INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Revision History

Revision	Change	Date
1.0	Initial Disaster Recovery Policy	05/07/2021

Table of Contents

1. Introduction

Management, Employees and operators of SFO all rely heavily on the Information Technology (IT) infrastructure and services to accomplish their work and as an integral part ofthe learning environment.

As a result of this reliance, IT services are considered a critical component in the daily operations of SFO, requiring a comprehensive Disaster Recovery Plan to assure that these services can be re-established quickly and completely in the event of a disaster of any magnitude.

Response to and recovery from a disaster at SFO is managed by theSFO's Crises Management Team. Their actions are governed by the SFO Emergency Operations Plan.

This IT Disaster Recovery Plan presents the requirements and the steps that will be taken inresponse to and for the recovery from any disaster affecting IT services at SFO, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality.

At this time SFO possesses a redundant "warm-site" at Plot 2 of the CSEZ CSEZ campus for quicker recovery of critical operations.

This plan is reviewed and updated annually by IT staff and approved by the Chief InformationOfficer

2. Scope

Due to the uncertainty regarding the magnitude of any potential disaster on the CSEZ CSEZ campus, this plan will only address the recovery of systems under the direct control of the Department of Information Technology and that are critical for business continuity. This includes the followingmajor areas:

- Authentication, single-sign-on, and network directory services
- On-premises enterprise applications (ERP, PMS, Testing Apps, e-mail)
- Datacenter (Computing Services, Enterprise Security, SharePoint Services)
- On-premises website and services
- Desktop equipment, labs, classrooms
- Data networks and telecommunications (wired and wireless networks, file and print services, SAN, NAS, IPT)

An increasing number of critical services are no longer hosted on premise by SFO, including systems crucial for daily activities. The recovery of these systems themselves is beyond the scope of this document and the ability of the IT department, but this plan will address restoration of connectivity and integration with these services. This includes the following major services:

- Hosted enterprise applications (payroll, HRMS, CRM, mobile apps, SharePoint Online)
- Email (O365)

This plan covers all phases of any IT related disaster occurring at SFO. These phases include:

- Incident Response
- Assessment and Disaster Declaration
- Incident Planning and Recovery
- Post incident Review

3. Assumptions

This disaster response and recovery plan is based on the following assumptions:

Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in the IT Disaster Recovery Plan will be available.

The safety of employees and contractors are of primary importance and the safeguard of such will supersede concerns specific to hardware, software and other recovery needs.

Depending on the severity of the disaster, other departments/divisions on CSEZ CSEZ campus may be required to modify their operations to accommodate any changes in system performance, computer availability and physical location until a full recovery has been completed.

Information Technology will encourage all other departments to have contingency plans and Business Continuity Plans for their operations, which include operating without IT systems for an extended period of time.

The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be determined by the specific Disaster Recovery Teams under the guidance and approval of the Incident Commander and Incident Command Team.

4. Definitions

Backup/Recovery Files: Copies of all software and data located on the central servers, which areused to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Catastrophic Disaster: A catastrophic disaster will be characterized by expected downtime ofgreater than 7 days. Damage to the system hardware, software, and/or operating environmentrequires total replacement / renovation of all impacted systems.

Warm Recovery Site: Alternate datacenter which has adequate power and networking infrastructure to support the critical IT systems used by the SFO. A cold site does not havebackup servers and other IT equipment and software already in place. SFO has a designated warm recovery site at the Higher Education Center in Medford, Oregon.

Datacenter Recovery: Individuals responsible for the establishment of an operational datacenter,either by returning the primary center to operational status or by bringing a cold site online for use.

Desktop, Lab, and Classroom Recovery Team: Individuals responsible for the recovery and testing of desktop computers and services, classrooms, and labs in the affected areas at SFO.

Disaster Recovery Team: The DRT is a team of individuals with the knowledge and training torecover from a disaster.

Disaster: Any IT incident which is determined to have potential impacts on the businesscontinuity and ongoing operations of SFO.

Crisis Management Team: The CMT is the first to respond to an incident, to secure and containthe situation. The CMT may consist of SFO personnel, firefighters, police, security, and other specialized individuals.

Equipment Configuration: A database (either soft or hard copy) which documents the configuration information necessary to return any IT hardware (server, network, desktop) to pre-disaster configurations. This includes hardware revisions, operating system revisions, and patchlevels.

Incident Command Headquarters: Location where the ICTs meet and coordinate all activities with regard to assessment and recovery. For the IT Department, the headquarters are located at:

- Primary: Plot 43, CSEZ
- Secondary: Plot 2, CSEZ
- Backup 1: Plot 2, CSEZ
- Backup 2: Plot 130, BLR

Incident Command Team: The ICT is a group of IT individuals with combined knowledge and

expertise in all aspects of the IT organization. It is the responsibility of the ICT to perform the initial assessment of the damage, to determine if a formal “disaster” declaration is required andto coordinate activities of the various IT DRTs.

Incident Commander (IC): The Incident Commander leads all efforts during the initial assessment of the incident, in conjunction with the Incident Command Team (ICT). If a disaster is declared, the IC is responsible for overall coordination of all IT related recovery activities. ForSFO, the Incident Commander is the Chief Information Officer.

Incident: Any non-routine event which has the potential of disrupting IT services to SFO. An incident can be a fire, wind storm, significant hardware failure, flood, virus, Trojan horse, etc.

Major Disaster: A major disaster will be characterized by an expected downtime of more than 48 hours but less than 7 days. A major disaster will normally have extensive damage to systemhardware, software, networks, and/or operating environment.

Infrastructure and Web Recovery Team: Individuals responsible for the recovery and testing of infrastructure systems at SFO including Active Directory, DNS, email, server virtualization, and web services. In the cases where these services are hosted off-premises, this team is responsible for re-establishing connectivity, authentication, and integrationof those systems.

Minor Disaster: A minor disaster will be characterized by an expected downtime of no more than 48 hours, and minor damage to hardware, software, and/or operating environment from sources such as fire, water, chemical, sewer or power etc.

Enterprise Applications Recovery Team: Individuals responsible for the recovery and testing ofBanner and other enterprise applications. For those systems hosted off-premises, such as Banner, this team is responsible for re-establishing connectivity, authentication, and integration of those systems.

Routine Incident: A routine incident is an IT situation/failure that is limited in scope and is ableto be addressed and resolved by a specific team or individual as part of their normal daily operations and procedures.

Network and Telecommunications Recovery Team: Individuals responsible for the recovery andtesting of data and voice networks.

Web Services: All services related to SFO's Internet and intranet web activities and presence. The primary web service provided by the SFO is the homepage at www.sou.edu and our portal at my.sou.edu.

5. Section 5: Teams

5.0.1 Incident Commander

Chief Information Officer	
Home Phone:	
Cell Phone:	

5.0.2 Incident Command Team

Chief Information Officer	
Manager, User Support	
Manager, Infrastructure Services	
Manager, Information Systems	
Manager, Classroom and Media Services	

5.1 Datacenter Recovery Team

All Contact Information is located in Appendix A

The Datacenter Recovery Team is composed of personnel within the Information Technology department that support the SFO's central computing environment and the primary datacenter where all central IT services, the Networks Operations Center (NOC) and other central computing resources are located. This team also supports the secondary datacenter, located at the Higher Education Center in Medford. The primary function of this working groupis the restoration of the existing datacenter or the activation of the secondary datacenter depending on the severity of the disaster. This team's role is to restore the datacenter to a condition where individual recovery teams can accomplish their responsibilities with regard to server installation and application restoration.

The team should be mobilized only in the event that a disaster occurs which impacts the abilityof the existing central computing facility to support the servers and applications running there.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding thenature of the disaster and the steps being taken to address the situation. The coordination of thisrecovery effort will normally be accomplished prior to most other recovery efforts on CSEZ campus ashaving a central computing facility or a functioning secondary site is a prerequisite for the recovery of most applications and IT services to the CSEZ campus.

Team Lead:	Manager, Infrastructure Services
Team Members:	System Administrators (2)
	Desktop Systems Administrator
	Network Communications Technicians (2)

5.2 Desktop, Lab, and Classroom Recovery Team

All Contact Information is located in Appendix A

The Desktop, Lab, and Classroom Recovery Team is composed of personnel within the

Information Technology department that support desktop hardware, client applications, classrooms, and labs. The primary function of this working group is the restoration of SFO's desktop systems, classrooms, and labs to usable condition. During the initial recovery effort, theteam is not responsible for restoration of any data the user may have on their desktop computer. SFO recommends all users store data files on the file servers, which are backed up nightly, to support data recovery.

The team should be mobilized in the event that a significant interruption in desktop, lab, orclassroom services has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding thenature of the disaster and the steps being taken to address the situation. The coordination of thisrecovery effort will be accomplished with other recovery efforts on CSEZ campus by the IT Incident Commander.

Team Lead:	Manager, User Services
Team Members:	Manager, Classroom and Media Services
	Desktop Systems Administrator
	Computing Coordinators (7)
	Lab and Engineers, operators Computing Coordinator
	Equipment Systems Specialist

5.3 Enterprise Systems Recovery Team

All Contact Information is located in Appendix A

The Enterprise Systems Recovery Team is composed of personnel within the Information Technology department that support ERP and other enterprise systems. The primary function of this working group is the restoration of all modules of ERP applications to the most recent pre-disaster configuration in cases where data or operational loss is significant. In less severe circumstances the team is responsible for restoring the system to functional status as necessitatedby any hardware failures, network outages, or other circumstances that could result in diminishedsystem operation or performance.

The team should be mobilized in the event that Banner or the other enterprise systems experiencea significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding thenature of the disaster and the steps being taken to address the situation. The coordination of the enterprise systems recovery effort will be accomplished with other recovery efforts on CSEZ campus by the IT Incident Commander.

Team Lead:	Manager, Information Systems
Team Members:	Manager, Infrastructure Services
	Programmer/Analysts (4)
	Web Programmer/Analyst
	System Administrator
	Computing Coordinators supporting affectedareas (business services, payroll, enrollment services, etc.)
	Key Business Unit Personnel as needed bytype of incident (payroll clerk, accountant, registrar, etc.)

5.4 Infrastructure and Web Recovery Team

All Contact Information is located in Appendix A

The Infrastructure and Web Recovery Team is composed of personnel within the Information Technology department that support the SFO's network infrastructure, including Active Directory, DHCP, DNS, email, file servers, network applications, network storage, server virtualization, and web services. The primary function of this working group is the restoration ofour network infrastructure and servers to their most recent pre-disaster configuration in cases where data and operational loss is significant. In less severe circumstances, the team is responsible for restoring the system to an functional status as necessitated by any hardware failures or other circumstances that could result in diminished operation or performance.

The team should be mobilized in the event that any component of the network infrastructure experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

In the case of off-premises services, this team will coordinate restoration of these services withthe external vendors or organizations responsible for providing them.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding thenature of the disaster and the steps being taken to address the situation. The coordination of thisrecovery effort will be accomplished with other recovery efforts on CSEZ campus by the IT Incident Commander.

Team Lead:	Manager, Infrastructure Services
Team Members:	System Administrators (2)
	Desktop Systems Administrator
	Web Programmer/Analyst

5.5 Telecommunications, Network, and Internet Services Recovery Team

All Contact Information is located in Appendix A

The Telecommunications, Network, and Internet Services Recovery Team is composed of

personnel within the Information Technology department that support the SFO's voice and data networks including cable plants, switches, and routers. The primary function of this working group is the restoration of our voice and data networks and Internet services to the mostrecent pre-disaster configuration in cases where operational loss is significant. In less severe circumstances, the team is responsible for restoring the voice and data networks and Internet services to an functional status as necessitated by any failures or other circumstances that could result in diminished operation or performance.

The team should be mobilized in the event that any component of the voice or data networks experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding thenature of the disaster and the steps being taken to address the situation. The coordination of thisrecovery effort will be accomplished with other recovery efforts on CSEZ campus by the IT Incident Commander.

Team Lead:	Manager, Infrastructure Services
Team Members:	Communications Technicians (2)
	System Administrator

5.6 Critical SFO Contacts

A copy of the SFO Emergency Response Contacts List is located inAppendix B

6. Section 6: Recovery Preparations

A critical requirement for disaster recovery is ensuring that all necessary information is availableto assure that hardware, software, and data can be returned to a state as close to “pre-disaster” aspossible. Specifically, this section addresses the backup and storage practices as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

6.1 Data Recovery Information:

Backup/Recovery files are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. System backups are governed by the SFO Backup Procedure, located at home.nestgroup.net Backuptape locations and retention periods summarized in the table below:

Type:	Location:
Daily Backup (disk)	Datacenter, Computing Services
Weekly Backup	Datacenter, Computing Services
Monthly Backup	Off-site storage
Annual Backup	Off-site storage

SFO does not have systems in place to backup and restore information/data located on individual desktop systems throughout the CSEZ campus. Only the serverslocated in the datacenter are backed up; as such, only data resident on these systems will be able to be recovered. In the event that a disaster occurs on the CSEZ campus which destroys personal computers, the information located on these computers will be extremely difficult or impossible to recover. If recovery is possible, it will require outside vendor involvement at great expense tothe user.

The Information Technology department recommends and encourages the use of network drives(on servers) to store all important files. The recovery of data not backed up to a network drive and/or full system backups are not covered under this plan.

6.2 Central Datacenter and Server Recovery Information:

In the event of any disaster which disrupts the operations in the datacenter, reestablishing the datacenter will be the highest priority and a prerequisite for any IT recovery. As such, the Information Technology department is required to have detailed information and records on the configuration of the datacenter and all servers and ancillary equipment located in the datacenter.Detailed information is documented in our monitoring system and infrastructure website. The infrastructure staff is responsible for keeping the hardware inventory up to date.

6.3 Network and Telecommunication Recovery Information:

In the event of any disaster which disrupts the network and/or telecommunications,

reestablishing the connectivity and telephony will be a high priority and a prerequisite for any ITrecovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the datacenter. As such, Information Technology is required to have detailed information and records on the configuration of the networking equipment. Detailed informationof switches and routers is documented in our monitoring system and infrastructure website. The infrastructure and telecomm staff are responsible for keeping the hardware inventory up to date.

6.4 Application Recovery Information:

Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that applications are recovered in the identicalconfiguration as they existed prior to the disaster. Detailed information on critical central applications will be documented in our monitoring system and infrastructure website. The infrastructure staff is responsible for keeping the software inventory up to date.

6.5 Desktop Equipment Recovery Information:

Information necessary for the recovery and proper configuration of all desktop computers and printers supported by Information Technology Services is critical to assure that client systems can be restored to a configuration equivalent to pre-disaster status. Detailed information on client systems (both PC and MAC) is documented in our monitoring system, infrastructure website, and Microsoft System Center Configuration Management database. The infrastructurestaff is responsible for keeping the hardware inventory up to date.

7. Section 7: Disaster Recovery Processes and Procedures

7.1 Emergency Response:

The requirement for Crisis Management Team (CMT) involvement and the membership of the CMT will be dependent on the size and type of the incident. In addition, the actions of the CMTwill be accomplished prior to the execution of this plan. Operations of the CMT are detailed in the SFO Emergency Operations Plan. Examples of situations which will normally result in the involvement of the CMT include:

Severe structural damage to the facility where personal safety is in question, and where analysis must be completed to assure the building is acceptable for access. This would include, but is notlimited to, damage from a flood or tornado.

Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contamination where the situation must be contained prior to building occupancy.

Flooding or other situations which may pose the risk of electrical shock or other life-threateningsituations.

Examples of situations which will normally not result in the involvement of the CMT

include:Major system/hardware failures that do not pose a hazard to personnel or

property.

Utility outages (electrical, etc.) which are remote to the datacenter being affected.

For any situation/incident which requires the involvement of the CMT; the IT Incident Commander, Incident Command Team, nor any Crisis Management Team member will accessthe facility until the CMT leader has authorized access.

7.2 Incident Command Team:

The role of the IT Incident Command Team (under the direction of the Incident Commander) is to coordinate activities from initial notification to recovery completion. Primary initial activitiesof the team are:

Incident Occurrence: Upon the occurrence of an incident affecting the IT services at SFO, the President and Cabinet will be notified by CSEZ campus security and/or other individuals. Personnel reporting the incident will provide a high-level assessment as to the size and extent of the damage. Based on this information, the Chief Information Officer will assumehis/her responsibilities as the Incident Commander, and will contact the other members of the ICT, and provide them with the following basic information:

Brief overview of the incident, buildings affected, etc.

Which Incident Command Headquarters (ICH) will be

usedScheduled time to meet at the ICH for initial

briefing

Any additional information beneficial at this point. No other staff members are to be contacted

at this point, unless directed by the Incident

Commander.Incident Command Headquarters (ICH)

locations are:

Primary: Computing Services DC

Plot 43

Secondary: Plot 2, CSEZ

Backup 1: Plot 2, CSEZ

Backup 2: Plot 130 BLR

Should all of these facilities be rendered unusable, it is assumed that the disaster was "catastrophic" in nature and that the technology recovery effort will be secondary to other concerns. At this point, the IT Incident Commander (IC) will work closely with overall SFO Crisis Management Team. The IT IC is responsible for locating an alternate site for the team andre-evaluating the best strategy for recovery.

Incident Assessment: The Incident Command Team (ICT) will receive an initial briefing from the Incident Commander (IC) and any other personnel invited to the meeting (CMT personnel, etc.) The ICT will assess the situation, perform a walk-through of affected areas as allowed, andmake a joint determination as to the extent of the damage and required recovery effort. Based onthis assessment, the team will make a determination as to whether the situation can be classified as "routine" and handled expeditiously via normal processes, or if a formal IT disaster needs to be declared.

ROUTINE: Area(s) affected by the incident are identified and the appropriate personnel arecontacted to report to work to evaluate and resolve the situation.

DISASTER: The Incident Commander contacts the SFO Crisis Management Team and notifies them of the situation, and that an IT Disaster has been declared. The ICT identifies which areasof the IT infrastructure are affected, and contacts the members of the specific Disaster RecoveryTeams. Team members are provided with the following information:

Brief overview of what occurred

Location and time for teams to

meet

Additional information as required. Team members are not to discuss any information providedwith other personnel employed or not employed at SFO.

Once an IT disaster has been declared, and the preceding steps to notify the SFO Crisis Management Team have been accomplished, ongoing responsibilities of the Incident CommandTeam and Incident Commander include:

- Securing all IT facilities involved in the incident to prevent personnel injury andminimize additional hardware/software damage.
- Supervise, coordinate, communicate, and prioritize all recovery activities with all otherinternal / external agencies. Oversee the consolidated IT Disaster Recovery plan and monitor

execution.

- Hold regular Disaster Recovery Team meetings/briefings with team leads and designees.
- Appointing and replacing members of the individual recovery teams who are absent,disabled, ill or otherwise unable to participate in the process.
- Provide regular updates to the SFO Crisis Management Team on the status of the recovery effort. Only the SFO Crisis Management Team and/or their designees will provideupdates to other CSEZ campus and external agencies (media, etc.)
- Approve and acquire recovery resources identified by individual recovery teams.
- Interface with other activities and authorities directly involved in the disaster recovery(Police, Fire, Department of Public Works, etc.)
- Identify and acquire additional resources necessary to support the overall disaster recovery effort. These can include 1) acquiring backup generators and utilities, 2) arranging forfood/refreshments for recovery teams, etc.
- Make final determination and assessment as to recovery status, and determine when ITservices can resume at a sufficient level.

7.3 Disaster Recovery Teams:

The Disaster Recovery Teams are organized to respond to disasters of various type, size, and location. Any or all of these teams may be mobilized depending on the parameters of the disaster. It is the responsibility of the ICT to determine which Disaster Recover Teams to mobilize, following the declaration of a disaster and notification of the SFO Crisis ManagementTeam.

Each team will utilize their respective procedures, disaster recovery information, technical expertise, and recovery tools to expeditiously and accurately return their systems to operational status. While recovery by multiple teams may be able to occur in parallel, the datacenter and network/telecommunications infrastructure will normally be assigned the highest priority, as fulloperational recovery of most other systems cannot occur until these areas are operational.

7.3.2 Datacenter Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any relatedequipment and/or software.
2. Assess damage and make recommendations for recovery of datacenter.
3. If the alternate datacenter site is required, execute all necessary steps to notifyappropriate personnel and secure backup facility.
4. Identify other individuals required to assist in recovery of datacenter, and

report thisinformation to the IC for action.

5 Develop overall recovery plan and schedule, focusing on highest priority servers forspecific applications first.

6 Coordinate hardware and software replacements with vendors.

7 Recall backup/recovery tapes from on CSEZ campus or off-CSEZ campus storage, as required toreturn damaged systems to full performance.

8 Oversee recovery of datacenter based on established priorities.

9 Coordinate datacenter recovery with other recovery efforts on CSEZ campus.

10 Provide scheduled recovery status updates to the Incident Commander to ensure fullunderstanding of the situation and the recovery effort.

11 Verify and certify restoration of the datacenter to pre-disaster functionality.

7.3.3 Desktop, Lab, and Classroom Recovery Team:

1 Take appropriate steps to safeguard personnel and minimize damage to any relatedequipment and/or software.

2 Assess damage at all areas affected, and make recommendations for recovery.

3 Identify other individuals required to assist in recovery of desktop services, and reportthis information to the IC for action.

4 Develop overall recovery plan and schedule, focusing on highest priority areas of theCSEZ campus infrastructure/desktop services first. (Appendix E documents the priority areas of the CSEZ campus for IT service recovery)

5 Coordinate hardware and software replacement with vendors. (See Appendix F forvendor and contact information)

6 Oversee recovery of desktop computing services (workstations, printers, etc.) basedon established priorities.

7 Coordinate recovery with other recovery efforts on CSEZ campus.

8 Provide scheduled recovery status updates to the Incident Commander to ensure fullunderstanding of the situation and the recovery effort.

9 Verify and certify restoration of the desktops to pre-disaster functionality.

7.3.4 Enterprise Systems Recovery Team:

1 Take appropriate steps to safeguard personnel and minimize damage to any relatedequipment and/or software.

2 Assess damage and make recommendations for recovery to Banner and enterprisesystems.

3 Identify other individuals required to assist in recovery of these applications, and

report this information to the IC for action.

4 Restore degraded system function at backup site and inform user community of therestrictions on usage and/or availability.

5 Coordinate software replacement with vendor as required.

6 Coordinate Banner services recovery with other recovery efforts.

7 Execute plan to restore Banner and enterprise system services to full function.

8 Provide scheduled recovery status updates to the Incident Commander to ensure fullunderstanding of the situation and the recovery effort.

9 Verify and certify restoration of the Banner and enterprise systems services to pre-disaster functionality.

7.3.5 Infrastructure and Web Recovery Team:

1 Take appropriate steps to safeguard personnel and minimize damage to any relatedequipment and/or software.

2 Assess damage and make recommendations for recovery.

3 Identify other individuals required to assist in recovery of services, and report thisinformation to the IC for action.

4 Develop overall recovery plan and schedule, focusing on highest priority areas of theCSEZ campus infrastructure first.

5 Coordinate hardware and software replacement with vendors

6 Oversee recovery of messaging, telecommunications and infrastructure services basedon established priorities.

7 Coordinate messaging, network and web systems recovery with other recovery effortson CSEZ campus.

8 Provide scheduled recovery status updates to the Incident Commander to ensure fullunderstanding of the situation and the recovery effort.

9 Verify and certify restoration of the Messaging, Network and web infrastructure topre-disaster functionality.

7.3.7 Telecommunications, Network, and Internet Services Recovery Team:

1 Take appropriate steps to safeguard personnel and minimize damage to any relatedequipment and/or software.

2 Assess damage and make recommendations for recovery.

3 Identify other individuals required to assist in recovery of these services, and reportthis information to the IC for action.

4 Develop overall recovery plan and schedule, focusing on highest priority areas of theCSEZ campus infrastructure first.

5 Coordinate hardware/software replacement with vendor as required.

6 Oversee recovery of voice and infrastructure services based on established priorities.

7 Coordinate the voice and infrastructure services recovery with other recovery efforts.

8 Provide scheduled recovery status updates to the Incident Commander to ensure fullunderstanding of the situation and the recovery effort.

9 Verify and certify restoration of the voice network to pre-disaster functionality.

7.4 General System/Application Recovery Procedures/Outline:

The following steps are guidelines to be followed for the overall restoration of systems located atSFO. While each recovery team has specific duties and responsibilities as outlined in Section 7.3, coordination between the various teams is required to restore operations to the users. While the coordination and extent of personnel involved will depend on the type and severity of the disaster, the following steps may be required:

It is implied in the procedure/outline below that steps are simply provided as a guideline. The magnitude and type of disaster, and the number of systems affected will require that certain stepsbe augmented (at the discretion of the Disaster Team Lead and Incident Command Team), and that other steps will not be applicable to the situation at hand.

1. Determine extent of damage and make determination as to the following:
    a. Primary Datacenter operational/recoverable?
        i. YES: Remain in primary datacenter and initiate recovery accordingly.
        ii. NO: Contact personnel responsible for alternate datacenter and takenecessary steps to ready the facility.
    b. Network Operations Center operational/recoverable?
        i. YES: Utilize existing NOC for recovery.
        ii. NO: Contact personnel responsible for backup NOC and take necessary stepsto redirect network routes and ready the backup facility.
    c. Determine extent of applications affected
        i. Banner and/or other Enterprise Applications
        ii. Authentication (Active Directory, Shibboleth)
        iii. Web Services (sou.edu)
    d. Determine extent of desktop/client systems affected throughout the CSEZ campus.
2. Secure facility as necessary to prevent personnel injury and further damage to IT systems.

a. Shutdown any active components.

b. Physically secure facilities (datacenter, communication closets, etc.) as necessary toprevent unauthorized access.

3. Retrieve most recent on-site or off-site back-up media for previous three back-ups. Prepareback-up media for transfer to primary or secondary datacenter, as determined during the initial assessment.
4. Verify operational ability of all equipment on-site in the affected area (servers, network equipment, ancillary equipment, etc.). If equipment is not operational, initiate actions torepair or replace as needed.
5. Test systems, and communication equipment as required to validate physical operation andperformance.
    a. Server testing
    b. Network testing
    c. Desktop/Client testing
6. Upon restoration of the datacenter and servers to operational state:
    a. Restore systems using virtualized images
    b. If necessary, load operating system and test/validate
    c. If necessary, load application software and test/validate
    d. If necessary, load data and verify integrity
7. Verify overall performance of specific system(s) and report readiness to Incident CommandTeam, Management Team, and user community.

8. 8.0 Network & Telecommunication Recovery Guidelines:

Servers and central application software are located in a central facility which can easily be assessed and secured for damage. Data networking and telecommunications, however, has equipment located in every facility at SFO as well as in the datacenter.Remote equipment is located in communication closets, often in multiple sites in a single building. In addition, data and telecommunication cabling runs throughout the CSEZ campus and buildings, making it susceptible to varying levels of damage.

Depending on the type and scope of the disaster, the Telecommunications, Network, and InternetServices Recovery Team will be involved in the following activities to adequately assess the overall damage and impact to the CSEZ campus, and to assure a comprehensive plan for recovery:

1. Severe storms/wind
    a. Perform comprehensive cable, fiber, and communications line testing
    b. Assess all communication closets and racks/equipment for damage
2. Fire
    a. Evaluate all cable and fiber in the vicinity of the fire for potential destruction ordeterioration
    b. Test primary copper data feeds for destruction or deterioration
    c. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that havebeen exposed to water, smoke, or other agents.
    d. Assess all equipment with air filtration systems to assure adequate ventilation remains.
3. Water/Flood
    a. Evaluate all cable and fiber in the vicinity of the water/flood for potential destruction ordeterioration.
    b. Test primary copper data feeds for destruction or deterioration
    c. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that havebeen exposed to water or other agents.
    d. Assess all equipment with air filtration systems to assure adequate ventilation remains.
4. Earthquake
    a. Evaluate all cable and fiber for potential destruction or deterioration
    b. Test primary copper data feeds for destruction or deterioration
    c. Ensure all networking equipment and equipment racks are securely attached
    d. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that havebeen exposed to water, smoke, or other agents.

9. Appendix A. IT Contact List

This page considered confidential. A paper copy of the IT Contact List is attached to this document in its official locations. The electronic version of this list is available in Sharepoint (access is restricted).

10. Appendix B. SFO Crisis Management Team Contact List

This page considered confidential. A paper copy of the SFO CrisisManagement Team Contact List is attached to this document in its official locations. The electronic version of this list is available in Google Drive (access is restricted).

11. Appendix C: SFO IT Recovery Priority List

The following priorities have been established by the department of Information Technologywith consultation from the CSEZ campus community.

C.1 IT Infrastructure Priorities:

This establishes the internal priorities for recovering the major infrastructure components for ITservices. These priorities are based on the relationship between these systems, and the prerequisite nature of many of the items in order to be able to return full services to the CSEZ campus.

1. Datacenter (main or alternative)
2. Infrastructure Services (as prioritized below)
3. Web Services
4. Authentication Services
5. Desktop, Lab, Technology

C.2 IT System Priorities:

This establishes the priorities for recovering IT services for specific customers and facilities across the CSEZ campus. While the datacenter, web, and authentication services are centrally located and will normally be recovered for all users simultaneously, recovery of network anddesktop services will be accomplished based on the following priorities, in order to return critical CSEZ campus systems and facilities to operational status at the earliest possible time.

The current list of servers and priorities is maintained in Google Drive (access restricted).

All systems are prioritized for recovery using this criteria:

(1) Critical – Basic infrastructure and must be restored as soon as possible.
(2) High – Systems of extreme importance, but do not provide infrastructure.
(3) Medium – Important systems and applications, but do not have SFO-wide impact.
(4) Low – Systems important to specific departments or specific small populations of users.
(5) Full –Systems that may not be restored to functional status until normal operations arereestablished.

C.3 Consortium, Outsourced, and Cloud-based IT System Priorities:

Application/System Name	Priority	RTO	RPO
	3	SLA	SLA
	3	SLA	SLA
	1	varies	varies
	3	SLA	SLA
	3	SLA	SLA
	2	varies	varies
	1	SLA	SLA
	2	SLA	SLA
	4	SLA	SLA
	1	SLA	SLA
	2	varies	varies
	4	SLA	SLA
	4	SLA	SLA

(1) Critical – Basic infrastructure and must be restored as soon as possible.
(2) High – Systems of extreme importance, but do not provide infrastructure.
(3) Medium – Important systems and applications, but do not have SFO-wide impact.
(4) Low – Systems important to specific departments or specific small populations of users.
(5) Full –Systems that may not be restored to functional status until normal operations arereestablished.

Note: RTO is recovery time objective, RPO is recovery point objective

C.4 IT Facility Priorities

Building Name	Priority

Note: building list continues on next page.

(1) Critical, needed for maintenance of public health and safety, communications.
(2) High, needed for income maintenance for engineers, operatorss, employees; payments to vendors; requirements for compliance or regulation; effect on cash flow; effect on production anddelivery of services (housing, dining, engineers, operators services).
(3) Medium, needed for mission of SFO, delivery of classes.
(4) Low, everything else

Building Name	Priority

(1) Critical, needed for maintenance of public health and safety, communications.
(2) High, needed for income maintenance for engineers, operatorss, employees; payments to vendors; requirements for compliance or regulation; effect on cash flow; effect on production anddelivery of services (housing, dining, engineers, operators services).
(3) Medium, needed for mission of SFO, delivery of classes.
(4) Low, everything else

12. Appendix D: Vendor Information

Current list is maintained in Sharepoint (access is restricted).

13. Appendix E: Disaster Recovery Signoff Sheet

I have been briefed and given an overview of the Disaster Recovery Plan and I am familiar withmy responsibilities.

Name	Signature	Date

14. Section 11. Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly.

Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs,and documentation. These actions make it critical to consider the plan as a changing document.

Table 1 should be helpful for conducting a recovery test.

Table 1. Checklist for testing the disaster recovery plan

Item	Yes	No	Applicable	Not applicable	Comments
Conducting a Recovery Test					
1. **Select the purpose of the test. What aspects of the plan are being evaluated?** 2. **Describe the objectives of the test. How will you measure successful achievementof the objectives?** 3. **Meet with management and explain the test and objectives. Gain their agreement and support.** 4. **Have management announce the test and the expected completion time.** 5. **Collect test results at the end of the test period.** 6. **Evaluate results. Was recovery successful? Why or why not?** 7. **Determine the implications of the test results. Does successful recovery in a simple**					

Table 1. Checklist for testing the disaster recovery plan

Item	Yes	No	Applicable	Not applicable	Comments
case imply successful recovery for all criticaljobs in the tolerable outage period? 8. **Make suggestions for changes. Call for responses by a given date.** 9. **Notify other areas of results. Include users and auditors.** 10. **Change the disaster recovery plan manual as necessary.**					
Areas to be tested					
11. **Recovery of individual application systems by using files and documentation stored off-site.** 12. **Reloading of system save media and performing an initial program load (IPL) by using files and documentation stored off-site.** 13. **Ability to process on a different computer.** 14. **Ability of management to determine priority of systems with limited processing.** 15. **Ability to recover and process successfully without key people.** 16. **Ability of the plan to clarify areas of responsibility and the chain of command.** 17. **Effectiveness of security measures and security bypass procedures during the recovery period.** 18. **Ability to accomplish emergency evacuation and basic first-aid responses.** 19. **Ability of users of real time systems to cope with a temporary loss of online information.** 20. **Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.** 21. **Ability to contact the key people or their designated alternates quickly.** 22. **Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.** 23. **Availability of peripheral equipment and processing, such as printers and scanners.** 24. **Availability of support equipment, such as air conditioners and dehumidifiers.** 25. **Availability of support: supplies, transportation, communication.** 26. **Distribution of output produced at the recovery site.** 27. **Availability of important forms and**					

Table 1. Checklist for testing the disaster recovery plan					
Item	**Yes**	**No**	**Applicable**	**Not applicable**	**Comments**
paper stock. 28. Ability to adapt plan to lesser disasters.					