Information Technology Services

Disaster Response and Recovery Plan – PL408.0

Central Washington University
400 East University Way
Ellensburg, Washington 98926-7436
509.963.2333

Updated by

Networks & Operations
Updated January 2012

Revision History Page

Rev #	Change	Date
1	Initial Release DRP - Networks & Operations	1-Jun-1993
2	Update DRP - Networks & Operations	1-Nov-1996
2.1	Reviewed DRP - Networks & Operations	2-Aug-2008
2.2	Reviewed DRP - Networks & Operations	3-Aug-2008
3	Rewrite of DRRP - Networks & Operations	6-Mar-2008
3.1	Minor Updates DRRP - Networks & Operations	6-Aug-2008
3.2	Updated Personnel Names DRRP – Networks & Operations	7-Apr-2008
3.3	Minor Updates DRRP – Networks & Operations	7-Aug-2008
3.4	Personnel Updates – Networks & Operations	8-Feb-2008
3.5	New Recovery Team -- Networks & Operations	14-Apr-2008
3.6	Staffing, Building Updates – Networks & Operations	August-2009
3.7	Staffing Updates – Networks & Operations	January-2012

Official copies of this document are located at the following locations:

- Information Technology Services Department Office
- Computer Support Services Managers Office
- Central Computer Facility Operations Office
- Hebeler Tape Vault
- Office and Home of AVP for Information Technology
- Network and Operations Directors Office
- IT Security Administrators Office

Information Technology Services (ITS Department)
Disaster Response and Recovery Plan

TABLE OF CONTENTS

1.0 INTRODUCTION

Central Washington University is a four year institute of higher education. Faculty, staff and students all rely heavily on the Information Technology (IT) infrastructure and services to accomplish their jobs, and as an integral part of the learning environment/curriculum at the university.

As a result of this reliance, IT services are considered a critical component in the daily operations at Central Washington University, requiring a comprehensive Disaster Response and Recovery Plan (DRRP) 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 Central Washington University is managed by the Emergency Council Members, named in section 2 of the Emergency Preparedness Plan. Their actions are governed by the Central Washington University Emergency Preparedness Plan located at **http://www.cwu.edu/~police/docs/emergency-preparedness-plan.pdf**.

This IT DRRP presents the requirements and the steps that will be taken in response to and for the recovery from any disaster affecting IT services at Central Washington University, 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 Central Washington University does not run on redundant servers which would minimize potential business disruption in the event of a disaster, nor does the university possess a redundant “warm-site” or “hot-site” for quick recovery of the Data Center. Should more resources become available this plan will be re-evaluated and updated accordingly.

This plan is reviewed and updated yearly by August by ITS/Networks & Operations staff and approved by the Assistant VP for Information Technology.

A hard copy of this plan is stored in the following areas:

- Hebeler vault
- ITS/Networks & Operations (Terilee Germain’s Office)
- Bouillon 218 Comm Room
- Computer Center
- Auxiliary Wall Safe

2.0 SCOPE

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

- PeopleSoft Systems (payroll, AP/AR, financial aid, finance, safari)
- Central Computer Facility (Wildcat Shop)
- Electronic Mail and Web Services
- Desktop Equipment, Labs, Classrooms
- Data Networks and Telecommunications (networks, file services, telephony)
- Auxiliary Computing (Conference Center, Facilities, Parking, University Store, CBORD Dining Services, Housing, Health, ResNet, Student Recreation)

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

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

At this time Central Washington University does not run on redundant servers nor possess a redundant “warm-site” or “hot-site” for training or testing purposes. Should these resources become available this plan will be updated to fully detail training and testing of this plan.

3.0 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 DRRP will be available.

- The safety of students, staff and faculty are of prime 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 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 Services 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 Response and Recovery Teams under the guidance and approval of the Incident Director and Incident Command Team.

4.0 DEFINITIONS: The following definitions pertain to their use in this IT Disaster Recovery Plan.

Auxiliary Services Recovery Team:	Individuals responsible for the recovery and testing of Auxiliary Computing technology. Team lead is the Manager of Auxiliary Computing. **(Steve Breyfogle)**
Backup/Recovery Tapes:	Copies of all software and data located on the central servers, which are used 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 of greater than 7 days. Damage to the system hardware, software, and/or operating environment requires total replacement / renovation of all impacted systems.
Cold Recovery Site:	Alternate Data Center which has adequate power and networking infrastructure to support the critical IT systems used by the university. A cold site does not have backup servers and other IT equipment and software already in place. CWU does not have a designated Cold Recovery Site at this time.
Database Recovery Team	Individuals responsible for the recovery and testing of CWU Databases. Team lead is DBA Admin. **(Tiffany Price)**
Data Center Recovery Team:	Individuals responsible for the establishment of an operational data center, either by returning the primary center to operational status or by bringing a Cold Site online for use. Team lead is the Director of Networks and Operations. **(Noah Rodriguez)**
Desktop Recovery Team:	Individuals responsible for the recovery and testing of desktop computers and services, classrooms and labs in the affected areas at Central Washington University. Team lead is the Manager of Computer Support Services. **(Chris Pratz)**
Disaster Recovery Team (DRT):	The DRT is a team of individuals with the knowledge and training to recover from a disaster. For ITS, there are 6 teams for specific IT areas to be addressed.
Disaster:	Any IT incident which is determined to have potential impacts on the business continuity and ongoing operations of Central Washington University.
Emergency Response Team (ERT):	The ERT is the first to respond to an incident, to secure and contain the situation. The ERT may consist of firemen, police, security, and other specialized individuals.
Equipment Configuration Database:	A database (either soft or hardcopy) 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 patch levels.
Incident Command Headquarters	Location where the ICTs meet and coordinate all activities with regard to assessment and recovery. For the CWU ITS Department, the headquarters are located at: Primary: ITS Conference Room (Bou-202) Secondary: Barge Conference Room (Barge 412) Backup 1: Library Classroom Lab (Lib 154) Backup 2: Shaw Smyser Lab (SS214)

Incident Command Team (ICT):	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 and to coordinate activities of the various IT DRTs.
Incident Director (ID):	The Incident Director leads all efforts during the initial assessment of the incident, in conjunction with the Incident Command Team (ICT). If a disaster is declared, the ID is responsible for overall coordination of all IT related recovery activities. For Central Washington University, the Incident Director is the Assistant VP of Information Technology. **(Carmen Rahm)**
Incident:	Any non-routine event which has the potential of disrupting IT services to Central Washington University. An incident can be a fire, earthquake, significant hardware failure, flood, volcano ash, 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 system hardware, software, networks, and/or operating environment.
Messaging/Networks & Web Recovery Team:	Individuals responsible for the recovery and testing of messaging systems at CWU including email, calendaring, and Web technologies. Responsible for the recovery and testing of the data networks and file servers. Team lead is the Director of Network and Operations. **(Noah Rodriguez)**
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.
PeopleSoft Recovery Team:	Individuals responsible for the recovery and testing of the PeopleSoft systems. Team lead is Director of Application Services. **(Gene Rau)**
Resnet Recovery Team:	Individuals responsible for the recovery and testing of the Resnet Services. Team lead is the Director of Networks and Operations. **(Noah Rodriguez)**
Routine Incident:	A routine incident is an IT situation/failure that is limited in scope and is able to be addressed and resolved by a specific team or individual as part of their normal daily operations and procedures. Incidents which are not of magnitude to be classified as formal disasters and considered "routine" incidents and are handled accordingly.
Telecommunications Recovery Team:	Individuals responsible for the recovery and testing of voice networks. Team lead is the Supervisor of Telecommunications. **(Nancy Jackson)**
Web Services:	All services related to Central Washington University's Internet and Intranet Web activities and presence. The primary Web Service provided by CWU is the homepage at www.cwu.edu.

5.0 TEAM MEMBERS & CONTACT INFORMATION:

5.0.1 Incident Director:

Name:	Carmen Rahm
Home Phone:	509 962-1547
Cell Phone:	509 899-0038
Home Email:	foreacres@elltelnet

5.0.2 Incident Command Team: All Contact Information is located in Appendix A

Name:	Carmen Rahm, Assistant VP for Information Technology
	Noah Rodriguez, Director Networks & Operations (Alternate Incident Director)
	Gene Rau, Director Application Services
	Chris Pratz, Manager of Computer Support Services
	Nancy Jackson, Manager of Telecommunications
	Don Diebert, Director Project Mgmt & IT Services
	Steve Breyfogle, Manager of Auxiliary Computing

5.0.3 CWU Management Team: All Contact Information is located in Appendix B

Name:	James Gaudino, President CWU
	Marilyn Levine, Provost/VP for Academic and Student Life
	George Clark, VP for Business and Financial Affairs
	John Swiney, VP for Student Affairs and Enrollment Management
	Linda Schactler, VP for University Relations

5.1 AUXILIARY SERVICES RECOVERY TEAM:
All Contact Information is located in Appendix A

The Auxiliary Services Recovery Team is composed of the IT Specialists within Information Technology Services that support the Auxiliary systems. The primary function of this small working group is the restoration of the Auxiliary 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 systems to an operational status as necessitated by any hardware failures, network outages or other circumstances that could result in diminished system performance.

The team should be mobilized in the event that the Auxiliary systems 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 Manager of Auxiliary Services has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of the Auxiliary Services recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Steve Breyfogle (Recovery Team Lead)
Housing	Marion Andrin
Dining (Kronos)	Nathan Hill
Computrition	Larry Beintema
CBORD	Tad Pierce
Facilities	Ed Castaneda
Health	Nathan Hill, Steve Breyfogle
Resnet	Nathan Hill, Felicia Case
Student Recreation	Nathan Hill
Store-POS	Tad Pierce, Nathan Hill
Conference Center	Felicia Case, Steve Breyfogle
Work Order System Aux	Steve Breyfogle
Trade Book	Nate Hill
Quasar.cts.cwu.edu	DBA Team

5.2 DATA CENTER Recovery Team:
All Contact Information is located in Appendix A

The Data Center Recovery Team is composed of personnel within Information Technology Services that support Central Washington University's central computing environment and the primary data center where all central IT services, the Networks Operations Center (NOC) and other central computing resources are located. The primary function of this small working group is the restoration of the existing data center or the activation of the secondary data center depending on the severity of the disaster. This team's role is to restore the data center 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 ability of the existing central computing facility to support the servers and applications running there.

The Director of Network and Operations has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will normally be accomplished prior to most other recovery efforts on campus as having a central computing facility is a prerequisite for the recovery of most applications and IT services to the campus.

System Name:	Noah Rodriguez (Recovery Team Lead)
Operations Coordinator	Ron Breckon
Networks	Chris Timmons (Alternate Team Lead)
Networks	David Hart
Operations Support	Bill Glessner, Don Allen
Web Management	Larry Beintema
Netware Servers	Greg Deluca
Blackboard	Larry Beintema
Communications Infrastructure	Steve Ashbrooks, Wade Richardson

5.3 DESKTOP Recovery Team:
All Contact Information is located in Appendix A

The Desktop Recovery Team is composed of personnel within the Information Technology Department that support Central Washington University's desktop hardware, client applications, classrooms, labs and academic development systems. The primary function of this small working group is the restoration of Central Washington University's desktop systems, classrooms and labs to usable condition. During the initial recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer. Central Washington University 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 any component of the network or telecommunication 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.

The Manager of Computer Support Services has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Chris Pratz (Recovery Team Lead)
IT Specialist	Dave Germain (Alternate Team Lead)
IT Specialist/Primary	Bill Miller
PCs	Tina Klampher
MACs	Jeff Knackstedt
Labs	Jim Pruitt, Jeff Knackstedt
Classroom Technology	Sandy Sperline
Alternates	Kerry Green

5.4 MESSAGING/NETWORKS AND WEB Recovery Team:
All Contact Information is located in Appendix A

The Messaging/Networks and Web Recovery Team is composed of personnel within Information Technology Services that support Central Washington University's network infrastructure including all cable plants, switches, routers, network applications, file servers, electronic email servers and web services. The primary function of this small working group is the restoration of Central Washington University's LAN and servers to the most recent pre-disaster configuration in cases where data and network loss is significant. In less severe circumstances, the team is responsible for restoring the system to an operational status as necessitated by any network hardware failures or other circumstances that could result in diminished 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.

The Director of Network and Operations has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Noah Rodriguez (Recovery Team Lead)
Networks	Chris Timmons (Alternate Team Lead)
Web Services	Larry Beintema
Email Services	Bill Glessner
Networks	David Hart
Servers	Greg Deluca
Alternates	Terilee Germain
Cable Plants	Steve Ashbrooks, Wade Richardson

5.5 PEOPLESOFT Recovery Team:
All Contact Information is located in Appendix A/B

The PeopleSoft Recovery Team is composed of the IT Specialists within Information Technology Services that support the PeopleSoft system as well as the User Application Specialists and a Network Specialist. The primary function of this small working group is the restoration of all modules of the PeopleSoft application to the most recent pre-disaster configuration in cases where data loss is significant. In less severe circumstances the team is responsible for restoring the system to an operational status as necessitated by any hardware failures, network outages or other circumstances that could result in diminished system performance.

The team should be mobilized in the event that the PeopleSoft HRSA and/or FM systems experience 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 Director of Application Services has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of the PeopleSoft recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Gene Rau (Recovery Team Lead)
DBA	Tiffany Price (Alternate Team Lead)
DBA	Larry Bergman
PSApps	Kim Black
Security	Jamie Schademan
Web Services	Larry Beintema
Payroll	Natalie Kovalerchuk
HR	Susan Haberman
SA	Crystal Wang
FMS	Greg Coles
Data Validation:	
Admissions	Kathy Gaer
HR/Payroll	Marie McGowan
	Jana Kruckenberg, Adrian Naranjo
SA	Jillian Hernandez, Tami Morrill
FMS	Tim McGuire

5.6 RESNET SERVICES RECOVERY TEAM:
All Contact Information is located in Appendix A

The Resnet Services Recovery Team is composed of the IT Specialists within Information Technology Services that support the Resnet services. The primary function of this small working group is the restoration of the Resnet services to the most recent pre-disaster configuration in cases where data loss is significant. In less severe circumstances the team is responsible for restoring the networks to an operational status as necessitated by any hardware failures, network outages or other circumstances that could result in diminished system performance.

The team should be mobilized in the event that the Resnet services 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 Director of Networks and Operations has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of the Resnet Services recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Steve Breyfogle (Recovery Team Lead)
Networks	Chris Timmons, Jason Gerdes
Auxiliary Services	Nathan Hill
Telecom	Nancy Jackson, Randy Patterson

5.7 TELECOMMUNICATIONS Recovery Team:
All Contact Information is located in Appendix A

The Telecommunications Recovery Team is composed of personnel within the Information Technology Department that support Central Washington University's voice networks. The primary function of this small working group is the restoration of Central Washington University's voice networks to the most recent pre-disaster configuration in cases where voice network loss is significant. In less severe circumstances, the team is responsible for restoring the voice network to an operational status as necessitated by any failures or other circumstances that could result in diminished 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.

The Manager of Telecommunications has the responsibility to keep the IT Incident Director up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will be accomplished with other recovery efforts on campus by the IT Incident Director.

System Name:	Nancy Jackson (Recovery Team Lead)
PBX	Randy Patterson (Alternate Team Lead)
Networks	Wade Richardson
Networks	Steve Ashbrooks

5.8 CWU CRITICAL SUPPORT CONTACTS:
All Contact Information is located in Appendix B

On Campus Contacts:	
President's Office	James Gaudino, President
Provost	Marilyn Levine, VP
Business and Financial Affairs	George Clark, VP
Student Affairs and Enrollment Management	John Swiney, VP
University Relations	Linda Schactler, VP
Facilities Management	Bill Vertrees, VP
Public Safety and Police Services	Michael Luvera, Director
Health Center	Jackson Horsley, Medical Director
University Housing	Richard DeShields, Director
Off Campus Contacts:	
Fairpoint Communications	Bill Malasich, Patrick Murphy
K20 Administrative Contact	Steve Paulson
City of Ellensburg (Inet)	Bob Johnson
K20 Internet Circuit	noc@wa-k20.net
Charter Communications	Ron Graaff
K20 Point-To-Point Circuits	Washington State DIS Helpdesk

6.0 DISASTER PREPAREDNESS

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

6.1 Data Recovery Information:

Backup/Recovery disks and tapes 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. At Central Washington University full backups of all servers are performed weekly. Those servers not in the full backup list have an incremental done. Backup/Recovery tapes are stored in the locations and for the retention periods outlined in Appendix D, and are summarized in the table below:

Backup Period	***Storage Location***	***Authorized Personnel***
Daily Backup	Backup Unit Wildcat Shop Central Washington University	Networks and Operations Personnel
Weekly Backup	Backup Unit Wildcat Shop Central Washington University	Networks and Operations Personnel
Monthly Backup	CWU Vault Hebeler Hall Central Washington University	Operations Personnel
Yearly Backup	CWU Vault Hebeler Hall Central Washington University	Operations Personnel

NOTE: Central Washington University does not have systems in place to backup and restore information/data located on individual desktop systems throughout the campus. Only the servers located in the Data Center and auxiliary Data Centers 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 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 to the user.

The Information Technology Services recommends and will encourage 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.

A cloned disaster recovery backup unit is in place in Bouillon 218 in a secured and alarmed communications room. This unit is for the purpose of off-site cloning of tapes. Networks & Operations Staff is responsible for the daily cloning of tapes for the purpose of disaster recovery.

6.2 Central Data Center and Server Recovery Information:

In the event of any disaster which disrupts the operations in the Data Center, reestablishing the Data Center will be the highest priority and a prerequisite for any IT recovery. As such, Information Technology Services is required to have detailed information and records on the configuration of the Data Center and all servers and ancillary equipment located in the Data Center and auxillary Data Center located in the SURC building. Detailed information is documented in the online database located at http://www.cwu.edu/~its/security/hardware.php. This database is updated and copied monthly to CD and stored in the Hebeler vault with the backup tapes. The operations staff is responsible for keeping the hardware inventory up to date.

6.3 Network & 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 IT recovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the Data Center. As such, Information Technology Services is required to have detailed information and records on the configuration of the networking equipment. Detailed information of switches and routers is documented in the online database located at http://www.cwu.edu/~its/security/hardware.php. This database is updated and copied monthly to CD and stored in the Hebeler vault with the backup tapes. The networking staff is responsible for keeping the networking 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 identical configuration as they existed prior to the disaster. Detailed information on critical central applications will be documented in the online database located at http://www.cwu.edu/~its/security/hardware.php. This database is updated and copied monthly to CD and stored in the Hebeler vault with the backup tapes. Server administrators are responsible for keeping the application 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 Computer Support 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 at http://www.cwu.edu/~its/security. This web site is backed up nightly.

7.0 DISASTER RECOVERY PROCESSES AND PROCEDURES:

7.1 Emergency Response: The requirement for an Emergency Response Team (ERT) involvement and the membership of the ERT will be dependent on the size and type of the incident. In addition, the actions of the ERT will be accomplished prior to the execution of this plan. Examples of situations which will normally result in the involvement of the ERT 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 not limited to, damage from an earthquake or tornado.
- Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contaminations 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-threatening situations.

Examples of situations which will normally not result in the involvement of the ERT include:

- Major system/hardware failures that do not pose a hazard to personnel or property.
- Utility outages (electrical, etc.) which are remote to the Data Center being affected.

NOTE: For any situation/incident which requires the involvement of an ERT; the IT Incident Director, Incident Command Team, nor any Recovery Team member will access the facility until the ERT leader has authorized access. The Emergency Preparedness Plan is located at: http://www.cwu.edu/~police/docs/emergency-preparedness-plan.pdf.

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

Incident Occurrence: Upon the occurrence of an incident affecting the IT services at Central Washington University, the President & Assistant Vice President of Information Technology will be notified by 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 AVP of IT will assume his/her responsibilities as the Incident Director, 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 used
- Scheduled 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 Director.

Incident Command Headquarters (ICH) locations are:

- Primary ICH: ITS Department Conference Room (Bouillon 202)
- Secondary ICH: Barge Conference Room (Barge 412)
- Backup ICH 1: Library Classroom Lab (Library 154)
- Backup ICH 2: Shaw Smyser Lab (SS214)

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 Director will work closely with overall CWU Disaster Recovery Management to determine the

appropriate course of action. The ID is responsible for locating an alternate site for the team and re-evaluating the best strategy for recovery.

Incident Assessment: The Incident Command Team (ICT) will receive an initial briefing from the Incident Director (ID) and any other personnel invited to the meeting (ERT personnel, etc.) The ICT will assess the situation, perform a walk-through of affected areas as allowed, and make a joint determination as to the extent of the damage and required recovery effort. Based on this 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 are contacted to report to work to evaluate and resolve the situation.
- **DISASTER**: The Incident Director contacts the CWU Management Team Lead (CWU President or designee) and notifies him/her of the situation, and that an IT Disaster has been declared. The ICT identifies which areas of the IT infrastructure are affected, and contacts the members of the specific Disaster Recovery Teams. 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 provided with other personnel employed or not employed at CWU.

Once an IT disaster has been declared, and the preceding steps to notify the CWU Management Team and the Recovery Teams have been accomplished, ongoing responsibilities of the Incident Command Team and Director include:

- Securing all IT facilities involved in the incident to prevent personnel injury and minimize additional hardware/software damage.
- Supervise, coordinate, communicate, and prioritize all recovery activities with all other internal / 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 CWU Management Team on the status of the recovery effort. Only the CWU Management Team and/or their designees will provide updates to other 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, CWU Teams, 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 for food/refreshments for recovery teams, etc.
- Make final determination and assessment as to recovery status, and determine when IT services can resume at a sufficient level.

7.3 Disaster Recovery Teams: Seven 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 Central Washington University Management Team.

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 Data Center and Network/Telecommunications infrastructure will normally be assigned the highest priority, as full operational recovery of most other systems can not occur until these areas are operational.

7.3.1 Auxiliary Services Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery to Auxiliary Services.
3. Identify other individuals required to assist in recovery of these applications, and report this information to the ID for action.
4. Restore degraded system functions at backup site and inform user community of the restrictions on usage and/or availability.
5. Coordinate software replacement with vendor as required. (See Appendix F for vendor and contact information)
6. Coordinate Auxiliary Services recovery with other recovery efforts.
7. Execute plan to the Auxiliary Services to full function.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Auxiliary Services to pre-disaster functionality.

7.3.2 Database Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery to Database services.
3. Identify other individuals required to assist in recovery of these applications, and report this information to the ID for action.
4. Restore degraded system function at backup site and inform user community of the restrictions on usage and/or availability.
5. Coordinate software replacement with vendor as required. (See Appendix F for vendor and contact information)
6. Coordinate Database services recovery with other recovery efforts.
7. Execute plan to restore Database services to full function.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Database services to pre-disaster functionality.

7.3.3 Data Center Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery of Central Data Facility. Determine if use of alternate/cold site is required.
3. If the alternate data center site is required, execute all necessary steps to notify appropriate personnel and secure backup facility.
4. Identify other individuals required to assist in recovery of data center, and report this information to the ID for action.
5. Develop overall recovery plan and schedule, focusing on highest priority servers for specific applications first. (Appendix E documents the priority areas of the campus for IT service recovery)
6. Coordinate hardware and software replacements with vendors. (See Appendix F for vendor and contact information)

7. Recall backup/recovery tapes from on campus or off-campus storage, as required to return damaged systems to full performance.
8. Oversee recovery of data center based on established priorities.
9. Coordinate data center recovery with other recovery efforts on campus.
10. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
11. Verify and certify restoration of the data center to pre-disaster functionality.

7.3.4 Desktop Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment 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 report this information to the ID for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure/desktop services first. (Appendix E documents the priority areas of the campus for IT service recovery)
5. Coordinate hardware and software replacement with vendors. (See Appendix F for vendor and contact information)
6. Oversee recovery of desktop computing services (workstations, printers, etc.) based on established priorities.
7. Coordinate recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the desktops to pre-disaster functionality.

7.3.5 Messaging Recovery/Network and Telecommunications Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of services, and report this information to the ID for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first. (Appendix E documents the priority areas of the campus for IT service recovery)
5. Coordinate hardware and software replacement with vendors. (See Appendix F for vendor and contact information)
6. Oversee recovery of messaging, telecommunications and network services based on established priorities.
7. Coordinate messaging, network and telecommunications recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Messaging, Network and Telecommunications infrastructure to pre-disaster functionality.

7.3.6 PeopleSoft Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery to PeopleSoft services.
3. Identify other individuals required to assist in recovery of these applications, and report this information to the ID for action.

4. Restore degraded system function at backup site and inform user community of the restrictions on usage and/or availability.
5. Coordinate software replacement with vendor as required. (See Appendix F for vendor and contact information)
6. Coordinate PeopleSoft services recovery with other recovery efforts.
7. Execute plan to restore PeopleSoft services to full function.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the PeopleSoft services to pre-disaster functionality.

7.3.7 Resnet Services Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of services, and report this information to the ID for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first. (Appendix E documents the priority areas of the campus for IT service recovery)
5. Coordinate hardware and software replacement with vendors. (See Appendix F for vendor and contact information)
6. Oversee recovery of resnet services based on established priorities.
7. Coordinate resnet recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Messaging, Network and Telecommunications infrastructure to pre-disaster functionality.

7.3.8 Telecommunications Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of these services, and report this information to the ID for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first. (Appendix E documents the priority areas of the campus for service recovery.)
5. Coordinate hardware/software replacement with vendor as required. (See Appendix F for vendor and contact information)
6. Oversee recovery of voice network services based on established priorities.
7. Coordinate the voice network recovery with other recovery efforts.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding 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 at Central Washington University. 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:

NOTE: 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 steps be 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 Data Center operational/recoverable?
        i. YES: Remain in primary data center and initiate DRP accordingly.
        ii. NO: Contact personnel responsible for Backup Data Center and take necessary 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 steps to redirect network routes and ready the backup facility.
    c. Determine extent of applications affected
        i. Peoplesoft System
        ii. Messaging (Email, Scheduling)
        iii. Web Services (cwu.edu)
    d. Determine extent of desktop/client systems affected throughout the 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 (Data Center, Communication Rooms, etc.) as necessary to prevent unauthorized access.
3. Retrieve most recent on-site or off-site back-up media for previous three back-ups. Prepare back-up media for transfer to primary or secondary data center, 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 to repair or replace as needed.
5. Test systems, and communication equipment as required to validate physical operation and performance.
    a. Server testing
    b. Network testing
    c. Desktop/Client testing
6. Upon restoration of the Data Center and servers to operational state:
    a. Load Operating System and test/validate
    b. Load Application Software and test/validate
    c. Load Data and verify integrity
7. Verify overall performance of specific system(s) and report readiness to Incident Command Team, Management Team, and user community.

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 on Central Washington University as well as in the Data Center. Remote equipment is located in Communication Closets, often in multiple sites in a single building. In addition, data and telecommunication cabling runs throughout the campus and buildings, making it susceptible to varying levels of damage.

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

1) Earthquake
    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 or deterioration
    b) Test primary copper data feeds for destruction of deterioration
    c) Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water 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 or deterioration
    b) Test primary copper data feeds for destruction of deterioration
    c) Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water or other agents.
    d) Assess all equipment with air filtration systems to assure adequate ventilation remains.

Central Washington University network diagrams are included in Appendix G.

APPENDIX A: Central Washington University: Information Technology Services Directory/Contact List.

Confidential information removed for web publishing.

APPENDIX B: Central Washington University Critical Support Contacts List.

Confidential information removed for web publishing.

The Central Washington University Personnel Directory (2006-2007) and contact information is included with the hardcopy version of this plan. Copies of the plan are located in the ITS Office (Bouillon 202), the Computer Center and the Vault (Hebeler).

Confidential information removed for web publishing.

APPENDIX C: Central Washington University – Asset Management Information

The following printouts, asset management information, and documents are included with the hardcopy version of this plan. Detailed information is documented in the online database located at http://www.cwu.edu/~its/security/hardware.php.

- Server Asset Management Information
- Network Active Hardware Asset Management Information
- Application Software Configuration Information
- Desktop Equipment Asset Management Information

APPENDIX D: Central Washington University – System Backup/Tape Retention Periods

All servers in the Computer Center are backed up on this schedule:
http://beintema.cts.cwu.edu/~beintema/networker_schedule.html
Retention information is located in section 6.1 of this document.

Schedule of Legato networker host saves (January 2012)

S - skip I - incremental F - full
Full saves start at 12:10 a.m., usually done by 8am
Incrementals start at 2:00 a.m., usually done by 5am

Hostname	Sun	Mon	Tue	Wed	Thu	Fri	Sat
aeolus.lab.cwu.edu	F	I	I	I	I	I	I
alecto	I	I	I	I	I	I	F
alipes2.cts.cwu.edu	S	F	I	I	I	S	I
ananke	F	I	I	I	I	I	S
anat.cts.cwu.edu	S	F	I	I	I	I	I
aphrodite	S	I	I	I	I	I	F
apollo.saffrs.cwu.edu	I	S	F	I	I	I	I
apps-01.aux.cwu.edu	F	I	I	I	I	I	S
arges.cts.cwu.edu	I	I	I	I	S	F	I
aries.cts.cwu.edu	S	S	S	S	S	S	S
aris	S	S	S	I	S	S	F
aristotle.lab.cwu.edu	I	I	I	I	I	F	S
asherah.cts.cwu.edu	S	I	I	I	I	I	F
athena.cwu.edu	S	I	I	F	I	I	I
atlas.cts.cwu.edu	I	S	F	I	I	I	I
azure.cts.cwu.edu	S	I	I	I	F	I	I
barchetta.lib.cwu.edu	S	S	S	S	S	S	S
bbdata.cts.cwu.edu	I	I	I	I	I	F	S
bbweb.cts.cwu.edu	I	S	I	I	I	F	S
beintema.cts.cwu.edu	S	I	I	I	I	F	I
blackbaud.unadv.cwu.edu	I	I	I	I	I	F	S
bonsai.cts.cwu.edu	F	I	I	I	I	I	S
boreas	F	I	I	I	S	S	I
bruker05.chemistry.cwu.edu	S	I	I	I	I	F	I
capricorn.cts.cwu.edu	S	S	S	S	S	S	S
ccs.aux.cwu.edu	F	I	I	I	I	I	S
ccstst.aux.cwu.edu	F	I	I	I	I	I	S
cerise.aux.cwu.edu	S	I	I	I	I	I	F
chinstrap.lib.cwu.edu	S	S	S	S	S	S	S
clmdb.cts.cwu.edu	S	F	I	I	I	I	I
clmtest.cts.cwu.edu	S	F	I	I	I	I	I
clmweb.cts.cwu.edu	S	F	I	I	I	I	I
clotho	I	I	I	I	I	F	I
columba.cts.cwu.edu	S	S	S	S	S	S	S
courses2.cwu.edu	S	S	S	S	S	S	F
crimson.cts.cwu.edu	S	S	F	I	I	S	I
cyan.cts.cwu.edu	I	S	I	F	I	I	I
cygnus.cwu.edu	I	S	F	I	I	I	I
daffy.cts.cwu.edu	S	I	I	I	I	I	F
dbackup0.cts.cwu.edu	S	I	S	F	S	I	S
dbackup1.cts.cwu.edu	S	S	F	S	I	S	I
dbtest.cts.cwu.edu	S	S	S	S	S	S	S
demeter	I	S	F	I	I	I	I
diana	F	I	I	I	I	I	S
diebolddb.aux.cwu.edu	I	S	F	I	I	I	I

donald.cts.cwu.edu	S	I	I	I	I	I	F
dynobites.aux.cwu.edu	S	I	F	S	I	I	I
eldorado.chemistry.cwu.edu	S	S	S	S	S	S	S
etclib.ed.cwu.edu	I	F	S	I	S	I	S
eunomia.cts.cwu.edu	I	I	I	I	I	I	F
ezp.lib.cwu.edu	S	F	I	I	I	I	I
fileproxy.cwu.edu	F	S	I	S	I	S	I
flex.aux.cwu.edu	F	I	I	I	I	I	S
fmail.cts.cwu.edu	S	I	I	I	I	I	F
fuschia.cts.cwu.edu	S	I	F	I	I	I	I
galileo.phyplt.cwu.edu	F	I	I	I	I	I	S
gizmonic.cts.cwu.edu	S	F	I	I	I	I	S
gridiron.cts.cwu.edu	F	I	I	I	I	I	S
gridlock.cts.cwu.edu	I	S	F	I	I	I	I
gw-gate2.cwu.edu	S	I	I	I	I	I	F
gw-stu1.cwu.edu	S	I	I	I	I	I	F
gw-stu2.cwu.edu	S	I	I	I	F	I	I
gw-stu3.cwu.edu	F	I	I	I	I	I	S
gw-stu4.cwu.edu	I	I	I	F	I	I	S
gw-stu5.cwu.edu	I	S	F	I	I	I	I
gw-stu6.cwu.edu	S	I	I	I	F	I	I
hcc.aux.cwu.edu	F	I	I	I	I	I	S
hccaud.aux.cwu.edu	F	I	I	I	I	I	S
hermes	I	S	S	F	S	I	S
horizon.cts.cwu.edu	F	I	I	I	I	I	S
housing.aux.cwu.edu	S	S	S	S	S	S	S
hubris.cts.cwu.edu	S	I	I	I	I	F	S
hypnos	S	F	I	I	I	I	I
indigo.cts.cwu.edu	I	S	I	I	F	I	I
keybox.cts.cwu.edu	S	F	I	I	I	I	I
kronos.aux.cwu.edu	S	F	I	I	I	I	I
kryten.cts.cwu.edu	S	I	I	I	I	I	F
labstats.cts.cwu.edu	F	I	I	I	I	I	S
lavender.cts.cwu.edu	S	I	F	I	I	I	I
library	I	F	I	I	I	I	S
lister.cts.cwu.edu	S	I	I	I	I	I	F
localhost6.localdomain6	S	S	S	S	S	S	S
logopolis.hpc.cwu.edu	S	I	I	I	I	I	F
magenta.cts.cwu.edu	I	I	I	F	S	I	I
maroon.aux.cwu.edu	I	I	I	S	I	S	F
mauve.cts.cwu.edu	F	I	I	I	I	I	S
megaera.cts.cwu.edu	S	I	F	I	I	I	I
mercury2.cts.cwu.edu	I	I	I	S	I	S	F
microsapp.aux.cwu.edu	S	I	F	I	I	I	I
microsdb.aux.cwu.edu	S	I	F	I	I	I	I
midas.adm.cwu.edu	S	F	I	I	I	I	I
min.cts.cwu.edu	F	I	I	I	I	S	I
mingo.lib.cwu.edu	S	S	S	S	S	S	S
mira.cts.cwu.edu	I	I	I	S	F	I	I
mot.resnet.cwu.edu	F	I	I	I	I	I	S
mtrainier.cts.cwu.edu	S	F	I	I	I	I	S
mysql.cts.cwu.edu	S	I	I	I	I	I	F
n.cwu.edu	S	F	I	I	I	I	I
nergal.cts.cwu.edu	S	I	S	I	I	I	F
nsc0.cwu.edu	I	S	F	I	I	I	I
nsc0.resnet.cwu.edu	F	I	I	I	I	I	S
nsc1-831.cwu.edu	I	F	I	I	I	I	S
nsc1.resnet.cwu.edu	S	F	I	I	I	I	I
nyx	F	I	I	I	I	I	S
ochre.cts.cwu.edu	S	I	I	I	I	I	F

```
otm.cts.cwu.edu                S   F   I   I   I   I   I
pa.cts.cwu.edu                 S   F   I   I   I   I   I
panteknicon.cts.cwu.edu        S   I   I   I   I   I   F
pc78221.d.cwu.edu              S   S   S   S   S   S   S
plato.lab.cwu.edu              S   I   I   I   I   I   F
pollux.cts.cwu.edu             S   S   S   S   S   S   S
poseidon                       I   S   F   I   I   I   I
prometheus.cts.cwu.edu         F   I   I   I   I   I   S
qadesh.cts.cwu.edu             F   I   I   I   I   S   I
r25.cts.cwu.edu                S   F   I   I   I   I   I
resheph.cts.cwu.edu            F   I   I   I   I   S   I
resnet.cwu.edu                 F   I   I   I   I   I   S
rima.cts.cwu.edu               F   S   S   I   S   S   S
rimmer.cts.cwu.edu             S   I   I   I   I   I   F
ronald.cts.cwu.edu             S   I   I   I   I   I   F
scarlet.cts.cwu.edu            I   S   I   I   F   I   I
screencast.clt.cwu.edu         S   S   I   F   I   S   I
sheena.cts.cwu.edu             F   I   I   I   I   I   I
smail.cts.cwu.edu              S   I   I   I   I   I   F
socrates                       S   I   I   I   I   F   I
spectrum.ed.cwu.edu            S   S   F   I   I   I   I
streamer0.cts.cwu.edu          S   S   I   S   S   F   S
studentmedia.cwu.edu           S   I   I   I   I   I   F
telemgr.cts.cwu.edu            S   I   I   I   I   I   F
telos.cts.cwu.edu              S   S   F   S   S   I   S
telsrv.cts.cwu.edu             S   I   I   I   I   I   F
tethys                         I   S   F   I   I   I   I
themis.cwu.edu                 I   S   F   I   I   I   I
tiamat.cts.cwu.edu             F   I   I   I   I   S   I
tisiphone                      S   I   I   I   I   I   F
trix.aux.cwu.edu               I   S   F   I   I   I   I
uhnsp.aux.cwu.edu              S   F   I   I   I   I   I
uhnsptst.aux.cwu.edu           F   I   I   I   I   I   S
umber.cts.cwu.edu              S   I   I   I   I   I   F
vmail.cts.cwu.edu              S   I   I   I   I   I   F
w3cache0.cts.cwu.edu           F   I   I   I   I   I   S
wmail.cts.cwu.edu              S   I   I   I   I   I   F
worf.cts.cwu.edu               S   I   I   F   I   I   I
zephyrus                       S   I   I   F   I   I   I
zeus.cwu.edu                   I   I   S   I   F   I   I
```

Servers:

Server information is documented in the online database located at http://www.cwu.edu/~its/security/hardware.php.

Hardware Database:

The hardware database is updated/reviewed every month by the Networks & Operations staff. The database is copied to CD monthly and stored in the vault located Hebeler.

When major configuration changes take place, new CDs will be created upon its completion.

APPENDIX E: Central Washington University: IT Recovery Priority List

The following priorities have been established by the Director of Information Technology Services and by CWU Senior Management for the recovery of IT Services to the university.

IT Infrastructure Priorities: This establishes the internal priorities for recovering the major infrastructure components for IT services. These priorities are based on the relationship between these systems, and the pre-requisite nature of many of the items in order to be able to return full services to the campus.

1. Data Center
2. Network Services (as prioritized below)
3. Messaging Services (email/calendaring)
4. Web Services
5. Peoplesoft Applications
6. Online Course Delivery and Classroom Technology

Central Washington University Functional Priorities for IT Recovery: This establishes the priorities for recovering IT services for specific customers and facilities across the campus. While the Data Center, Peoplesoft, Web, and Messaging Services are centrally located, and will normally be recovered for all users simultaneously, recovery of network and desktop services will be accomplished based on the following priorities, in order to return critical campus systems and facilities to operational status at the earliest possible time.

Priority	Administrative System	Primary Staff
L	Alumni	Jim Armstrong
M	Blackboard	Jane Chinn
L/M	Conference Center (CCS)	Ken Baxter
M	Course Management R25	Xinbao Wang
L	Daycare Management	Janie Charlton
C	Diebold/CBORD	Tad Pierce
H	Dining Services (DINE,Computrition)	Dan Layman
H/C	Electronic Mail	Bill Glessner, Greg DeLuca
M	Facilities Planning (Facility MAX)	Jason Cathcart,
M	File Services	Greg DeLuca, Terilee Germain
H	Finance (FMD)	Shirley Pruitt
H	Financial Aid (HRSA)	Jillian Hernandez, Tami Morrill
L	Health Services	Jackson Horsley
H	Housing	Richard DeShields
L	Institutional Research	Mark Lundgren
L/M	Instructional Computing (MTIS)	Jane Chinn
L/M	Library	Ping Fu
L	Parking (CPAS)	Trish Swanson
H	Payroll (Safari)	Darcy Hansen
H/C	ResNet	Jason Gerdes
H	Safari / HR	
L	Student Recreation (Class)	Bob Ford
C	Telecommunications	Nancy Jackson
L/M	University Store (Sequoia,IBIDie)	Steve Wenger
C	Web Services	Linda Schactler

Classifying computer application systems:

Critical – Must be processed in normal mode; no degradation is acceptable.
High – Only high priority; e.g., high dollar item transactions or critical reports will be processed.
Medium – Processing will be carried out on a "time available" only basis.
Low – Processing will be suspended, but data collection will continue.
Full – No processing or data collection will be carried out until normal computer capacity is restablished.

Facility Priorities:

Priority	Building Name	Priority	Building Name
M	1800 Building	L	Lyon (Yakima)
L	Archives	L	Mail and Duplicating
H	Barge	C	Manastash
H	Barto	L/M	McConnell
H	Beck (Resnet Sector Building)	H	Meisner
M	Black	M	Michaelsen
C	Boiler Plant	H/C	Mitchell (Sector Building)
C/H	Bouillon (Sector Building)	M	Moses Lake
H	Brooklane	H	Munson
H	Button	M	Music
H	Carmody-Munro	L	Naneum
M	CHCI	M	Nicholson
C	Computer Center	H	Old Boiler Plant
M	Dean	M	Olympic (Pierce)
M	Deccio (Yakima)	M	Dorothy Purser (PE)
M	Des Moines	M	Peterson (ROTC)
M	Farrell	H	Wendell Hill (SVS)
M	Flight	L	Pool
H	Green (Resnet Sector Building)	M	Power Tech
L	Grounds	M	PresRes
C	Health Center	M	Psychology
M	Hebeler	M	Randall
L	Hertz	H	Residential Housing
M	Higher Education Center (Highline)	C/H	Science (Sector building)
M	Hogue	M	Shaw-Smyser
L/M	International	C	Student Union & Recreation Center
H	Jansen	L	SUB (OLD)
C	Jongeward	M	Sue Lombard
H	Kamola	L	Surplus
H	Kennedy	H	Tunstall
M	L and L	L	Warming Hut
C/H	Library (Sector Building)	M	Wenatchee
M	Lind	H	Wilson
M	Lynnwood		

Classifying buildings:

Critical, needed for maintenance of public health and safety, communications.
High, needed for income maintenance for students, employees; payments to vendors; requirements for compliance or regulation; effect on state government cash flow; effect on production and delivery of services (housing, dining, student services).

Medium, needed for mission of university, delivery of classes.
Low, everything else.

APPENDIX F: Central Washington University: Vendor Information

Confidential information removed for web publishing.

APPENDIX G: Central Washington University: Network Diagrams

Printouts of the Central Washington University network architecture diagrams are included with the hardcopy version of this plan.

APPENDIX H: Excerpt from the Emergency Preparedness Plan

SECTION 2

Emergency Preparedness Organizational Chart
Board of Trustees
*
President
*
Emergency Coordinator
(Executive Assistant to the President)
*
Emergency Council

Council Members

Response Coordinator (Director of Public Safety and Police Services)
- Emergency operations center/communications systems (Radios)
- Field operations (Police Services)
- Coordination with responding agencies
- Security/access for restricted and sensitive areas
- Short and advanced warning notice/call list
- Search and rescue

Facilities Coordinator (Director of Facilities Management)
- Building/grounds assessment, inspection, and operations
- Utility assessment, inspection, and operations
- Field operations (Facilities Management Services)
- Coordination to Telco, Data, and Video Systems
- Emergency sanitation facilities
- Arrange for temporary classroom facilities
- Coordination of utilities with outside agencies

Finance Coordinator (VP for Business and Financial Affairs)
- Registration of emergency workers
- Cash and negotiables safeguarding
- Record keeping
- Emergency purchases and leasing
- Data safeguarding

Academic Coordinator (Provost)
- Coordinate on-going teaching/classroom operations
- Arrange for temporary classroom equipment
- Arrange for temporary faculty resources

Student Affairs (VP for Student Affairs and Enrollment Management)
- Student support and counseling
- Emergency Shelter
- Emergency feeding
- Sign-up and organize emergency workers/message runners
- Mass casualty/medical services center/liaison
- Disabled people

Community Relations (VP for University Relations)
- Media Liaison
- Public relations
- Emergency message/contact center
- Organize video documentation of damage

Business Services (Director of Business Services and Contracts)
- Emergency proclamations
- Emergency contracts
- Risk Management
- Supply and procurement

Appendix J – Business Impact Matrix

CWU IT System Business Impact Matrix	Maintenance of Public health and safety	Income maintenance for citizens	Income maint. for gov. employees	Payments to vendors for G&S	Requirements for compliance or regulation	Effect of state government cash flow	Recovery Costs	Effect on product and delivery of services	Volume of activity	Effect on public image	Inter-system dependency
Alumni*	L	L	L	L	L	L	L	L	L	L	L
Blackboard	L	L	L	L	L	L	L	L	L	L	L
Campus Security (CAMPSA)*	H	L	L	L	H	L	L	H	H	H	H
Central Stores	L	L	M	L	L	H	L	H	H	H	M
Conference Center (CCS)*	L	L	L	L	L	L	L	H	M	M	L
Course Management (R25)	L	L	L	L	L	L	L	L	L	L	L
Daycare Management*	L	L	L	L	L	L	L	L	L	L	L
Diebold/CBord*	H	L	H	L	L	L	M	H	H	H	H
Dining Services (DINE,Computrition)*	M	L	H	L	L	H	H	H	H	H	H
Electronic Mail	L	L	L	L	L	L	L	L	H	L	L
Facilities Planning (WOS)*	L	L	L	L	L	L	M	H	H	H	M
File Services	L	L	L	M	M	L	M	H	H	M	H
Finance (FMD)	L	L	L	M	H	L	H	H	H	H	H
Financial Aid (HRSA)	L	L	L	L	H	L	H	H	H	H	H
Health Services	H	L	L	L	H	L	M	H	H	H	M
Housing/Resnet	H	L	L	L	L	L	H	H	H	H	M
Institutional Research*	L	L	L	L	L	L	L	L	L	L	L
Instructional Computing (MTIS)	L	L	L	L	L	L	L	L	L	L	L
Library*	L	L	L	L	L	L	L	L	L	L	L
Parking (CPAS)*	M	L	L	L	L	L	L	L	L	L	L
Safari (Payroll/AP/AR)	L	L	L	L	H	L	H	H	H	H	H
Telecommunications	H	L	L	L	L	L	H	H	H	H	H
University Store (POSS/Censtore)*	L	L	M	L	L	L	L	L	L	L	L
Web Services	H	L	L	L	L	M	L	H	H	H	L
Web Services	L	L	L	L	L	L	L	L	H	H	L

Appendix K - Threat and Vulnerability Matrix - Physical

THREAT	VULNERABLE AREAS	RESULT	PROTECTIVE MEASURES	RISK
Electrical outages Fluctuations	Computer Center Networks LANs Telephone Service	-Equipment Damage -Denial of Service -Data Destruction -Data Corruption	UPS System System Backups Generator Staff Training	High
Telecommunicatio n Network Failure	Main Computing Networks LANs Telephone Service	-Denial of Service	Alternate routing UPS System Generator Staff Training	High
Hardware Failure	Computer Center Networks LANs Telephone Service	-Denial of Service -Data Destruction -Data Corruption -Equipment Loss	On-Site Engineer Hardware contracts 24-hour support by Networks & Operations System Backups Staff Training	High
System Software Failure Alteration of Software	Main Computing Networks	-Denial of Service -Data Destruction -Data Corruption	Software support by vendor System Backups Staff Training	Low
Application Software Failure	Applications	-Denial of Service -Data Destruction -Data Corruption	24-hour support by applications System Backups Staff Training	Medium
Fire	Computer Center Networks LANs Telephone Service	-Denial of Service -Data Destruction -Equipment Loss -Facility Loss	Fire alarm systems Halon systems Employee training Access control Structural Design Off-site backups Contingency Plan	High
Water Damage	Computer Center Networks LANs Telephone Service	-Denial of Service -Data Destruction -Equipment Loss -Facility Loss	Structural Design Off-site backups Contingency Plan Off-Site backups	High
File Alteration - (Accidental or Intentional) Disclosure System user error Employee Sabotage Unauthorized Use Viruses	Databases Software System integrity	-Data Corruption -Data Destruction -Denial of Service -Confidentiality breach	Security auditing Login authentication Audit trails Access control Security monitoring System Backups Staff Training	High
Physical Security Unauthorized Use Fraud External Sabotage Hackers	Computer Center Networks LANs Telephone Service	-Denial of Service -Equipment Loss -Facility Loss -Data Destruction -Data Corruption	Access control Structural design Employee training System Backups Login authentication	Medium

THREAT	VULNERABLE AREAS	RESULT	PROTECTIVE MEASURES	RISK
		-Theft	Staff Training	
Civil Disturbances Dam Collapse Earthquake Flood Lightening Smoke, dirt, dust Snow/Ice Storm Volcano Windstorm	Computer Center Networks LANs Telephone Service	-Denial of Service -Equipment Loss -Facility Loss -Data Destruction	Structural design System Backups Contingency Plan	Medium
Bomb Threats Building Collapse Epidemics Explosions Hostage Taking Hurricanes Landslides Liquid leakage Nuclear Reactor Accident Panic Crushes Sandstorms Strike Terrorism Thermo-Nuclear Disaster Tidal Waves Tornado Toxic Spills Tsunami	Computer Center Networks LANs Telephone Service	-Denial of Service -Equipment Loss -Facility Loss -Destruction of data	Structural design System Backups Contingency Plan	Low
Theft	Computer Center Databases	-Confidentiality breach -Equipment Loss	Access control Login authentication Separation of duties Staff Training	High

Appendix L – Tape Inventory

Here are the current inventory procedures for backup tapes.

Operations staff take tapes over daily and bring back the ones that are being replaced. (These are the LMS nightly processing backups).

Operations takes the weekly VMS cumulative backup tape over on Mondays. It dismounts Sunday and a new, prestaged backup initiates Monday morning at 6:30 am. Again, Operations returns the tape being replaced. weekly backups are retained for 30 days and the monthly backups for 365 days. Only the most current monthly backup is stored in the vault, older monthlies are stored in the on site tape repository.

Networks & Operations staff (Larry Beintema) uses the oldest monthly backups (created 1 year earlier) from Legato as scratch tapes for the current monthly backup. Operations brings them over the Monday after the first weekend of the month and returns the newly created backups the following morning.

Operations takes backup tapes from the email machines and the VCS console to the vault on Monday and brings the tapes being replaced back.

There are currently old tapes that were created with 5 and 10 year retentions stored in the vault and they are returned and scratched as they expire.

Each of the above backups has their own space in the vault so they are easily identified and retrieved when necessary.