



# SUNY Potsdam Information Systems Disaster Recovery Planning

Ali Shahidi  
Director  
Computing and Technology Services  
SUNY Potsdam

## DRP Scope

- Business Continuity Planning is an arrangement agreed upon in advance by College management and key personnel of the steps that will be taken to help the organization recover should any type of disaster occur.
- Disaster Recovery Planning is the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume critical business functions after the event of a disaster.
- Disaster is any event, which causes prolonged outage to the Campus Data Center, which forces relocation of IT operations and its people to an alternative work sites (earthquakes, power outages, floods, or fires).

## Preventive Strategy – Data

- Disk protection via RAID
- Data stored on Storage Area Network (SAN)
- Storage shelves located in the data center and a remote on-campus location
- Replication of data to remote on-campus on a daily basis
- Data backup to tape on a daily basis
- Critical data copied off-site to a data center in Syracuse
- Syracuse Data Center: NYSERNet, server, network switch, and storage shelf, redundant path over I1 and I2, backup Web server to inform users during emergencies



## Preventive Strategy – Infrastructure

- Spare inventory of switches, drives, storage shelf, servers (not stored in the data center)
- Uninterruptible Power Supply with backup generator
- Backup AC
- WAN I1 and I2 circuits
- Virtual servers
- Blade servers plus spare
- Server Clustering (Database and Email)

# DRP Table of Contents

## Disaster Recovery Overview and Scope

- Definition of Disaster

- Command Teams (Network, System, Telcom, Application, User Services)

- Command Center (Power, Phone, Network)

- Coordination with Campus Emergency Response Team

## Disaster Recovery Process

- Notification (Detection, Physical Plant, UP)

- Evaluation (Assessment)

- Activation (Authorization, Notification, Mobilization)

- Recovery (Recovery service level)

- Return to Normal (Reconstruction, Restoration)

## Campus Information

- Maximum Acceptable Downtimes (MAD)

- Data Loss Tolerance and Recovery Point Objectives (RPO)

- Alternative Data Center location (Cold and Hot sites)

- Work Area Recovery (Office space for recovery team)

- Passwords

- Keys/Card Access

- DRP book ( electronic copy on Flash Drive )



## DRP Table of Contents – continued

### System Recovery

- Minimum hardware required
- Spare hardware inventory
- Data backup and media

- Alternative DC site (Power, AC, Security)
- Network (LAN, WAN, DNS, LDAP)
- Data Storage (SAN)
- Critical systems recovery (Start-up / Shutdown

### Order)

- System Runbooks in the CTS Wiki  
(Runbook contains information on Server hardware,  
OS and Application configuration, and other  
technical  
detail required to recreate the environment)



## DRP Table of Contents – continued

### Test and Training

- Paper/Exercise walk through, Dry run
- Operations/Wet test, Recovery of mission critical systems
- Annual test

### Maintenance

- Annual review and update
- Print and distribute copies
- Update electronic copy on a Flash Drive

### Appendices

- Network diagrams
- Sample forms (damage assessment, ...)
- System Classification Definition
- Data Classification Definition
- System and Data Classification Table
- Contact Information
- Physical Plant / CTS Emergency Call List





## System Classification Definition

Tier 1: The loss of information and activities within this classification would adversely affect **critical campus wide operations**.

Tier 2: The loss of information and activities within this classification impacts the productivity of selected **groups/departments** and/or **important campus operations**.

Tier 3: The loss of information and activities within this classification impacts **individuals, smaller groups**, and/or **non-critical campus operations**.

## System Classification Definition

System Classification	Tier 1	Tier 2	Tier 3
<b>Criteria</b>	The loss of information and activities within this classification would adversely affect <b>critical campus wide operations</b> .	The loss of information and activities within this classification impacts the productivity of selected <b>groups/departments</b> and/or <b>important campus operations</b> .	The loss of information and activities within this classification impacts <b>individuals, smaller groups, and/or non-critical campus operations</b> .
<b>Response Time during business hours (8:00-16:30)</b>	1 hr	2 hrs	4 hrs
<b>Response Time after hours</b>	2 hrs	M-F until midnight: 2 hrs Else: next business day	Best Effort
<b>Recovery Time</b>	NA	NA	NA
<b>Uptime / Availability (minimum)</b>	Default value: 99.97% Equates to: 5 minutes of outage time per week	Default value: 99.8% Equates to: 20 minutes of outage time per week	Default value: 99.5% Equates to: 50 minutes of outage time per week

Response and Recovery time applies to normal business hours, After hour metrics are based on best effort. The metrics timing starts when problem is first reported by users or when CTS staff is informed via the monitoring system.

Recover systems based on these priorities:

1. Protect life safety
2. Secure critical Infrastructure
3. Resume teaching



## Data Classification Definition

**Institutional:** Institutional data needed for critical campus operations. Must be restored in the case of a disaster. A loss of data could result in legal ramifications, economic loss, and reputation loss for the university.

**User:** User data considered important to campus operations. Data may be reconstructed from alternative sources. A loss of data could result in user inconvenience, loss of productivity, and minimal reputation loss for the university.

**Communication:** User communication data used in normal day to day university operations. Data may be reconstructed from alternative sources. A loss of data could result in user inconvenience and loss of productivity for the university.

**Service:** OS and App related system files. Data may be reconstructed in the event of loss. A loss of data could result in lost productivity and inconvenience for the IT staff, and potential delay in service recovery.

# Data Classification Definition

<b>Classification</b>	<b>INST</b>	<b>USER</b>	<b>COMM</b>	<b>SRVC</b>
<b>Criteria</b>	Institutional data needed for critical campus operations. Must be restored in the case of a disaster. A loss of data could result in legal ramifications, economic loss, and reputation loss for the university.	User data considered important to campus operations. Data may be reconstructed from alternative sources. A loss of data could result in user inconvenience, loss of productivity, and minimal reputation loss for the university.	User communication data used in normal day to day university operations. Data may be reconstructed from alternative sources. A loss of data could result in user inconvenience and loss of productivity for the university.	OS and App related system files. Data may be reconstructed in the event of loss. A loss of data could result in lost productivity and inconvenience for the IT staff, and potential delay in service recovery.
<b>Examples</b>	Banner, Blackboard	Home and Department shares	email, voicemail	control files, logs, config files, scripts, images, reports
<b>Backup Media and location</b>	T, L, R, O			L, R, O
<b>Backup Schedule / Frequency</b>	T-GFS, L/R/O-Nightly Full			L- Nightly Full, R-Nightly Diff, O-Weekly Diff
<b>Retention period</b>	T-3 Months, L/R/O-10 days			1 Month
<b>Recovery Test Period</b>	Recover files monthly, Full restore test bi-annually			Recover files monthly, Full restore test bi-annually

Media/Location Codes:

- L Local on server or Data Center SAN storage
- R Remote SAN storage on campus
- T Tape (no off site storage, tapes remain in the library)
- O Off-site (Syracuse)
- GFS 4 Mon-Thu Daily incremental (Son), 5 Fri Weekly full (Father), 3 Monthly (Grand father)

## System and Data Classification Table

System Function	System Classification (Tier)	Data Classification	System Owner	System Owner Backup
Oracle Database(s)	1	INST,SVRC		
DNS/DHCP	1	INST,SVRC		
Email	1	COMM, SVRC		
LAN Core and Routing	1	SVRC		
Phone Service, PBX	1	SVRC		
Web Server	1	INST,SVRC		
Storage Area Network	1	SVRC		
User Storage, Helios	2	USER,SVRC		
Calendering software	2	INST,SVRC		
Voicemail	2	COMM,SVRC		
Network Management SW	3	SVRC		
Remote Access VPN	3	SVRC		

## Contact Information

CTS Name	Role	Email	Phone	Mobile	Home
Andy	Ass. VP	andy			
Ali	Director	shahidae			
Matt K.	Network Security	kellermg			
Jeff	HNS	hardyjm			
Greg	HNS	kuchytgi			
Vendors	Function/System	Email / Web Site	Phone	Contract #	Customer ID #
PAETEC	local and long distance service	see "PAETEC NOC esc list" in the contact folder			
Avaya	Definity G3R PBX PPN/EPN	see "Telcom Vendor contacts" in the contact folder			
HP	Servers	<a href="mailto:john.doe@hp.com">john.doe@hp.com</a>			
NYSERnet	NYSERnet WAN				
Nortel Telecom	Networking Gear				
SUNY ITEC	Oracle DB	<a href="http://itec.suny.edu/info/">http://itec.suny.edu/info/</a>			
CORAID	SAN Storage	support@coraid.com			

# Physical Plant / CTS Emergency Call List

Incident Type	When	Impacting	Contact 1	If no answer, leave msg and call Contact 2	If no answer, leave msg and call Contact 3
<b>Power Outages</b>	Lasting more than 5 minutes and still unresolved	Campus wide, multiple buidlings, Data Center, or remote NOC	CTS on Call	Director	CIO
<b>Environmental Alarms (humidity / temperature)</b>	Greater than 5 minutes and still unresolved	Campus wide, multiple buidlings, Data Center, or remote NOC	CTS on Call	Director	CIO
<b>AC Failures</b>	Always	Campus wide, multiple buidlings, Data Center, or remote NOC	CTS on Call	Director	CIO
<b>Flood</b>	Always	Campus wide, multiple buidlings, Data Center, or remote NOC	CTS on Call	Director	CIO
<b>Fire</b>	Always	Campus wide, multiple buidlings, Data Center, or remote NOC	CTS on Call	Director	CIO
<b>Telephone Outage</b>	Always	Campus wide	Telcom Manager	CIO	Director

<b>KEY</b>	<b>Name/Note</b>	<b>Primary #</b>	<b>Secondary #</b>
CTS on Call	Rotating Schedule		
Director			
CIO			
Telcom Manager			