan for the MyCalStateLA Portal.
CMS Disaster Recovery Plan	**CSU-Unisys Joint Backup and Restore Procedures** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This document outlines the backup and restoration plan for offsite CMS systems including the backup types, frequency and times.
NA	**Vendor Contact List** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This list provides the vendor name, contact person and telephone number for all vendors supporting systems, services, software and hardware for ITS.
NA	**ITS Server Spreadsheet** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document lists all physical and virtual servers housed in the data center.
NA	**ITS Data Center Diagram Visio.vds** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document visually locates all equipment housed in the data center.

NA	**Cal State LA Recovery Timeline** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document identifies critical ITS functions, the assets they support, estimated recovery time and responsible individuals.

Network Recovery Documents	
NA	**Network Systems List** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document uniquely identifies, locates and prioritizes restoration of all network devices.
NA	**Cal State LA Campus Network Diagram** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document graphically depicts the critical paths of the campus network.
NA	**Network IP and VLAN Schema** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document identifies the IP addresses for the campus DMZs and VLANs.
Telecommunications Recovery Documents	
NA	**Emergency Student Use Elevator Lines.xls** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document describes recovery procedures for campus elevator telephones.
NA	**Special Circuits.xls**

	Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document identifies all Cal State LA telephone and communications circuits.
NA	**Satellite Phone Installation** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document identifies the portable and antenna satellite phone assignments, Administration building roof layout, general usage, campus-specific dialing instructions, vendor information and detailed phone information.
NA	**Master Satellite Phone List** Available in electronic format on the cla-entsys-cdp.calstatela.edu (ITS Emergency Document Management server) server and all emergency laptops. This confidential document identifies all satellite telephone owners and telephone numbers on CSU campuses.