University of New Orleans

EMERGENCY PROCEDURES MANUAL
For
University Computing and Communications

I. GOALS

SAFETY GOALS

• Ensure that University Computing and Communications (UCC) staff have adequate time to secure their own personal property and take appropriate safety measures for their families
• Protect the university’s mission critical data
• Protect the university’s major computer and communications systems

SERVICE GOALS

• Continue to provide the university with mission critical communication systems throughout the emergency
• Remote voice messaging
• Backbone networking
• Access to emergency administrative systems
• Access to E-mail
• Access to the Internet and UNO home page
• Provide the university with a rapid restoration of normal computer and communication services after an emergency

DATA INTEGRITY GOALS

• Assemble three (3) complete sets of software and data files for mission critical functions:

  1. Exists in the UNO Main Campus Computer Center on the normal production disk subsystem.
  2. Exists in the data center at the Frey Computer Center at the LSU Baton Rouge Campus.
  3. Exists in offsite commercial storage space and is comprised of the current weekly incrementals and the previous full backup. See Appendix I.
II. INTRODUCTION

Due to the costs associated with completely duplicating all computer functions running on the UNO campus, UNO has opted to maintain a mirror site only for mission critical functions. See Appendix B. This site is located at the Frey Computer Center on the LSU Baton Rouge campus. The main site can be switched over to the mirror site within 30-60 minutes depending on circumstances.

The following are identified as mission critical functions:

- DNS (Domain Name Server)
- Domain controllers (Active Directory)
- Web (UNO Home Page)
- Email (MS Exchange for faculty/staff and students)
- PeopleSoft Learning Solutions (HR/Payroll/Student Administration)
- PeopleSoft Financials (General Ledger, Purchasing, Payables)
- SharePoint
- Enterprise Backup and Restore

Additionally, servers for DNS and Active Directory functions are also maintained at a third site located at the Louisiana Tech University in Ruston.

Actions taken by the technical support staff in the event of an emergency will be determined by the type/nature of the threat and by the amount of advanced warning received.

Types of Threats
The types of threats addressed in this emergency procedures manual include bomb, fire, water, wind, electrical, hurricane and pandemic. Advanced warning is the amount of time available to respond to a particular threat. The advanced warning time values are no warning, thirty minutes, one hour, four hours and eight hours for bomb, fire, water, wind or electrical threats. Hurricane alert times are 12, 24, 48, and 72 hours. The threat and response time will determine what alert level will be declared and the corresponding actions to be taken.

Plan Updates
This plan shall be reviewed and updated, at a minimum, annually. Also, it shall be updated in response to environmental or operational changes that affect any part of the plan and following exercise of any portion of the plan that reveals deficiencies. See Appendices G and H. Copies of the plan, updates and a record of changes to the plan shall be kept on the UNO SharePoint Intranet site http://sharepoint.uno.edu. The plan shall be approved annually by the Associate VP / CIO for Computing and Communications. See Appendix C. The approved plan will then be posted in SharePoint at which time a notification will be sent automatically to the emergency team with responsibilities for the plan. See Appendix A for a listing of individuals on the emergency team.

Training
The emergency response personnel shall receive training on the emergency plan, at least annually. See Appendix F. As part of the training event, emergency response personnel will be required to take a test on the information reviewed during the event. A record of each training event, who attended and a summary of the content of the training shall be maintained within Blackboard, UNO’s learning management system.

**Plan Testing**

Those elements of the plan identified as mission critical functions shall be tested annually before the start of hurricane season. However, the testing may be done in phases or at different times of the year. Email notification that the tests will be performed shall be sent by the Associate VP / CIO for Computing and Communications to the emergency response team. Documentation on annual completion of testing shall be maintained at the back of the plan. Periodically, the Associate VP / CIO for Computing and Communications will review the documentation log to ensure adequate testing of critical functions has occurred.

**III TYPES OF THREATS**

**A. BOMB THREAT**

1. A bomb threat is information received in person or otherwise that an explosive or incendiary device has been placed in or near the Computer Research Center.

2. All UCC Employees must have a copy of and be familiar with the following UNO documents:
   1. Office Guidelines for Building Evacuations (posted in UCC front office)
   2. Bomb Threat Report (posted in UCC front office)

3. Any member of the UCC Staff receiving a bomb threat, shall perform the following actions based on the amount of warning received:

   **ACTION:**
   1. **NO WARNING TO FIFTEEN MINUTES** – Evacuate the building adhering to the Office Guidelines for Building Evacuation, seek safe shelter, contact Campus Security (x3-6666), contact a UCC Manager or Supervisor and complete Bomb Threat Report.
   2. **FIFTEEN MINUTES OR GREATER WARNING** – Follow Bomb Threat Response Procedure, contact Campus Security (x3-6666), contact a UCC Manager or Supervisor, evacuate the building adhering to the Office Guidelines for Building Evacuations, seek safe shelter and complete Bomb Threat Report.

**B. ELECTRICAL THREAT**

1. Upon loss of electrical power from Entergy, a UPS (Uninterrupted Power Supply) will supply power to the UCC machine room servers and network equipment. Within 30 seconds of switching to UPS power, a natural gas powered generator on the roof will engage and begin supplying power to the UPS and computer room AC units in place of the Entergy feed. In the event of a generator failure, the UPS can only
supply power to all UCC machine room systems for approximately 20-30 minutes.

2. Any member of the UCC Staff witnessing an electrical threat, shall perform the following actions:

ACTION:

1. Alert the Emergency Response Team, see Appendix A.
2. Contact Facility Services and inform them of the situation.
3. If the power outage is perceived to be lengthy (greater than 30 minutes) and the generator has failed to engage, all but minimal systems are shutdown to preserve battery life. The systems that are left up are comprised of Campus print servers, Campus DNS server, and a Windows Active Directory Domain Controller. The UPS systems can provide power to those systems as well as campus network equipment located in the machine room for 2 hours.
4. The Emergency Response Team will determine if “fail-over” is necessary and, if necessary, begin the changeover.
5. After one (1) hour and 45 minutes has passed and the power situation has not been resolved, responsible staff will power down remaining servers and network equipment.
6. When the power is restored and Facility Services tells the UCC that the power is stable, responsible staff will power all systems back up.

C. FIRE THREAT

1. All UCC Employees must have a copy of and be familiar with the UNO Office Guidelines for Building Evacuations document (posted in UCC front office)
2. Any member of the UCC Staff witnessing a fire, shall perform the following actions:

ACTION:

1. Pull the fire alarm.
2. Evacuate the building adhering to the Office Guidelines for Building Evacuation and seek safe shelter, closing doors and windows surrounding the fire area.
3. Contact Campus Security (x3-6666), call 9-1-1 and contact a UCC Manager or Supervisor.
4. Use a fire extinguisher only if the fire is small and:
   a. There is an escape exit or route behind you.
   b. You have received training in the use of fire extinguishers.
   c. You know the fire extinguisher is fully charged.
   d. You know what is burning and what type of extinguisher to use.
   e. The fire is not spreading rapidly
   f. There is no toxic smoke present.

D. HURRICANE THREAT
The six month period from June 1 through November 30 is considered the Atlantic and Gulf area hurricane season. During this period the UNO Computer Facility may be subject to high winds, heavy rains and other destructive phenomena generally associated with hurricanes. Storm related definitions are listed below. More information on hurricane intensity is contained in TABLE 1: HURRICANE CATEGORIES, while information on types of warnings is listed in TABLE 2: WARNING CATEGORIES.

**HURRICANE DEFINITIONS:**

**TROPICAL DISTURBANCE:** A cluster of thunderstorms poorly organized, but, usually no closed surface circulation.

**TROPICAL DEPRESSION:** A cluster of thunderstorms well organized around a central circulation with surface winds up to 39 mph.

**TROPICAL STORM:** A cluster of thunderstorms very well organized around a central circulation with surface winds sustained between 40 – 73 mph.

**HURRICANE:** Nature’s most powerful storm with surface winds above 74 mph.

**TABLE 1: HURRICANE CATEGORIES**

<table>
<thead>
<tr>
<th>Category</th>
<th>Central Pressure</th>
<th>Winds</th>
<th>Surge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Minimal</td>
<td>Greater than 980 mb or 28.94 in</td>
<td>74-95 mph or 64-82 kts</td>
<td>4-5 ft</td>
</tr>
<tr>
<td>2 – Moderate</td>
<td>965-980 mb or 28.50-28.91 in</td>
<td>96-110 mph or 83-95 kts</td>
<td>6-8 ft</td>
</tr>
<tr>
<td>3 – Extensive</td>
<td>945-965 mb or 27.91-28.47 in</td>
<td>111-130 mph or 96-113 kts</td>
<td>9-12 ft</td>
</tr>
<tr>
<td>4 – Extreme</td>
<td>920-945 mb or 27.17-28.88 in</td>
<td>131-155 mph or 114-135 kts</td>
<td>13-18 ft</td>
</tr>
<tr>
<td>5 – Catastrophic</td>
<td>Less than 920 mb or 27.17 in</td>
<td>Greater than 155 mph or 135 kts</td>
<td>Greater than 18 ft</td>
</tr>
</tbody>
</table>

**WATCH/WARNING:**

**TABLE 2: WARNING CATEGORIES**

<table>
<thead>
<tr>
<th>Warning Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coastal Flood Watch</td>
<td>The possibility exists for the inundation of land areas along the coast within the next 12 to 36 hours.</td>
</tr>
<tr>
<td>Coastal Flood Warning</td>
<td>Land areas along the coast are expected to become, or have become, inundated by seawater above the typical tide action.</td>
</tr>
<tr>
<td>Tropical Storm Watch</td>
<td>Tropical storm conditions with sustained wind from 39 to 73 mph are possible in your area within the next 36 hours.</td>
</tr>
<tr>
<td>Tropical Storm Warning</td>
<td>Tropical storm conditions are expected in your area within the next 24 hours.</td>
</tr>
<tr>
<td>Hurricane Watch</td>
<td>Hurricane conditions (sustained winds greater than 73 mph) are possible in your area within 36 hours. Issued 24-36 hours in advance of landfall advising residents to be prepared to evacuate.</td>
</tr>
<tr>
<td>Hurricane Warning</td>
<td>Hurricane conditions are expected in your area in 24 hours or less. Issued 12-24 hours in advance of landfall advising residents to evacuate inland to areas of safe shelter.</td>
</tr>
</tbody>
</table>
HURRICANE ALERT LEVELS are keyed to the forecasted time of arrival of a perceived threat.

**Alert Level I:** Hurricane has crossed geographical coordinates for longitude 75 degrees West, latitude 20 degrees North; or, the National Weather Service (NWS) forecasts development of a hurricane in the Gulf of Mexico with 72 hours.

**Alert Level II:** The NWS 72-hour forecast places the UNO Campus in a hurricane watch or warning area with a probability of 5% or more.

**Alert Level III:** The NWS 48-hour forecast places the UNO Campus in a hurricane watch or warning area with a probability of 10% or more; or the local authorities have issued an evacuation warning.

**Alert Level IV:** The NWS 24-hour forecast places the UNO Campus in a hurricane warning or strike area; or the NWS 36-hour forecasts hurricane landfall that includes the New Orleans area at a probability of 20% or more; or local authorities have issued an evacuation warning.

HURRICANE EMERGENCY PROCEDURES

In the event of a pending hurricane, UCC’s first concern is the safety of its personnel. A secondary, but critical concern is to the Computer Facility and data integrity. Below are the procedures to follow in order to protect personnel, the Computer Facility and data integrity. These procedures are to be used only as a guide. Due to unpredictability of tropical storms and hurricanes, no set of rigid procedures and time frames can be established to cover every condition. The UCC Management will notify the emergency team and other UCC Personnel what alert level currently exists and what actions to perform when a tropical storm or hurricane condition exists.

Although hurricane season starts June 1, the following actions should be performed each May:

**ACTION:**
1. Review Hurricane Emergency Procedures
2. Update employee phone and address listings
3. Test flashlight batteries
4. Ensure plastic covering is available for equipment
5. Test emergency lighting
6. Ensure sufficient tapes are available for Emergency Backups
7. Ensure PM schedule on UPS and Emergency generator is current

Note: The actions outlined for the month of May are in addition to the formal testing performed on a continuous basis and documented in Appendices G and H. As such, the May procedures will be performed only when time and man power permits and may not be supported by additional documentation.
EVACUATION PROCEDURES
Once a decision is made to evacuate the campus, UCC will begin planning the orderly shut down of the Computer Center.

ALERT LEVELS
UCC Management will direct all actions during the Alert Levels. UCC Management will notify the emergency team as to what Alert Level exists and what actions to take.

ALERT LEVEL I: As established by UNO Emergency Operations and approved by UCC Management:

ACTION:
1. Issue warning to system users that a hurricane threat exists and the possibility of suspension of operations exists
2. Ensure all employees have current on-call phone numbers
3. Notify all off duty employees of condition
4. Notify UNO Administration of condition
5. Make arrangements for payroll and other related matters contained in the university’s business continuity plan
6. Review Hurricane Emergency Procedures
7. Test flashlight batteries
8. Ensure plastic covering is available for equipment
9. Notify system users to back up critical information on Personal Computers
10. Ensure sufficient tapes are available for Emergency Backups
11. Perform full backup on the WINDOWS Systems (NetVault)

ALERT LEVEL II: As established by UNO Emergency Operations and approved by UCC Management:

ACTION:
1. Issue warning to system users that a hurricane threat exists and the possibility of suspension of operations exists
2. Begin preparations for securing the UCC computer center and redirecting computing functions to the Frey Computer Center at LSUBR
3. Begin relocation of items and materials subject to water damage away from windows and floor to the extent possible
4. Prepare current weekly incrementals and full backup tapes for transfer to off-site storage
5. Contact off-site storage contractor and schedule pick up time for tapes based on estimated completion of backups

ALERT LEVEL III: As established by UNO Emergency Operations and approved by UCC Management:
ACTION:
1. Issue warning to system users that a hurricane threat exists and that a suspension of operations and change of location of services will occur
2. Begin incremental backups:
3. Box completed incrementals with previous day’s incrementals and previous week full backup, and give to courier for delivery to remote storage facility
4. Switch on-campus functions to the “fail-over” system at the Frey Computer Center
5. Complete orderly shutdown of entire system and power off all equipment.
6. Cover all equipment with protective plastic covering
7. Secure all facilities and evacuate the premises

ALERT LEVEL IV: As established by UNO Emergency Operations and approved by UCC Management:

ACTION:
1. Evacuate area if needed

E. TORNADOES
The National Weather Service issues a tornado *watch* when conditions that may produce tornadoes are present or developing. A tornado *warning* is issued when a tornado has been detected or sighted. The warning will tell the location and movement of the tornado. If the facility is in the path of the storm, implement the safety plan immediately.

Continue normal activities but be ready to implement a safety plan if a tornado *warning* is issued.

If a tornado *WARNING* is issued, UCC staff should take the following action:

ACTION:
1. Take shelter *immediately*.
2. Stay inside buildings and off campus grounds.
3. Go to the interior of the building on lower floors.
4. Take cover under a sturdy object.
5. Protect your head, neck and face.
6. Stay away from windows, exterior walls and doors, and items that might fail.

F. WATER THREAT
The Computer Research Center’s computer room has a sunken floor. Any water entering the building either from outside or the second floor will seek the lowest point in the building. Electrical and data cables run under the raised floor providing electrical power to the computer hardware and communication connections. Water detection devices located under the raised floor will sound an alarm when one quarter of an inch of water is detected.
If water is observed entering the computer room or if the water detection alarm sounds, UCC staff should take the following action:

**ACTION:**
1. ASSESS the threat by determining how much water is entering the computer room, where the water is coming from, how much water has accumulated on the computer sub floor and which device(s) is/are being affected.
2. If time permits, perform a “system shutdown”, then a “system powerdown”. Otherwise, SAFELY power down and cover the devices with plastic sheeting. If it is unclear if a possible electrical hazard exists, do not hesitate to use the next higher breaker in the circuit.
3. SAFETY NOTE: Water conducts electricity! Do NOT attempt to power off any device that is wet. Select the next higher breaker in the circuit.
4. Alert the Emergency Response Team, see Appendix A.
5. Continue shutdown and powerdown procedures for equipment likely to be affected next.
6. The Emergency Response Team will determine if “fail-over” is necessary and, if necessary, begin the changeover.
7. The Emergency Response Team will work in conjunction with Facility Services to determine the source of the water damage, stop the intrusion of water into the computer center, drain any standing water in the computer room floor and “dry” or replace any hardware affected by the water.
8. Once given the “all clear” by university administrators, UCC Personnel will begin power up and start up procedures.

G. PANDEMIC

In the event a pandemic impacts the ability of computer personnel to work on site at the UNO Computer Center, the emergency team can work from any remote location by using the following components and infrastructure.

1. All servers at the main computer center and our remote site are configured with ILO (Integrated Lights Out). These components allow for complete control of the server from a remote location. Servers can be turned off or on without physical access to the server.
2. A VPN (Virtual Private Network) has been established to allow communications to servers and other resources within the UNO domain without actually being physically on campus connected to the domain.

If the university encounters a pandemic threat, UCC staff should take the following actions:

**ACTION:**
1. Evacuate infected area and begin working remotely.
IV. APPENDICES LISTING

A. Emergency Response Team
B. Mission Critical Systems Annual Approval of Plan by Associate VP / CIO
C. Individual Record of Receipt of Contingency Plan by Emergency Team
D. Record of Changes to Plan
E. Record of Training
F. Record of Testing Contingency Plan
G. Record of Testing Procedures for Restoration from Backup
H. Backup Procedures and Rotation

Appendix A
Emergency Response Team

<table>
<thead>
<tr>
<th>System Administrators:</th>
<th>Name</th>
<th>UNO</th>
<th>Cell</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Directory</td>
<td>Pierre Minnis</td>
<td>3-5513</td>
<td>504-473-7693</td>
</tr>
<tr>
<td></td>
<td>PeopleSoft System</td>
<td>Pierre Minnis</td>
<td>3-5513</td>
<td>504-473-7693</td>
</tr>
<tr>
<td></td>
<td>File Server / SharePoint</td>
<td>Ken D’Aquin</td>
<td>3-7068</td>
<td>504-621-9663</td>
</tr>
<tr>
<td></td>
<td>Backup / Restore</td>
<td>Billy Martinez</td>
<td>3-1198</td>
<td>504-495-1238</td>
</tr>
<tr>
<td></td>
<td>Web</td>
<td>Billy Martinez</td>
<td>3-1198</td>
<td>501-495-1238</td>
</tr>
<tr>
<td></td>
<td>Exchange (email)</td>
<td>Billy Martinez</td>
<td>3-1198</td>
<td>501-495-1238</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Administrators:</td>
<td>Senior Engineer</td>
<td>Phil Stott</td>
<td>3-5661</td>
<td>504-236-8466</td>
</tr>
<tr>
<td></td>
<td>Network Engineer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Administrators:</td>
<td>Senior DBA</td>
<td>Bill Sicard</td>
<td>3-1306</td>
<td>985-774-4116</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact Information for Backup Tapes:

Jim Teske, President
RecordMax USA, LLC
Cell (205) 422-4675
RecordMax Baton Rouge (225) 334-8163
RecordMax New Orleans (504) 363-4110
RecordMax Mobile (251) 433-3067
RecordMax Chattanooga (423) 643-3561
www.recordmax.com
Appendix B

The following are identified as mission critical functions:

- DNS (Domain Name Server)
- Domain controllers (Active Directory)
- Web (UNO Home Page)
- Email (MS Exchange for faculty/staff and students)
- PeopleSoft Learning Solutions (HR/Payroll/Student Administration)
- PeopleSoft Financials (General Ledger, Purchasing, Payables)
- SharePoint
- Enterprise Backup and Restore
- VOIP (Phone)

During an evacuation, once the UNO network has been shutdown, the Emergency Response Team will remotely test the function of all mission critical systems to verify they are still functioning.
Appendix C

Annual Approval of Contingency Plan by Associate VP / CIO for Computing and Communications

A record of updates and approvals to this document can be found in SharePoint.
Appendix D

Individual Record of Receipt of Contingency Plan

Receipt of this contingency plan by the UCC Emergency Response Team can be verified by reviewing the attendance log files in the Blackboard Learning Management System.
Appendix E

Record of Changes to Plan

UCC uses SharePoint to store the Contingency Plan. The plan must be “check-out” before changes can be made. Once a change is made the Plan must be “checked-in”. All changes resulting from “checking-out” or “checking-in” a document will be recorded within this system. It will also keep track of all versions of the Plan. By viewing the Plan in SharePoint it is possible to see individuals responsible for making changes and checking the Plan back into the system.
Appendix F

Record of Training.

All Emergency Team members with responsibilities under this plan must be trained annually, and at each change in the plan that affects their responsibility. Every person involved in the plan must be accounted for. A training module has been created in Blackboard, UNO’s learning management system. To verify that an individual has completed the module we require that a short quiz be completed. Therefore within Blackboard we have a record of all individuals and the date they completed the training.
Appendix G

Record of Testing Contingency Plan

The plan must be exercised on an annual basis. This may be done one portion at a time. Maintain records of each test.

<table>
<thead>
<tr>
<th>Section Tested</th>
<th>Result (Sat/Unsat)*</th>
<th>MANAGER</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Satisfactory</td>
<td>Pierre Minnis</td>
<td>1-22-2007</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Satisfactory</td>
<td>Bill Sicard</td>
<td>1-10-2007</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Satisfactory</td>
<td>Ken Daquin</td>
<td>8-30-2007</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>5-24-2008</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>5-24-2009</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>6-10-2010</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>7-13-2011</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>6-08-2012</td>
</tr>
<tr>
<td>All Systems</td>
<td>Satisfactory</td>
<td>Juan Henriquez</td>
<td>7-19-2013</td>
</tr>
</tbody>
</table>

* If unsatisfactory, prepare an evaluation of the test, include recommended changes or training, and document the implementation of these recommendations.
Appendix H

Record of Testing Procedures for Restoration from Backup

Satisfactorily test each procedure at least once annually, including retrieval from offsite storage. A test should also be done whenever the procedure is changed, or a procedure is newly implemented. Offsite retrieval need only be tested once for each separate location.

<table>
<thead>
<tr>
<th>Procedure Tested</th>
<th>Result (Sat/Unsat)</th>
<th>MANAGER</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeopleSoft</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>4-13-2007</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>4-16-2008</td>
</tr>
<tr>
<td>PeopleSoft</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>5-15-2009</td>
</tr>
<tr>
<td>File Server</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>6-10-2010</td>
</tr>
<tr>
<td>File Server</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>7-13-2011</td>
</tr>
<tr>
<td>File Server</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>6-08-2012</td>
</tr>
<tr>
<td>File Server</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>7-19-2013</td>
</tr>
<tr>
<td>File Server</td>
<td>Satisfactory</td>
<td>Billy Martinez</td>
<td>6-4-2014</td>
</tr>
</tbody>
</table>
Appendix I
Backup Procedures and Rotation

Weekly/Monthly/Yearly full backups are done once a week on Fridays and Saturdays.

Yearly backups are done on the first Friday/Saturday of the new calendar year.
Monthly backups are done on the first Friday/Saturday of each month excluding when yearly backups run.

Weekly backups are done on the remaining Friday/Saturdays.

Daily incremental backups are done 5 times a week from Sunday to Friday morning.

Yearly backups tape sets are retained indefinitely including the corresponding daily incremental tape sets.

Monthly backups tape sets are retained for 52 weeks including the corresponding daily incremental tape sets.

Weekly backups tape sets are retained for 8 weeks including the corresponding daily incremental tape sets.

To do a full system backup at current data levels and with 10 working tape drives it takes a minimum 30 hours provided all the jobs go as planned.

Backup tape sets remain offsite for a minimum of 6 weeks, they are sent offsite every Friday after the daily incremental backups are complete for the week.