Business Continuity Plan for Information Technology Services				
	Document No.	ITS-9506-Web	Rev:	D
	Owner:	ITS Administration		
	Approved by:	Tosha Pham, Associate Vice President Information Technology Services		
	Issued:	12-2-10	Reviewed & Revised:	6-23-17
				Page 1 of 19

Table of Contents

1 Purpose

The ITS Business Continuity Plan describes how Information Technology Services responds to an event to ensure that its critical business functions will continue to serve campus constituents without unacceptable delay or change.

This document outlines the roles and responsibilities of the division and its employees toward ensuring that the division's most critical business processes can recover and operate while the ITS disaster recovery team is focused on restoring mission-critical campus administrative systems and infrastructure following a disaster or disruption. The plan also identifies non-essential ITS services that, if affected by the incident, will be suspended until normal campus operations resume.

The objective of the ITS Internal Business Continuity Plan is to reduce the consequences of a disruption to an acceptable level through:

- The execution of pre-established backup procedures for all units and individuals;
- Prioritized recovery instructions for each unit and if appropriate, the individuals within each unit; and
- Detailed interim operating procedures to ensure continuity of ITS business services to the campus.

2 Related California State University Policies and Standards

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

ID/Control #	Description	Title
8085.0.0	**Policy**	**Business Continuity and Disaster Recovery**

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

3 Entities Affected by this Document

Business continuity planning is the responsibility of every ITS employee. While backup and recovery of University administrative systems is an integral area of ITS disaster recovery, the division must also be capable of recovering and sustaining its most critical business processes in the shortest time possible. To accomplish this, each employee should consider his or her role within the division and ensure that appropriate preventive measures are taken for recovery and business continuity should a disaster or disruption occur.

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. Critical Business Function Categories: A prioritization of business functions that correlates to the duration of time required for recovery.

- Non-essential 30 days
- Normal 7 days
- Important 72 hours
- Urgent 24 hours
- Critical/essential 1-4 hours

c. 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.

d. Disaster Level: Classification according to severity that helps business continuity teams and disaster recovery teams determine the appropriate responses in a timely manner.

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

f. Disaster Recovery Team: The team comprised of ITS directors, associate directors, assistant directors, managers and technical staff who are responsible for executing tasks of the ITS Technical Disaster Recovery Plan.

g. Disaster Scope: The buildings, departments, outdoor areas, systems and services disrupted by the disaster that must be considered when determining the appropriate business continuity steps.

h. Disasters – Man-made: Man-made disasters include bombings, explosions, disgruntled employee actions, fires, purposeful destruction, aircraft crashes, hazardous or toxic spills, chemical contamination and malicious code.

i. Disasters – Natural: Natural disasters include earthquakes, floods, storms (lightening, hail, electrical, snow, winter ice), tornados, hurricanes, volcanic eruptions and natural fires.

j. Disasters – Political: Political disasters include terrorist attacks, espionage, riots, civil disturbances and strikes.

k. Disasters – System/Technical: System or technical disasters include hardware failure, software failure, programming errors and system failures.

l. Disasters – Supply Systems: Supply system disasters include communications outages, power distribution (i.e., brown-outs or black-outs) and broken pipes.

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

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

o. 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 associate vice president and four ITS directors who are responsible for leadership within their respective areas.

p. 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, project director and managers.

5 Levels of Disasters and Emergencies

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

5.1 Minor State

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

Examples include the temporary loss of network connectivity, data center servers, portal access, access to cloud-based services, the ITS Help Desk LANDesk system, switchboard or telephone service.

5.2 Intermediate State

Intermediate incidents occur less frequently but with greater impact than minor incidents. These incidents impact portions of the campus, disrupt normal operations of some but not all critical business units and generally result from major failures of multiple systems and equipment. ITS would activate a subset of the ITS disaster recovery plans.

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

5.3 Major State

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

Examples include fires, floods, earthquakes and sabotage.

6 Scope of Disasters and Emergencies

In addition to determining the disaster level and before initiating its internal business continuity plan, ITS must assess the scope of the disaster or emergency. The pervasiveness and locations affected by the incident will also determine what ITS services require alternate delivery methods, if any. Unlike the ITS disaster recovery plans, which may be activated for disaster incidents located anywhere on campus, the business continuity plan only needs to be activated when the incidents occur in physical locations where ITS services are provided or the systems that provide ITS services are disrupted.

Following are the disaster scopes affecting ITS business processes:

1. Entire campus
2. Data center
3. Library North basement
4. Library Palmer Wing, all ITS offices
5. Administration building or the switchroom

7 ITS Services Available During Disaster Recovery

In preparation for a disaster or emergency, ITS must determine which of its services will need to be sustained throughout the disaster recovery period. All ITS units and services in this section were prioritized for business continuity operations based upon:

a. The critical need for continued service to the campus during a disaster.
b. The critical need for the unit itself to be fully functional.
c. The availability of the unit or its employees who are responsible for executing the ITS disaster recovery plan and will therefore not be able to concurrently provide other ITS services.

7.1 Priority 1 - Critical and Urgent ITS Units and Services

Critical ITS units and services play an important role during the initial disaster recovery period by informing the University of the status of ITS systems recovery, offering communications vehicles to disseminate timely information, coordinating the ITS business continuity and disaster recovery processes, and if necessary, securing electronic data. In the event that normal operations are affected, these units and services will follow the alternate operating plans outlined below.

7.1.1 ITS Help Desk

The ITS Help Desk is located in the Library PW Lobby and will serve as the coordinating department to receive user work and outage requests during the business continuity period. In the event the physical location is affected by the event, services will be reestablished in a safe, secure location. The incident management system's trouble ticket capability will be transferred manually to laptop computers during the event through the use of form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity*, and returned to ServiceNow at the incident conclusion.

7.1.2 Switchboard and PBX

A single PBX provides telephone service for the entire campus. The University switchboard routes callers who do not have the direct-dial number for their contact. During disaster recovery, if operable, the switchboard will serve as one communications point for incoming callers and will provide scripted information to callers on the status of the University and its recovery.

A major incident that destroys or renders the PBX unusable will require vendor intervention to install a small, temporary PBX capable of handling basic telephone service for essential University departments. IT Infrastructure Services is responsible for declaring an emergency state and activating the ITS disaster recovery plan. Normal telephone communications will not be available during this period.

7.1.3 ITS Alerts, Twitter and Advisories

ITS will provide email and social media notifications regarding system status for outages, maintenance, upgrades and incidents, and information security warnings about viruses, scams, fraud and phishing. When appropriate or necessary, ITS will email alerts and advisories to students, faculty and staff. Interested parties may also follow @mycalstatela on Twitter for up-to-the-minute information about ITS.

7.1.4 Web Services

The University web home page will serve as one communications method during an incident. The University web management system is hosted remotely, and will not be affected by a campus incident. Webpages remaining on the local web server will be unavailable until system restoration is completed

7.1.5 Associate Vice President's Office

The ITS associate vice president's office is the central ITS communications center during disaster recovery. Ongoing communications between the associate vice president for ITS and the vice president for Administration/CFO and ITS directors is by cell phone or text message. The administrative assistant to the associate vice president receives messages and requests from other University departments, administrators and vendors, forwards them to the associate vice president or designee and determines when direct communication between parties is required.

7.1.6 Information Security and Compliance

Following certain incidents and at the direction of University Counsel or Public Safety, IT Security and Compliance may be requested to assist with electronic investigations. The director of IT Security and Compliance or designee shall follow all standard procedures and protocols for obtaining and securing electronic data. Collected electronic data will be stored in a secured location until directed to submit the results of the investigation to law enforcement.

7.2 Priority 2 - Normal ITS Units and Services

Normal units and services play an important role in returning the University to its former operational state but do not provide critical or urgent services during disaster recovery. Some or all of these units will be fulfilling their respective roles through execution of the ITS disaster recovery plan, and as a result, the affected services will be returned to normal. But some services may be important to the recovery process and will require the actions or alternate processing methods described below during the incident recovery phase.

7.2.1 University Email

Email servers are hosted remotely and service will not be affected by a campus incident. Access to email will be available even if the incident affects the authentication servers because the University will sync to Azure AD for O365 email authentication. Operational readiness of the campus networks may impact users' ability to access the email servers from on-campus, however, if the authentication servers are unaffected, remote access is available from any functional internet access point, cell connection or Wi-Fi hot-spot.

7.2.2 GETmobile

During a minor or intermediate incident that does not affect the campus network and authentication server, GETmobile functions will remain accessible to users. If damage has occurred during a major incident, normal service will be restored as the server and network are restored.

7.2.3 Open Access Labs (OALs)

Open Access Labs in any and all areas affected by an intermediate or major incident will be secured and evaluated for safety prior to reopening. Client Support Services, Desktop Services and Baseline Services Groups, Visual and Media Support and IT Infrastructure Services employees not involved in conducting ITS disaster recovery procedures will begin work to restore the labs. All OALs not damaged and determined to be safe will reopen as deemed appropriate when normal University operations resume.

In the event a single OAL is rendered unusable or a portion of campus OALs are damaged during an incident, Client Support Services staff who normally supervise OAL activities will begin recovery planning. Staff assigned this task will work with the Desktop Services and Baseline Services to:

- Determine if the computers, printers, furniture and other lab equipment are usable, repairable or require replacement.
- Prepare purchase requisitions for replacement equipment and furniture.
- Submit work orders to Facilities for physical repairs.
- Utilize usage statistics to:
    - Determine if the affected lab can remain closed without impacting students during the reconstruction period, or
    - Determine if the lab needs to be reopened in an alternate location.
    - Identify a new location, if needed, and begin temporary implementation.
- In conjunction with Visual Media and Graphics Services staff, prepare any signage and handouts necessary to alert students to OAL closures or temporary facilities.
- Issue an ITS Alert and a tweet to notify the campus of the lab closure or alternate lab locations

7.2.4 Electronic Classrooms (ECs)

Electronic Classrooms in any and all areas affected by an intermediate or major incident will be secured and evaluated for safety prior to reopening. Desktop Services Group, Baseline Services Group, Visual and Media Support, Classroom Media Support and IT Infrastructure Services employees not involved in conducting ITS disaster recovery procedures will begin work to restore the ECs. All ECs not damaged and determined to be safe will reopen immediately when normal operations resume.

In the event a single EC is rendered unusable or a portion of ECs are damaged during an incident, IT Infrastructure Services staff who normally supervise EC activities will begin recovery planning. Staff assigned this task will:

- Determine if the computers, furniture and other lab equipment are usable, repairable or require replacement.
- Prepare purchase requisitions for replacement equipment and furniture.
- Submit work orders to Facilities for physical repairs.
- Work with the Scheduling Office to:
    - Determine if the affected classroom can remain closed without impacting students during the reconstruction period, or
    - Determine if the classroom needs to be reopened in an alternate location.
    - Identify a new location, if needed, and begin temporary implementation.
- In conjunction with Visual and Media Support, prepare any signage and handouts necessary to alert students to EC closures or temporary facilities.

7.2.5 Technology Enhanced Classrooms (TECs)

Technology Enhanced Classrooms (TECs) in any and all areas affected by an intermediate or major incident will be secured and evaluated for safety prior to reopening. Desktop Services, Visual and Media Support, Baseline Services, Classroom Media Support and IT Infrastructure Services employees not involved in conducting ITS disaster recovery procedures will begin work to restore the TECs. The TECs not damaged and determined to be safe will reopen immediately when normal campus operations resume.

In the event a single TEC is rendered unusable or a portion of TECs are damaged during an incident, IT Infrastructure Services staff who normally supervise TEC activities will begin recovery planning. Staff assigned this task will:

- Determine if the computers, furniture and other lab equipment are usable, repairable or require replacement.
- Prepare purchase requisitions for replacement equipment and furniture.
- Submit work orders to Facilities for physical repairs.
- Work with the Scheduling Office to:
    - Determine if the affected classrooms can remain closed without impacting students during the reconstruction period, or
    - Determine if the classroom needs to be reopened in an alternate location.
    - Identify a new location, if needed, and begin temporary implementation.

- In conjunction with Visual and Media Support, prepare any signage and handouts necessary to alert students to TEC closures or temporary facilities.

7.2.6 Desktop Services Group (DSG)

While Desktop Services staff will be busy with ITS disaster recovery tasks, they will continue to work closely with the Baseline Services Group to ensure that correct Baseline computer and images are deployed to critical areas that need them. DSG will also provide technical support and assistance when imaging fails, and when additional applications or additional configurations are needed.

7.2.7 Baseline Services Group (BSG)

The Baseline Services staff will assist with critical services to relocated departments and users, and assist with computer set-ups. Staff will also assist departments with purchase requisitions for replacement computer equipment, receipt of the equipment and set-up within the department's permanent or temporary location. Baseline staff will assist the DSG staff with setup and reimaging needed systems.

First priority of Baseline services will be provided to the Essential Business Units identified in the *System Backup and Recovery Plan and Business Unit Resumption Guidelines* (Report No ITS-R03-2, November 7, 2003).

Essential Business Units

The campus identified four (4) essential business units for providing business services during an unplanned disruption of data processing services. There is no intended priority to the order of the following list, since the nature of any unplanned disruption and the campus disaster and contingency plan would determine whether all or only some units would continue to operate.

1. *Student Admissions/Registration*
2. *Cashiering*
3. *Accounts Payable*
4. *Purchasing*

Two additional Essential Business Units were subsequently identified and added to the list.

5. *Public Safety*
6. *Student Health Center*

All other departments requiring Baseline services will be prioritized on a first-come, first-serve basis. Exception requests to any scheduled priorities can be addressed to the vice president for Information Technology Services.

7.2.8 ATI E&IT Procurement Approval Process

As owners of the business process, Procurement and Contracts is responsible for accepting and evaluating form *ATI-4801 Electronic and Information Technology (E&IT) Procurement Requests*. ITS. ITS serves as a participant in the review and approval process. Procurement and Contracts may or may not process these requisitions and forward them to ITS for review during an emergency event.

Apart from emergency purchase requisitions related to disaster recovery for ITS and any other University departments that require immediate replacement of technology products to restore their business processes, ITS will not review or approve any general *Electronic and Information Technology (E&IT) Procurement Requests* (form ATI-4801) during major state disaster recovery.

Emergency requisitions can be delivered to the assistant to the associate vice president for Information Technology Services or designee in LIB PW 1070, who is responsible for logging the request and obtaining approval from the associate vice president or his designee. If the LIB PW 1070 work area is unavailable, an ITS Alert, tweet or other communication will be sent to notify the University of the alternate delivery location.

7.2.9 PBX Call Accounting Collection

Call accounting records are gathered by an appliance connected to the PBX and subsequently processed by a Windows server that reads the records from the appliance and processes them into usage chargebacks by reporting unit.

There are two collection devices for redundancy in case of an equipment failure. In the event of a disaster that caused both to fail, recording of call records would resume after the equipment is replaced. The server that processes the call records for billing will be restored to service as part of the ITS disaster recovery plan.

Responsibility for equipment recovery or replacement and resumption of call collection resides with Network and PBX Operations in IT Infrastructure Services.

7.3 Priority 3 - Non-essential ITS Units and Services

Non-essential units and services do not serve a supporting role during a disaster or disruption. This does not indicate that they are not important to ongoing University operations, but these non-essential or non-critical services are not key priorities during a disaster or disruption. Employees in these units and services may be reassigned to other duties as outlined in *ITS-7502 ITS Technical Disaster Recovery Plan* or *ITS-9507 ITS Management Disaster Preparedness Plan*.

The following services may not be affected by the incident and may therefore remain available; however, if disrupted, they will **not be provided during a major disaster recovery period**.

7.3.1 *MyCalStateLA Portal*

If the incident does not affect the Library North, the data center or the web server, the portal will remain available to provide recovery status to students. If the incident affects any or all of these areas, the portal will not be available during the disaster recovery period. The *MyCalStateLA Portal* and single sign-on applications through the portal will be restored during disaster recovery restoration of the campus servers. Information regarding the recovery status will be available through other communications methods. Refer to section 7.1.4 Web Services for further information.

7.3.2 ITS Training

The ITS Training Center in the Library Palmer Wing, 4th floor will be secured during major disaster recovery and staff may be reassigned to other duties. In the event the training center or equipment is damaged, Baseline Services and Desktop Services are responsible for evaluating damage and procuring replacement equipment. The director of Client Support Services is responsible for identifying alternate space during the reconstruction and overseeing the restoration after all other Client Support Services disaster recovery tasks have been completed. Training workshops for students, faculty and staff will not be available during major disaster recovery.

Online training offered by external resources, such as Lynda.com, will remain available from any location with internet access provided the incident has not affected campus authentication servers and the external resource. *MyCalStateLA YouTube* training will remain available if the incident does not affect external resources.

7.3.3 Visual and Media Support

The media studios will be secured during major disaster recovery and staff may be reassigned to other duties, including, but not limited to, developing and distributing incident signage, handouts, posters and communications. In the event the media studio or equipment is damaged, the director of Client Support Services is responsible for evaluating damage, procuring replacement equipment, identifying alternate office space during the reconstruction, and overseeing the restoration after all other Client Support Services disaster recovery tasks have been completed. The Visual Media Center will not be available for general campus use during major disaster recovery.

7.3.4 Telecommunications Chargebacks

If the incident does not affect the Administration building or the PBX switchroom, the PBX call collection appliances will continue to collect and store outgoing call data. Monthly processing of user charges will be suspended during major disaster recovery and will resume as soon as the campus returns to normal operations. ITS will not process telecommunications charge backs manually. The impact on departments will be a delay in these charges appearing on monthly budget reports.

If the incident affects the Administration building or the PBX switchroom, the status of the redundant call collection devices will be evaluated by IT Infrastructure Services after telephone service is restored. The call data and billing information is processed by a server in the PBX switchroom and this server is backed up as part of normal ITS backup procedures. If the call data is intact, ITS will resume telecommunications chargebacks when the campus returns to normal operations. In the event that call data is compromised, ITS will notify the University that chargebacks for the outage period will be a) delayed while alternative data is acquired or b) suspended for lack of data.

7.3.5 FERPA Testing and Certification

The online FERPA website, including the interactive test and certificate printing, resides on a secured server in the data center. In situations where the data center, web server and network communications remain intact, this service will remain available. If any one or all of these services are disrupted, FERPA training will remain unavailable until full restoration occurs. ITS will not provide FERPA training by alternate methods during disaster recovery.

7.3.6 Invoice Receipt, Approval and Payment

During minor and intermediate incidents that do not affect department offices, invoice receipt, approval and payment will continue as normal. During major incidents, ITS will not process any invoices. Any invoices already in the ITS approval process will be secured in the associate vice president's office during disaster recovery and approved invoices will be returned to the Business Financials office when normal operations resume.

7.3.7 *MyCalStateLA ID Identity*, Network and Email Account Requests

During minor and intermediate incidents, ITS will continue to receive and process the new *MyCalStateLA ID* account requests that are automatically generated by the identity management system provided the minor or intermediate incident does not affect the network, data center, Enterprise Applications or the *MyCalStateLA ID* server. During minor and intermediate incidents, ITS will not process new account requests that are submitted on printed forms.

During major incidents, ITS will not process any new *MyCalStateLA ID*, network or email account requests, automatically generated or printed forms, since the systems will be unavailable and personnel resources will be focused solely on disaster recovery. Departments should retain the new account requests for submission after normal operations are restored. If the network is unaffected and emergency network access is required, the requesting department administrator should contact the associate vice president for Information Technology Services for assistance.

7.3.8 Administrative System Account Requests

During minor and intermediate incidents, ITS will continue to receive and process approved account requests provided the minor or intermediate incident does not affect the Library North, data center, local administrative system servers or CMS remote servers. During major incidents, ITS will not process new administrative system account requests or modification requests since personnel resources will be focused solely on disaster recovery. Departments should retain these requests for submission after normal operations are restored.

7.3.9 Budget Reporting

During minor or intermediate incidents, ITS will continue to process budget-related tasks (e.g., requisitions, chargebacks, reports, spreadsheets) and submit quarterly budget assessments as required. During major incidents, ITS will not maintain budget activities but will retain all budget-related documentation. Budget information will be manually re-entered into the ITS budget database when ITS operations resume. For this reason, ITS will not submit semester reports during a major incident, but will resume budget reporting when normal campus operations resume.

7.3.10 Data Warehousing

During minor, intermediate and major incidents that do not affect the network, Library North, the data center or local ITS servers used to house GET reporting data, data warehousing will remain available to the University. If any one or all of these areas are affected, data warehousing will not be available until disaster recovery procedures are complete and the normal operations resume.

8 Tasks and Procedures for Business Continuity

8.1 Immediate Response

The ITS management team is the first-line responder for any incident and is responsible for assessing and evaluating the incident to determine if the *ITS Technical Disaster Recovery Plan* should be started. The ITS management team is responsible for enacting all immediate preparations.

8.2 Environmental Restoration in an Alternate Site

The ITS management team is responsible for enacting a declaration to resume business at an alternate site.

8.3 Functional Restoration in an Alternate Site

Functional restoration tasks are undertaken concurrently, not sequentially, so it is important that all functions are assigned to the appropriate individuals at the start of the function restoration. The ITS team leaders are responsible for performing or assigning the functions.

8.4 Verify System Functionality

Systems include both ITS employees' computers with their respective applications and data and any software applications specific to the work unit (e.g., incident management system, University telephone directory). Baseline Services, Desktop Services and ITS employees are responsible for this task.

8.5 Resumption of ITS Business Processes in an Alternate Site

After the ITS team leaders complete restoration and testing all support functions, and verifying the integrity of the data files, resume ITS business processes.

8.6 Return of Business Processes to Home Site

The ITS team leaders are responsible for performing or assigning restoration tasks.

9 Business Continuity Pre-planning and Advance Preparation

ITS directors and managers provide guidance to ITS employees under their supervision regarding the individual and unit responsibilities for maintaining normal ITS business processes during a disaster recovery period. Some employees will be responsible for specific disaster recovery tasks while others will be assigned responsibility for carrying out the business continuity tasks outlined herein.

This section covers the recommendations that must be considered and implemented in advance to ensure that business continuity can begin promptly following an incident. Not all ITS employees will have the same planning and preparation requirements, so managers must determine the best business practices for their respective areas and inform each employee of his or her responsibilities.

9.1 Department System and Database Backups

In some situations it is advisable to back up important department data to an ITS server that is in turn backed up and stored remotely. Currently documents necessary for disaster recovery (e.g., network configurations, emergency contact lists, critical restoration procedures, etc.) are backed up on a department server and in the cloud. But managers should identify other critical business processes (e.g., financial databases and budget reports, campus directory database, personnel information, media signs and flyers, training materials, etc.) for their areas and ensure that those are also replicated in a safe, secure area.

Backing up important department information to a server is a sound business practice. However, when doing so, consider whether that data will be needed immediately during a disaster or whether it can wait for later recovery. Critical University services and systems (e.g., network, email, web and administrative systems) will have first recovery priority. Data center servers used to backup department or individual's files are a much lower priority and in a major disaster involving extensive damage, may not be available for up to 7 to 10 days. Backups of all critical campus systems are stored off-site and will need to be returned for recovery, again adding a wait-period for restoration. If files will be needed immediately, it is recommended that staff also perform a daily backup as described in section 9.2.

9.2 Individual Workstation Backups

Every ITS employee with a computer has documents and data that are crucial to performing his or her daily work. In the event that a computer, office or building is destroyed or secured against access, every employee needs an accessible backup of all documents and data in order to restore his or her work to a new computer or a new location. This requirement is outlined in every ITS employee's position description.

Workstation backups require thought and careful planning. Backup requirements will not be the same for every ITS employee. Consider the following:

- Are there any critical ITS business processes on the computer, (e.g., one-of-a-kind documents, financial information, budget spreadsheets or reports, personnel data, project plans and files, test results, media campaigns, surveys, department process mapping, system drawings and diagrams, usage charge backs or cost center information) that, if destroyed, would affect the division's ability to continue business?
- Is this employee's work mission-critical and does it require daily backup to the cloud?
- Will these business processes need to continue during disaster recovery or will anyone need to see the data files during the recovery? Or can access wait until normal operations resume?
- Is the data from these critical business processes currently being backed up on a server? And if it is, can the employee afford to wait 7 to 10 days for recovery should a major incident occur?
- If it is backed up to a server and the data center is destroyed or becomes inaccessible, how will the employee continue working?

- If the entire University is closed due to the severity of the disaster, can the employee continue normal work routine from an alternate location?
- Is the entire data content on the computer backed up to a server? If not, can the employee afford to lose the data that is not currently backed up?
- Is there Levels 1 or 2 confidential data on the computer?
- Are all documents and databases containing Levels 1 and 2 confidential data encrypted?

  Does the employee need every document on the computer or just selected documents to resume work?
- Is the computer already backed up daily? Weekly? Monthly? Is the backup schedule adequate to ensure that valuable files will not be lost?
- If the data is backed up on an electronic storage device, is it secure should the device be lost or stolen?
- Does the employee's director or a designated system administrator have access rights (i.e., password, scanned fingerprint) to the electronic storage device should the employee not be available to access the backup copy?
- Is the electronic storage device backup copy stored in a secured, alternate location that enables the employee to readily retrieve it should the office or building be inaccessible?

9.2.1 Frequency of Computer Backups

Computer backups can be completed daily, weekly or monthly. The frequency of backups correlates to the criticality of the computer's data content. Directors and managers are responsible for working with each employee within their respective areas to determine if computer backups are required and if so, how frequently.

Daily backups are recommended because it's relatively easy and daily backups ensure files are always readily retrievable. Either or both of the following options are recommended.

- Option 1 – Use Windows Explorer to drag-and-drop documents and files as they are updated throughout the day to an electronic storage device.
- Option 2 – Use the Microsoft OneDrive available through Microsoft Office 365 Outlook Web App (OWA) to back up documents and files in the cloud. Instructions are online at http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/training/pdf/onedrive.pdf

Weekly or monthly backups of the entire data folder to the electronic storage device or Microsoft OneDrive can further ensure that no files are missing should an incident occur.

9.2.2 Acceptable Electronic Storage Media

There are two acceptable electronic storage devices for ITS employee computer backups – external hard drives and flash drives. Both drives must be encrypted or otherwise protected (e.g., biometrics, password protected) to ensure all documents are secure in the event the drive is lost or stolen. Biometric hard drives are preferable. IT Security and Compliance can provide guidance on specific approved products.

CDs and DVDs are not acceptable for employee computer backups due to their limited storage capacity, the requirement for individual files containing protected data to be encrypted prior to backup and the high probability for loss or damage.

Managers and other ITS employees with ITS-issued emergency laptops should use these password-protected, biometric laptops to back up desktop computers if the laptop is not used as the manager's primary workstation. Again, files containing protected data must be encrypted on the desktop computers.

9.2.3 Encryption

All ITS employees should be knowledgeable regarding encryption standards and techniques, and the types of Levels 1 and 2 confidential data documents on their computers that require encryption. *ITS-1027-G User Guidelines for Encryption Security* details these requirements. An up-to-date list of recommended encryption tools is available at:
http://www.calstatela.edu/its/services/software/encryptiontools.php

9.2.4 Working Remotely

The associate vice president, directors and managers are responsible for issuing work assignments during disaster recovery or business continuity periods. During major incidents, some employees not required to be on-site may be requested to continue work from an off-campus location, such as a temporary office space or home office. At least one form of communications (i.e., email, telephone, cell phone) between the off-campus site and the campus must be in place for remote work to be approved.

Tasks directly related to disaster recovery system restoration or Priority 1 Critical and Urgent Units and Services cannot be performed remotely. Examples of tasks that might be approved for working remotely include: writing campus communications, manning phones at a remote call center, updating and issuing recovery status reports, updating web pages, creating and printing handouts for campus wide distribution, receiving or delivering equipment or other items.

Employees may not work remotely unless specifically assigned and authorized to do so by their respective director or the associate vice president for Information Technology Services.

Employees working remotely on personal computers must adhere to information security best practices. Unencrypted confidential documents must not be saved to personal computers used by others. All work must be backed up on the employee's acceptable electronic storage device so it can be restored to the employee's office computer when normal business operations resume.

9.3 Emergency Laptops

A biometric/password protected emergency laptop has been issued to each ITS manager and other designated employees who serve in an exempt, critical system support role. These laptops remain in their personal possession at all times and travel from office to home, which ensures that these employees have access to critical information in the event the disaster occurs during off-hours. All critical, updated disaster recovery and business continuity documents, emergency contacts, network diagrams, internal procedures, forms and other important ITS documents and information that may become unavailable during an incident reside on an ITS emergency server (Availl) and the ITS SharePoint cloud site. Most of this information is confidential and/or proprietary and must not be shared with individuals unauthorized to view the information.

Each ITS director is responsible for posting relevant new and updated documents to the ITS server and the cloud immediately upon completion. Laptop owners are strongly encouraged to minimally perform weekly synchronizations with the server in the event that server or cloud access is unavailable during an emergency. Laptop owners should update the laptop more frequently (e.g., daily) if it is determined to be needed. Desktop Services Group provides user assistance with the backup and synchronization processes as needed.

10 Emergency Contacts

During business continuity and disaster recovery processes, the following ITS management team will respond to the noted questions, issues and requests for information.

a) **Associate Vice President for Information Technology Services:**

Office Phone: 323-343-2704

Contact for: Second-level contact for all ITS services and systems, and updates on the status of ITS disaster recovery measures.

b) **Director, IT Infrastructure Services:**

Office Phone: 323-343-2676

Contact for: Campus wired and wireless networks, email servers, web servers, all ITS-managed department servers and general technology issues.

c) **Assistant Director, Network Operations Center:**

Office Phone: 323-343-2629

Contact for: Campus wired and wireless networks, email servers, web servers, all ITS-managed department servers, classroom media support and general technology issues.

d) **Assistant Director, Baseline Services:**

Office Phone: 323-343-2643

Contact for: Desktop hardware and software, desktop computer restoration and imaging, Electronic Classrooms (ECs) and Technology Enhanced Classrooms (TECs).

e) **Assistant Director, Baseline Services:**

Office Phone: 323-343-2643

Contact for: Desktop hardware and software, desktop computer restoration and imaging, Electronic Classrooms (ECs) and Technology Enhanced Classrooms (TECs).

f) **Manager, Network and PBX Operations:**

Office Phone: 323-343-2665

Contact for: PBX, switchboard, call accounting and LAN/WAN problems.

g) **Director, Client Support Services and Training**

Office Phone: 323-343-2573

Contact for: ITS Help Desk, Open Access Labs, web services, ITS training and documentation, and media and graphics services.

h) **Manager, Technology Client Services**

Office Phone: 323-343-4533

Contact for: ITS Help Desk, Open Access Labs.

i) **Director, Enterprise Applications:**

Office Phone: 323-343-2651

Contact for: CMS, auxiliary systems, data warehousing and business intelligence.

j) **Assistant Director, Enterprise Applications**

Office Phone: 323-343-2611

Contact for: Second-level contact for CMS, auxiliary systems, GETmobile, data warehousing and business intelligence.

k) **Director, IT Security, Compliance and Training:**

Office Phone: 323-343-4534

Contact for: Information security issues and investigations, fiscal services and ITS administrative support.

l) **Director, ITS Projects:**

Office Phone: 323-343-2706

Contact for: Second-level contact for updates on the status of ITS disaster recovery measures.