
Department:	UW Medicine Information Technology Services
Policy Number:	SEC-07.02 – Server Disaster Recovery/Business Continuity Standard
Effective Date:	June 11 th , 2007
Review Date:	April 27 th , 2007

Purpose:

The purpose of this document is to define the required content for creating a Disaster Recovery/Business Continuity plan.

Definitions:

- See SEC-REF UW Medicine Information Security Program Glossary of Terms.

Standard

It is the responsibility of the System Owner to perform appropriate Disaster Recovery/Business Continuity planning as outlined within this standard.

I. Business Continuity Plan

In the Business Continuity Plan the System Owner needs to plan how to continue in business and perform all tasks required to do so while the computer hardware, network and data are being recovered.

Business Continuity plans must document the following procedures:

1. How to keep records while the systems are down and how the data would be updated once the system is recovered.
2. How to communicate with other systems that the system receives data from and sends data to during and after an outage.
3. How to synchronize the data created during an outage with other systems after an outage.
4. How to test the plan.
5. How to maintain the plan.
6. How to audit the plan.

II. Documentation of the Disaster Recovery Plan

In the Disaster Recovery Plan the System Owner needs to plan how to recover to the recovery goal from a disaster. This includes all computer hardware, data, data storage and network connections.

1. The System Owner needs to document the order in which systems would be recovered. What level of functionality would they recover each system to, and in which order? Not all systems may need to be recovered simultaneously or to 100% for the system to begin functioning. The System Owner needs to consider this when planning the system recovery.

2. The System Owner needs to document the resources (staff, hardware, software, vendors, backups) they would use and where these resources are located.
3. The System Owner needs to document who would manage the disaster recovery process and what the communication plan would be with vendors, support staff, and others.

III. Recovery Goal

The System Owner needs to document a recovery goal. This goal is a function of the criticality of the system to the institution. In case of a major outage to numerous systems, recovery resources will be limited. The System Owner needs to define a minimum recovery level by:

1. Defining the recovery goal within the context of the size of the outage, available resources, and the importance of the system to the institution.
2. Defining the consequences to the institution of not meeting the recovery goal.

UW Medicine IT Services: _____ Date: _____
James S. Fine, M.D., CIO, ISO

Disaster Recovery and Business Continuity Template

This sample template is designed to assist the system owner in performing a Disaster Recovery and Business Continuity procedure for an IT system. The template is not a plan, but exists to assist the System Owner in documenting the procedure for creating a business continuity plan and disaster recovery procedure.

Administration	
Your name	Supervisor's name
Your phone/page	Supervisor's phone/page
Your email	Department
Who is responsible for system recovery in case of a disaster	Who would you notify in case of a disaster
What is the specific contact information for that person	What is the specific contact information for that person
Server Identification	
Server Name	Server Location (Bldg)
Primary IP	Server Location (Room, rack, U)
Secondary IP's	Sales Vendor
Mfg	Repair Vendor
Model	Repair Vendor contact info
Purchase Date	Virtual Server Identification
Warranty Expiration date	Virtual server physical location
OS and Patch/SP level	Spare parts inventory and location
Serial Number	Inventory tag
Server Insured by	
Technical Support	
Primary Support Person	Primary support group
Primary Support Phone/page	Support group Manager
Primary Support Email	Support Group Manager phone/page
Server Backup and Restore	
Scheduled Downtime	Support Level (1 is critical, 4 is "as time permits")
Backup Media	Backup device
Full Backup frequency	Backup storage location
Incremental backup frequency	Offsite storage location
Backup verification frequency	Offsite vendor phone
Disk Image location	Offsite vendor contract ID
How often disk image is updated	Data retention length
Server replica location	Server replica technology
Who is affected, and how, if this server crashes?	

System Information	
System Owner Name	System Owner Dept
System Owner Email	System Owner Phone/page
System Operator Name	System Operator Email
System Operator Phone/page	System Diagram location
Upstream systems	Downstream systems
Upstream applications	Downstream applications
Applications running on this server	What this server does
Does this server have PHI	Server monitoring process
Server Recovery procedures. Include or attach explicit and detailed recovery instructions.	Server Recovery procedures documentation location
Business Continuity procedures. Include or attach explicit and detailed continuity instructions.	Business Continuity procedures documentation location