Internal Business Continuity Plan	Document No.	ITS-9506	Rev:	G
	Owner:	ITS Administration		
	Approved by:	Tosha Pham, Associate Vice President Information Technology Services		
	Issued: 12-2-10	Reviewed & Revised:		09-29-2021
				Page 1 of 41

Table of Contents

1 Purpose

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

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

The objective of the ITS Internal Business Continuity Plan is to reduce the impact of an unexpected 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 University.

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**

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 are 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 take appropriate preventive measures 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 an organization’s resulting financial and operational impacts become 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 is 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 (lightning, hail, electrical, snow, and 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 is responsible for first-line response to any incident, 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 is 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 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 incident management system, switchboard or telephone service.

5.2 Intermediate State

Intermediate incidents occur less frequently but with greater impact than minor incidents. These incidents impact portions of the 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 execute relevant components of the ITS disaster recovery plans.

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

5.3 Major State

Major incidents have a low possibility of occurring, but the extent has a 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 will require alternative 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 University 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 in a position 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

7.1.1.1 Minor State

Scenarios	Actions
ITS Help Desk is not affected	Business operations will continue normally.
Loss of all ITS Help	ITS Help Desk will initiate a trouble ticket to IT Infrastructure Services who in turn will contact the onsite vendor for remediation, marking this a

Desk telephones	high priority restoration.
	ITS Help Desk staff will continue to assist those at the counter.
	Campus operators will remotely log in to the cloud based ITS Help Desk call center and continue to pick up calls received for the main University (3-3000) line.
	ITS will tweet from @mycalstatela and send an email to notify the campus of the temporary loss of telephone service and state that callers can be assisted by emailing helpdesk@calstatela.edu, calling the ITS main office at 3-2600, or tweeting to @mycalstatela. If those options are unavailable, users may be instructed to come to the walk-up counter.
Loss of computers and/or incident management system	ITS Help Desk will manually create a trouble ticket using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* and submit it to IT Infrastructure Services who will begin remediation.
	ITS Help Desk staff will handle incoming requests as normal using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity*.
	ITS Help Desk staff will manually enter hard-copy *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* data into the incident management system when the system is recovered.

7.1.1.2 Intermediate State

Scenarios	Actions
ITS Help Desk is not affected	Business operations will continue normally.
Loss of all ITS Help Desk telephones	ITS Help Desk will initiate a trouble ticket to IT Infrastructure Services who will contact the onsite vendor for remediation, marking this a high priority restoration.
	If the phones are non-functional but the lines are functional, the ITS Help Desk staff will be relocated to the main office in LIB PW 1070 and log into CxEngage, the ITS Help Desk cloud telephone support system.
	ITS Help Desk staff will continue to assist those at the counter.
	Campus operators will remotely log in to the cloud based ITS Help Desk call center and continue to pick up calls received for the main University (3-3000) line.
	ITS will tweet from @mycalstatela to notify the campus of the temporary loss of telephone service and state that callers can be assisted by emailing helpdesk@calstatela.edu, calling the ITS main office at 3-2600, or tweeting to @mycalstatela. If those options are unavailable, users will

	be instructed to come to the walk-up counter.
	Alternate available communications (i.e., web, portal, phone broadcast, email) will be used to notify the University of the temporary loss of service and provide instructions for contacting the ITS Help Desk. Help Desk Manager will log onto the cloud-based call system and turn on the emergency message that states “Thank you for calling the ITS Help Desk. Due to an unexpected outage, no one is available to assist you at the moment. Please press 1 to leave a voicemail and we will get back to you as soon as possible.”
Loss of computers and/or incident management system	ITS Help Desk will manually create a trouble ticket using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* and submit it to IT Infrastructure who will begin remediation.
	ITS Help Desk staff will handle incoming requests as normal using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity*, which replicates the incident management system screens.
	ITS Help Desk staff will manually enter hard-copy *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* data into the incident management system when the system is recovered.

Loss of work area	IT Infrastructure will identify an alternate work area and install telephones. ITS Help Desk phone lines will be forwarded to the alternate work area.
	Baseline and Desktop Services Groups will relocate the existing computers to the alternate work area or, if they are inaccessible or damaged, will install backup computers from stock or other available locations.
	ITS Help Desk staff will handle incoming requests as normal using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* until the new computers are functional and then manually re-enter form content when the new work area is complete.
	ITS will issue a tweet from @mycalstatela and send an email to notify the University of the alternate work location.
	Visual and Media Support will create and post signage and posters directing users to the new location.

7.1.1.3 Major State

Scenarios	Actions
ITS Help Desk is not affected	Business operations will continue normally.
ITS Help Desk is affected, and the University remains open	ITS will activate the ITS disaster recovery plan. Recovery of the ITS Help Desk systems will be priority level 2, following recovery of critical campus systems.
	If the University remains open, communications methods remain intact, and the ITS Help Desk workplace is unaffected, staff will continue to handle in-person, telephone, Twitter and email requests related to the disaster or emergency.
	If the University remains open, the ITS Help Desk workplace is unaffected, but communications methods are unavailable, staff will continue to handle in-person requests.
	If the incident management system is unavailable, ITS Help Desk staff will handle incoming service requests as normal using form *ITS-4823 ITS Help Desk Support Ticket for Business Continuity*. Forms will be sequentially numbered to ensure no requests are lost and securely stored in the ITS Help Desk manager's office for later data entry.
	ITS Help Desk staff will manually re-enter all hard-copy *ITS-4823 ITS Help Desk Support Ticket for Business Continuity* data into the incident

Scenarios	Actions
	management system when the system is recovered.
	If the ITS Help Desk workplace is damaged or destroyed, the ITS Help Desk will be relocated to another safe location, e.g., the Annex Link or work from home. • Desktop Services and the Baseline Services Groups will oversee installation and imaging of computers. • Desktop Services and Baseline Services Groups will move or install new printers. • IT Infrastructure Services will oversee installation of telephone lines. • Network Services will provide access for email account maintenance and password resetting. • Enterprise Applications will provide access for administration account maintenance and password resetting.
	Campus operators will remotely log in to the cloud based ITS Help Desk call center and continue to pick up calls received for the main University (3-3000) line.
	ITS will issue a tweet from @mycalstatela and send an email to notify the University of the new location, contact information and full recovery status.
	Alternate available communications (i.e., web, portal, phone broadcast, email, posters and signage) will be used to notify the University of the temporary location and any other relevant information.
ITS Help Desk is affected, and the University is closed	ITS Help Desk services will be conducted remotely using ServiceNow and the cloud-based call system.
	The associate vice president for ITS will provide status and contact information to Public Affairs for posting on the university web page.
Regional disaster	ITS Help Desk services will be conducted remotely using ServiceNow and the cloud-based call system.

7.1.2 ITS Alerts 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.

7.1.2.1 Minor State

Scenarios	Actions
Hosted email systems or University networks are not affected.	Email notifications, alerts and advisories will be available.
University networks are unavailable.	If the University network is not available, Tweets will continue using cellular service.
Twitter or University networks and cellular services are unavailable.	If Twitter and/or the University network and cellular service is not available, no tweets will be issued. Given the temporary outage during a minor state, no other communications methods will be used.

7.1.2.2 Intermediate State

Scenarios	Actions
Hosted email systems or University networks are not affected.	Business operations will continue normally.
Twitter or University networks are unavailable.	If Twitter and/or the University network is not available, no tweets will be issued.

7.1.2.3 Major State

Scenarios	Actions
Hosted email systems or University networks are not affected.	Business operations will continue normally.
Twitter or University networks are unavailable.	If Twitter and/or the University network is not available, no tweets will be issued. The associate vice president for ITS will provide periodic disaster recovery updates to Public Affairs for distribution of general status reports.

7.1.3 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 a local web server will be handled as follows.

7.1.3.1 Minor State

Scenarios	Actions
The web server is not affected.	Business operations will continue normally.
The web server is affected.	IT Infrastructure Services will remediate the problem.
	ITS will notify the site owners affected.

7.1.3.2 Intermediate State

Scenarios	Actions
The web server is not affected.	Business operations will continue normally.
The web server is affected.	ITS will activate a subset of the ITS disaster recovery plan.
	ITS will notify the site owners affected.

7.1.3.3 Major State

Scenarios	Actions
The web server is not affected and the University remains open.	Business operations will continue normally.
	Public Affairs will write and post emergency status reports, which will be posted on the campus home page.
The web server is destroyed or inaccessible and the University is closed.	ITS will activate the ITS disaster recovery plan.
	ITS will work with the site owners affected.
	University webpages will be unavailable during the recovery and will be restored when normal business operations resume.

7.1.4 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.

7.1.4.1 Minor State

Scenarios	Actions
AVP ITS office is not affected.	Business operations will continue normally.
AVP ITS office is affected.	The associate vice president's and administrative assistant to the associate vice president's office phones will be forwarded to an available office within ITS.
	The associate vice president will communicate by cell phone.
	ITS Desktop and Baseline Services Groups will relocate both desktop computers to the alternate location if the incident is predicted to last longer than four hours.
	Visual and Media Support will create and post signage and posters directing users to the new location if it is determined that the relocation is expected to last longer than one working day.

7.1.4.2 Intermediate State

Scenarios	Actions
AVP ITS office is not affected.	Business operations will continue normally.
AVP ITS office is affected.	The associate vice president will communicate primarily by cell phone since she will likely be working in the affected areas.
	All office phones in the affected area will be moved to available offices within ITS.
	If the computers are not damaged or destroyed by the incident, the Desktop and Baseline Services Groups will relocate all desktop computers in the area to alternate locations.
	If the computers are damaged or destroyed, Baseline and Desktop Services Groups will identify spare computers, install them in an alternate location and install the computer user's data from their daily computer backup.
	Visual and Media Support will create and post signage and posters directing users to the new location.

7.1.4.3 Major State

Scenarios	Actions
The ITS disaster recovery plan has been activated and the University is open.	The associate vice president will communicate exclusively by cell phone.
	The associate vice president will release disaster recovery information to Public Affairs and other campus constituents. Only Public Affairs is authorized to release information to the media.
	The associate vice president or designee will approve any emergency information technology purchase requisitions. Non-emergency purchase requisitions will not be accepted or processed until normal operations are restored.
	The associate vice president may designate an ITS director to receive and respond to non-urgent requests from campus constituents.
	All other activities and services performed by this office will be suspended until normal operations are restored and office staff may be reassigned to other ITS areas to assist with the disaster recovery.
The ITS disaster recovery plan has been activated and the University is closed.	The associate vice president will communicate exclusively by cell phone.
	The associate vice president will release ITS disaster recovery status information to Public Affairs and other University constituents.
	Emergency purchase requisitions will be processed as outlined in Procurement and Contract's business continuity plan. This level of signature approval will be designated to the associate vice president, or in that person's absence, any of the ITS directors, and the ITS Fiscal Manager, as appropriate for the purchased item.
	The associate vice president, ITS directors or managers responsible for disaster recovery tasks will assign recovery responsibilities to ITS employees, as appropriate.

7.1.5 Information Security and Compliance

Following certain incidents and at the direction of University Counsel or University Police, 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.

7.1.5.1 Minor State

Scenarios	Actions
The office is not affected.	Business operations will continue normally.
The office is affected.	Business operations will continue normally using the assigned ITS emergency laptop and encrypted drive of backup data if the incident is predicted to last longer than four hours.
	The assigned ITS emergency laptop will be used to communicate with the data center servers and network devices that contain potential evidence. Any evidence will be stored on the encrypted drive containing backup data.

7.1.5.2 Intermediate State

Scenarios	Actions
The office is not affected.	Business operations will continue normally.
The office is affected.	Business operations will continue normally using the assigned ITS emergency laptop and encrypted drive of backup data if the incident is predicted to last longer than four hours.
	The assigned ITS emergency laptop will be used to communicate with the data center servers and network devices that contain potential evidence. Any evidence will be stored on the encrypted drive containing backup data.
The data center is affected.	Business operations will continue normally using the assigned ITS emergency laptop and encrypted drive of backup data if the incident is predicted to last longer than four hours.
	Evaluation of data from the data center servers and network devices that are still accessible will be conducted using the emergency laptop and encrypted drive.
	If the data center is completely unavailable, security evaluation of the

	data center servers and network devices will be placed on hold until the data center has been recovered.
	If the server containing online ITS forms is unavailable, hard copies can be reproduced and distributed from SharePoint ► ITS Documents.
	Critical ITS user forms are backed-up on Microsoft Teams Cloud system – ITS Document Control Center group and can be downloaded, printed and distributed by emergency laptop owners.

7.1.5.3 Major State

Scenarios	Actions
The ITS disaster recovery plan has been activated and the University is open.	If the equipment suspected of intrusion is accessible and undamaged, and the data center is operational, IT Security will use the forensic software on the server and dongle (USB key for the software) to investigate the incident.
	If the equipment suspected of intrusion is inaccessible and undamaged, and remains connected to the functional campus network, IT Security will use the server and dongle (USB key for the software) to access the hard drive over the network to investigate the incident.
	If the equipment suspected of intrusion is inaccessible and damaged, IT Security will not be able to investigate the incident. Following the eventual recovery of the hard drive, IT Security will attempt the investigation.
	Evaluation of data from the data center servers and network devices that are still accessible will be conducted using the emergency laptop and encrypted drive.
	If the data center is completely unavailable, security evaluation of the data center servers and network devices will be placed on hold until the data center has been recovered.
	Email/network and administrative systems account request forms will not be accepted or processed until normal business operations resume.
	If the network or servers are not available, all ITS forms and documentation generated by IT Security are recoverable from backup drives maintained by the director. These forms, if not available online due to server or network disruption, can be printed for manual use.

	If the equipment suspected of intrusion is accessible and undamaged, and the data center is unavailable, IT Security will obtain the hard drive and use the forensic software on the emergency laptop and dongle (USB key for the software) to investigate the incident.
	If the equipment suspected of intrusion is inaccessible and undamaged, and remains connected to the functional campus network, IT Security will use the emergency laptop and dongle (USB key for the software) to access the hard drive over the network to investigate the incident.
	If the equipment suspected of intrusion is inaccessible and damaged, IT Security will not be able to investigate the incident. Following the eventual recovery of the hard drive, IT Security will attempt the investigation.
	Evaluation of data from the data center servers and network devices that are still accessible will be conducted from a remote location, if necessary and possible, using the emergency laptop and biometric drive.
	If the data center is completely unavailable, security evaluation of the data center servers and network devices will be placed on hold until the data center has been recovered.
	The ITS procurement approval process to evaluate the purchase of security items and services will be suspended until normal business operations resume.

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 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 synchronizes to Azure AD for O365 email authentication. Operational readiness of the campus networks may also 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 GET/GETmobile

During a minor or intermediate incident that does not affect the campus network and authentication server, GET/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, 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 major impact to students during the reconstruction period; or
    - Determine if the lab needs to reopen in an alternate location;
    - Identify a new location, if needed, and begin temporary implementation.
- In conjunction with Visual and Media Support staff, prepare any signage and handouts necessary to alert students to OAL closures or temporary facilities.
- Issue a tweet from @mycalstatela and send an email to notify the University of the lab closure or alternate lab locations.
- Seek assistance from Public Affairs to issue a tweet from @calstatela to reach a wider range of student population or work with Admin Tech area and use the campus emergency response system (RAVE) to send text messages to students.

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, Baseline Services, 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 operations resume

In the event a single TEC is rendered unusable or a portion of TECs are damaged during an incident, IT Infrastructure 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 computers 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 associate vice president for Information Technology Services.

7.2.8 Accessible Procurement Process (ATI)

The Information & Communication Technologies (ICT) Purchase Approval Request form is located in the ServiceNow catalog under Accessibility. For each submission, the form workflow requests approvals from College ITCs, ITS Accessibility, Information Security, Infrastructure, and the CIO. Once completed, the approval is submitted with requisition paperwork to Procurement and Contracts. This business process is shared between ITS and Procurements and Contracts.With the exception of 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 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 ITS 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

The portal is hosted in O365 SharePoint, and will remain available to provide recovery status to students. 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, room 4056 as well as Library North B130, 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 in person during major disaster recovery, but might be offered virtually.

Online training offered by external resources, such as LinkedIn Learning, 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 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 University 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 in the hosted web environment. The training for faculty, staff and auxiliaries depends on the Chancellor’s Office CSU Learn. For vendors and third parties, the training is provided by the Department of Education. 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*, Network and Email Account Requests

During minor and intermediate incidents, ITS will continue to receive and process 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* system. During minor and intermediate incidents, ITS will not process new network or email 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 these 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 new account and modification 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 semester 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 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 and host the Tableau visualization application, data warehousing reporting 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 outlined in section 8.1.

8.1.1 Immediate Response to Business Disruption

Ste p	Task	Description	Completed By	Date & Time
1.	Initiate emergency response procedures.	Reference the *Multihazard Emergency Plan* for specific instructions.		
2.	*If on campus at the time of disaster* - call University Police.	Call University Police (3-3700) and briefly describe the situation. Give specifics on location and request appropriate assistance.		
3.	Initiate evacuation procedures if appropriate.	Building occupants should be directed to assemble in the assigned areas as published annually in the *Campus Information and Telephone Directory*, Emergency Information section.		
4.	Advise staff not to speak to media.	Advise all staff members not to respond to media but to refer inquiries to Public Affairs.		
5.	*If not on campus at the time of disaster* - receive details of disaster.	Verify caller and obtain as much information as possible.		
6.	Provide information to ITS team leaders.	The ITS management team will contact ITS team leaders as soon as possible to communicate key information about the business interruption. **INITIAL TEAM BRIEFING** ◆ Inform the team leaders what happened. Confirm the time of event and who is involved in the situation thus far.		

		◆ Confirm who must report to the Emergency Operations Center. ◆ Identify a location and phone number for the ITS Command Center. ◆ Use the Fan-out Call Tree located in the *ITS-7502 ITS Technical Disaster Recovery Plan* to notify all required staff of their responsibilities in carrying out the disaster recovery. ◆ Determine who is <u>not</u> available to travel to the alternate site (if applicable). ◆ 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 travel allowance form and provide emergency funding, if necessary. ◆ Verify that all management team and team leaders have installed the CodeTwo emergency contacts app on their smartphones that includes all the ITS contacts and cell numbers. ◆ Maintain phone accessibility for team members. Confirm callback number (if not the ITS Command Center). Phone #: ________________ *(Record at time of briefing)*		

		◆ Distribute ITS Command Center phone number for team to give to their family. Phone #: ___________________ *(Record at time of briefing)*		

8.1.2 Alert the Disaster Recovery Team and Standby

Step	Task	Description	Completed By	Date & Time
1.	Assemble the disaster recovery team and place members on alert.	Reference contact information in the Fan-out Call Tree found in *ITS-7502 ITS Technical Disaster Recovery Plan*. Begin tracking status of notification time and availability.		
2.	Salvage records or work in progress from the disaster area, if requested.	If permission is obtained from appropriate source, retrieve as much work as possible from the disaster site. Equipment and furniture will be salvaged at a later date after appropriate authorities have assessed the damage, inventoried the items and tagged items for disposal.		
3.	Await decision to DECLARE or CANCEL the alert.	The ITS management team will notify the disaster recovery team of a disaster declaration. If the decision is to CANCEL the alert, notify all parties initially contacted that the alert has been cancelled.		

8.1.3 Proceed with Critical Notifications

Step	Task	Description	Completed By	Date & Time
1.	If CANCEL: Notify all personnel.	Notify all personnel previously alerted that normal operations will resume.		
2.	If DECLARE: Assemble the disaster recovery team.	Prepare a team briefing with the disaster recovery teams and initiate the ITS disaster recovery plan.		

3.	Notify key vendors.	Verify response times for vendors critical to restoration. Reference the Vendor Master List located in *ITS-7502 ITS Technical Disaster Recovery Plan*.		
4.	Notify other contacts.	Notify other University contacts as required.		
5.	ITS management team to communicate status to associate vice president for ITS.	Communicate the status of recovery to the associate vice president for ITS on a regular basis.		

8.2 Environmental Restoration in an Alternate Site

8.2.1 Establish Alternate Site

The ITS management team is responsible for enacting a declaration to resume business at an alternate site. The following steps are required to prepare the alternate site operations.

Step	Task	Description	Completed By	Date & Time
1.	Confirm alternate facility requirements and receive verification of site availability from the site management.	This facility will house the business function until the primary site is restored. Confirm site availability with the associate vice president for ITS and ITS management team members not involved in securing the alternate facility. Reference the Pre-established Alternate Location section in *ITS-7502 ITS Technical Disaster Recovery Plan*.		
2.	Inform employees about the alternate site location.	Confirm that all staff members know how to get to the alternate site. Confirm day and time to report into the new location.		
3.	Verify appropriate departmental security at alternate site.	Ensure that vital records, sensitive data, etc., will be adequately protected at the alternate site.		
4.	Coordinate team transportation	Coordinate requirements through the ITS team members.		

	requirements.			
5.	Inform appropriate parties of the new location.	Notify external agencies, vendors and key University personnel regarding the relocation of the unit. Confirm timeframes for site start-up and new contact numbers, if available. If known, communicate any variations from normal processing schedules.		

8.2.2 Obtain Necessary Alternate Site Materials

Alternate site materials are those materials required to restore services or operate the equipment. Each individual system's disaster recovery plan has its own unique set of required information. Examples include the individual disaster recovery plans, system or network diagrams, vendor specifications, data backups, console operation, incident management operation, etc. The ITS team leaders are responsible for the following functions.

Step	Task	Description	Completed By	Date & Time
1.	Initiate retrieval of alternate site materials.	If any alternate site materials are needed, call the vendor for materials or media. Confirm the location to which the materials should be delivered and the name of the specific staff member designated to receive them.		
2.	Verify that all alternate site materials were received.	Log in the time and date of any delivered materials. Inventory materials against the offsite manifest delivered with the materials. Inform the management team leader of any missing materials.		
3.	Confirm number of available personnel - immediately and long term.	Meet with team members to schedule staffing requirements. Report child/spouse/elder/animal care and other issues to the ITS management team. Coordinate the acquisition of additional personnel through the ITS management		

		team.		
4.	Coordinate procurement of resources with the ITS management team.	Verify whether requested timeframes can be met for critical requirements.		
5.	Order necessary documentation manuals.	Verify whether manuals are necessary for staff who may be working on unfamiliar equipment (i.e., switchboard, incident management system). Verify whether necessary manuals have been salvaged or can be obtained from other departments before ordering replacements.		
6.	Report status to ITS management team.	Use form *ITS-9807 Disaster Recovery Situation Status Report* to provide ongoing status reports.		

8.3 Functional Restoration in an Alternate Site

Functional restoration tasks are undertaken concurrently, not sequentially, so it is important that all the following 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 outlined in section 8.3.

8.3.1 Review Critical Business Functions

Step	Task	Description	Completed By	Date & Time
1.	Review and confirm critical business function priorities.	Verify critical business functions in relation to the current incident. Consider volume, peak periods and critical timeframes that may require priorities to be altered.		
2.	Confirm the staffing and work day schedules required.	Confirm the start and end of the work day. If shifts will be implemented, confirm the schedules for each shift and the projected timeframe during which shifts will be utilized.		
3.	Develop a staffing	Create an alternative staffing schedule or hours of availability schedule in the event		

	contingency plan.	that assigned staff are unable to fulfill their schedule due to illness or family emergency.		

8.3.2 Begin Manual Processing

Step	Task	Description	Completed By	Date & Time
1.	Verify the scope of the computer processing disruption.	Coordinate with the ITS management team to determine the extent of processing disruption. If the disruption is the result of a communications failure, determine the anticipated time required to establish connectivity to the area. If the disruption requires that the data center restore processing capabilities, verify the recovery time required before files will be available, as well as projected date of restored files (i.e., they may be 1 to 2 days old). If only the business unit has been affected, confirm the amount of time required to restore connectivity to the new location.		
2.	Use manual procedures to resume critical business processes.	If necessary, begin using manual procedures to continue critical business operations identified in this *ITS Internal Business Continuity Plan*.		
3.	Report status to the ITS management team.	Use form *ITS-9807 ITS Disaster Recovery Situation Status Report* to provide ongoing status reports.		

8.3.3 Equipment Set Up and Connectivity

Step	Task	Description	Completed By	Date & Time
1.	Confirm status of computers and software requests.	Verify status of delivery and installation, including the person(s) responsible for this action.		
2.	Confirm computer connectivity.	Verify status of the LAN, WAN and system connections, including the person(s) responsible for this action.		
3.	Ensure that telephone service is restored.	Report problems and status to the ITS management team.		
4.	Coordinate furniture and equipment deliveries with the ITS management team.	This includes new or salvaged furniture.		

8.3.4 Obtain Necessary Supplies

Step	Task	Description	Completed By	Date & Time
1.	Replace internally produced forms.	Review requirements for those forms generated within the department. Ensure replacement forms are replicated as required. Copies of important forms should be stored on backup media or a copy should be retained offsite if the form is to be replicated. A small supply of critical forms should be copied and stored in a safe campus location so operations can resume immediately while a larger supply is replicated.		
2.	Confirm status of office supplies.	Order office supplies through ITS management team.		

8.3.5 Identify and Address Financial Requirements

Step	Task	Description	Completed By	Date & Time
1.	Determine financial needs and obtain funding as required.	Coordinate all requests for emergency funding with the ITS management team. Ensure that all monetary distributions are recorded on *ITS-9803 Emergency Cash Disbursement Log*. Reference the *ITS-9507 Management Disaster Preparedness Plan* for *ITS-9803 Emergency Cash Disbursement Log.*		
2.	Document approval for special charges.	All approvals must be coordinated through the ITS management team. Retain the appropriate documentation for later review.		
3.	Document recovery-related time worked and expenses incurred.	All expenses must be documented for insurance purposes. Reference the *ITS Management Disaster Preparedness Plan* for *ITS-9805 Emergency Recovery Employee Work Hours Log* and *ITS-9804 Emergency Recovery Expense Log* in the *ITS-9507 Management Disaster Preparedness Plan*.		

8.4 Verify System Functionality

Systems referenced here include both ITS employees' personal 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 the tasks in this section.

8.4.1 Verify Capabilities

Step	Task	Description	Completed By	Date & Time
•	Verify computer performance and verify restored files.	Ensure that all personal computers are properly functioning and all necessary LANs are in place and operable.		
•	Verify that proper applications and data are restored.	Verify the date of all restored files. Ensure that restored applications reflect support-critical functionality (i.e., interfacing applications reflect synchronized data).		
•	Confirm staffing work schedules and duties.	Ensure that all staff are informed of their scheduled work hours, particularly those who have been assigned interim shifts or duties during the recovery period.		
•	Meet with departmental personnel to evaluate the status.	Review outstanding issues; resolve outstanding problems.		

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.

8.5.1 Identify ITS Services Readiness

Step	Task	Description	Completed By	Date & Time
1.	Verify operational readiness with the ITS Command Center.	Reference the *ITS-9507 Management Disaster Preparedness Plan* for a sample of *ITS-9807 Disaster Recovery Situation Status Report*. Notify the ITS management team leader of the readiness to resume business processes and obtain approval to proceed.		

2.	Initiate notifications regarding resumption of normal business operations.	Notify any affected parties regarding resumption of normal processing. This includes internal business areas that send or receive work.		

8.6 Return of Business Processes to Home Site

The ITS team leaders are responsible for performing or assigning the tasks in this section

8.6.1 Relocate to the Home Site

Step	Task	Description	Completed By	Date & Time
1.	Meet with ITS management team to plan the return move.	Review the return move and confirm the time period for final move. Ensure that the department manager or representative attends appropriate meetings. *ITS-7502 ITS Technical Disaster Recovery* Plan should be referenced for issues to be considered.		
2.	Coordinate a relocation date with appropriate parties.	Schedule the relocation date to minimize disruption of business processing and customer interface.		
3.	Contact necessary faculty, staff, vendors, agencies, etc.	Include all individuals who need to know about the move. Confirm the move date and address changes as appropriate.		
4.	Establish resource requirements and monitor their status.	Request the resources necessary to facilitate the move.		
5.	Start up business processing at the new site.	Reference normal procedural documentation for the department.		

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. Employee responsibilities are documented in each individual's position description.

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 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, University directory database, personnel information, media signs and flyers, training materials, etc.) for their areas and ensure that they 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 University 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. If a computer, office or building is destroyed or secured against access, every employee needs an accessible backup of all documents and data 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?
- Are there Levels 1 and 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.

ITS computers are backed up on a daily basis using a cloud backup provider that ensures files are always readily available and retrievable.

Microsoft OneDrive is available through Office 365/ Microsoft 365to back up documents and files in the cloud. Instructions are online at https://support.microsoft.com/en-us/onedrive?ui=en-us&rs=en-us&ad=us

Acceptable Mobile Electronic Storage Media

There are two acceptable mobile 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.

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.

9.2.2 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.

9.2.3 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, employees who are 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 University communications, manning phones at a remote call center, updating and issuing recovery status reports, updating webpages, creating and printing handouts for University-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 Laptops

A laptop has been issued to all ITS staff members and these laptops will be used in the event of an emergency. Every employee should have the ability to utilize their laptop in the event of an emergency. 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 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
Cell Phone: 323-842-5047

Contact for: First-level contact for all ITS services and systems, emergency information technology procurement approvals, and updates on the status of ITS disaster recovery measures.

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

Office Phone: 323-343-2676
Cell Phone: 323-400-9984

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

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

Office Phone: 323-343-2629
Cell Phone: 323-365-7507

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

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

Office Phone: 323-343-2643
Cell Phone: 310-544-9563

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

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

Office Phone: 323-343-2665
Cell Phone: 323-532-9593

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

f) **Director, Client Support Services and Training:**

Office Phone: 323-343-2573
Cell Phone: 323-459-1407

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

g) **Manager, IT Client Support Services**

Office Phone: 323-343-4533
Cell Phone: 323-379-5791

Contact for: ITS Help Desk, Open Access Labs, @mycalstatela Twitter, campus-wide email.

h) **Director, Enterprise Applications:**

Office Phone: 323-343-2706
Cell Phone: 562-314-9521

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

i) **Assistant Director, Enterprise Applications**

Office Phone: 323-343-2611
Cell Phone: 626-890-9030

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

j) **Director, IT Security and Compliance:**

Office Phone: 323-343-4534
Cell Phone: 323-742-4808

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

11 Applicable Federal and State Laws and Regulations

Federal	Title
NA	
State	**Title**
NA	