Weill Cornell Medical College

Information Technology Disaster Recovery Policy

Policy Statement

This policy defines acceptable methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services at Weill Cornell Medical College.

Entities Affected By This Policy

The Weill Cornell Medical College and Graduate School of Medical Sciences

- **Responsible Executives:** WCMC Chief Information Officer
- **Responsible Department:** Information Technologies and Services (ITS)
- **Dates:** *Issued:* Interim, July, 1st 2010. *Final Issuance:*
- **Contact:** Information Technologies and Services

Reason for Policy

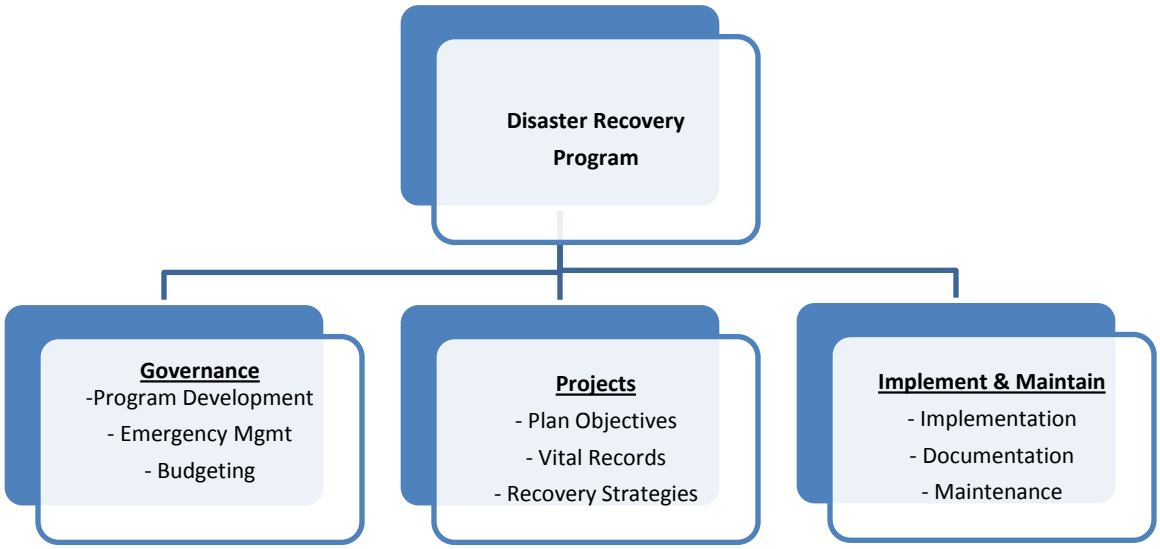
The disaster recovery standards in this policy provide a systematic approach for safeguarding the vital technology and data managed by the Information Technologies and Services Department. This policy provides a framework for the management, development, and implementation and maintenance of a disaster recovery program for the systems and services managed by ITS.

Document Conventions

To assist in the usage of this policy document, the Appendix Section below contains a summary of all the DR Timeline deliverables plus a DR glossary. Please check the DR glossary for the definition of DR terms.

Principles

Disaster Recovery planning is a program that has a continuous lifecycle. Detailed requirements for each of these steps are below. The high-level process for DR Lifecycle is as follows:



1. **Governance**

a. All ITS-managed systems must comply with WCMC disaster recovery policies and requirements.
b. The IT Disaster Recovery Manager is responsible for IT DR program coordination and project management: including reporting status of IT DR planning, testing, and auditing activity to ITS senior management on a regular basis; **at least twice per year**.
c. ITS senior management is responsible for ensuring sufficient financial, personnel and other resources are available as needed.
d. The DR Manager will review and update the DR Policy as necessary **at least every other year**. All modifications must be approved by ITS senior management.

2. **Program Development**

a. The ITS Disaster Recovery Program (DRP) addresses the protection and recovery of WCMC IT services so that critical operations and services are recovered in a timeframe that ensures the survivability of WCMC and is commensurate with customer obligations, business necessities, industry practices, and regulatory requirements.

b. Plans must be developed, tested, and maintained to support the 2.a objectives of the Program, and those plans should include relevant IT infrastructure, computer systems, network elements, and applications. At minimum, **annual updating** is required.
c. The Disaster Recovery Manager is responsible for conducting Business Impact Analyses (BIA) to identify the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each; **at least every other years.**
d. The Disaster Recovery Manager is responsible for conducting Capability Analyses (CA) to determine ITS's capacity to recover critical IT services that support defined critical business processes and recovery objectives; **at least every other years.**
e. The Disaster Recovery Manager is responsible for maintaining the Recovery Tier Chart , which defines the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of all ITS-managed systems. The Service managers are required to prioritize their IT processes and associated assets based upon the potential detrimental impacts to the defined critical business processes.
f. ITS is required to create disaster recovery plans for the IT portion – including services, systems, and assets – of critical business processes. These IT services, systems, and assets must be inventoried and correlated according to the technical service catalog , prioritized based upon results of the Business Impact Analysis, and ranked according to their Recovery Time Objectives and Recovery Point Objectives.
g. A Risk Assessment must be conducted **at least every other year** to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure.
h. For each risk or vulnerability identified in the Capability Review and Risk Assessment, a mitigation or preventive solution must be identified.
i. The IT DR program must include a change management and quality assurance process.
j. Above Program Development statements will be progressively fulfilled via Disaster Recovery Manager, Departmental and/or other resources.

3. Emergency Management

a. The IT Disaster Recovery Team/Manager is responsible for overseeing IT DR activities in the event of an emergency –i.e., an unplanned outage where RTO is in jeopardy.
b. The IT Disaster Recovery Manager should be part of the ITS representation within the institution's Emergency Management Team .
c. Each IT division must develop and maintain a documented emergency plan including notification procedures.
d. Each IT division shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the associates they supervise.
e. The IT Disaster Recovery Team/Manager is required to complete a post-mortem report documenting outages and recovery responses within **45 days** after the occurrence of a disaster recovery event.

4. Budgeting

a. IT DR budgeting must be informed **annually** by requirements gathered in the BIA and CA as well as the ITS budgeting process.
b. IT Managers are responsible for tracking and reporting on planned and unplanned outage spending related to the recovery and restoration effort. During an outage, IT Managers may incur special recovery and restoration costs that are unbudgeted. For a small outage, these costs would be immaterial; but for a longer outage, these costs could be significant.

5. Plan Objective

a. IT DR plans must provide information on Business Impact Analysis, Data Backup, Recovery, Business Resumption, Administration, Organization Responsibilities, Emergency Response & Operations, Training and Awareness and Testing.
b. Plans must contain Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).
c. Technological solutions for data availability, data protection, and application recovery must be considered by data gathered by the BIA and CA.

6. Vital Records

a. ITS must maintain a single, comprehensive electronic inventory of all servers, network equipment, relevant configuration, and model information, and the applications they support. This inventory should be aligned with the service catalog and the technical service catalog.
b. All Backup data must be labeled and logged, and are available for use during an emergency within stated recovery time objectives. A documented decision making process will be used to determine what subset of backup data will be additionally encrypted, and stored off-site in a secured location outside of the geographical area of the system they are backups of.
c. DR plans must be stored in a single, comprehensive database.
d. DR plans owners need to be able to access a copy of emergency and recovery plan(s) independent of ITS services and/or network.
e. Upon completion or update, DR plans must be sent to the Disaster Recovery Manager and ITS Change Manager for review.
f. Plan information must be reviewed and updated as warranted by business and/or information systems environment changes, **at least annually**.

7. Plan Attributes

a. Plans must address an outage that could potentially last for a period of up to six weeks.
b. Plans must identify risk exposure and either accept the risk or propose mitigation solution(s).
c. Backup strategies must comply with predefined businesses continuity requirements, including defined recovery time and point objectives. Backup strategies must be reviewed **at least every other year.**
d. Recovery strategies must meet recovery objectives defined in the DR tier chart.
e. Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives.

f. Recovery strategies must be implemented within a previously agreed upon period of time, generally **not more than 180 days** after management approval.
g. The ITS Disaster Recovery Manager is required to provide DR training and awareness activities **at least twice per year.**

8. Maintenance

a. Plans must contain current and accurate information.
b. Planning must be integrated into all phases of the IT system life cycle.
c. IT DR tests that demonstrate recoverability commensurate with documented IT DR plans must be conducted regularly; as well as when warranted by changes in the business and/or information systems environment.
d. Backup media supporting critical business processes must be tested **semi-annually**. Reviews are required within **60 days** after a test to correct exposed deficiencies.
e. Plan revisions must be completed **within 60 days** after a DR test is completed.
f. The following maintenance activities must be conducted **annually**:
    i. Updating the documented DR plan
    ii. Reviewing the DR objectives and strategy
    iii. Updating the internal and external contacts lists
    iv. Conducting a simulation/desktop exercise
    v. Conducting a telecommunication exercise
    vi. Conducting an application recovery test
    vii. Verifying the alternate site technology
    viii. Verifying the hardware platform requirements
    ix. Submitting the DR Status and Recoverability Report
    x. IT managers are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

9. Appendix Section

a. DR Timeline Deliverables

Reference	Frequency	Activity
1. Governance	At least twice per year	Summary: Report on DR activity to ITS Senior Leadership Policy Reference: 1.b
	At least every other years	Summary: Review and update DR Policy as necessary. Policy Reference: 1.d
2. Program Development	At minimum, annual updating is required.	Summary: Update existing DR Plans Policy Reference: 2.b
	At least every other years	Summary: Conduct Business Impact Analysis Policy Reference: 2.c
	At least every other years	Summary: Conduct Capability Assessment Policy Reference: 2.d
	At least every other years	Summary: Conduct Risk Assessments Policy Reference: 2.g
3. Emergency Management	Within 45 days of the event	Summary: Complete post-mortem report after outage and recovery response Policy Reference: 3.e
4. Budgeting	Annually	Summary: Complete DR budget Policy Reference: 4.1
6. Vital Records	At least annually	Summary: Review and update published DR plans Policy Reference: 6.e
7. Plan Attributes	Reviewed annually	Summary: Review of backup strategies compliance Policy Reference: 7.c
	Generally not more than 180 days	Summary: Implement defined recovery strategies Policy Reference: 7.f

	Twice per year	Summary: Provide DR training and awareness activities Policy Reference: 7.g
8. Maintenance	Semi-annually	Backup media supporting critical business processes must be tested Policy Reference 8.d
	Within 60 days	Summary: Reviews are required after a test to correct exposed deficiencies Policy Reference: 8.d
	Within 60 days	Summary: Complete Plan revisions after the test review. Policy Reference: 8.e
	Annually	Summary: Conduct DR maintenance activities Policy Reference: 8f

b. Disaster Recovery Glossary

Business Impact Analysis (BIA) is the process that identifies critical business functions, set priorities and determines the impact on the organization if those functions are not performed for a specified period of time.

Capability Assessment (CA) is ITS assessment of our estimated recovery time of critical services.

Disaster Recovery Team is a temporary team assembled during an Emergency Management situation/outage. This team is led by the team leader / incident coordinator.

Emergency Management Team (EMT) is WCMC cross-functional response team that manages potential/actual large-scale outages. A published Emergency Management Plan governs the activities of this team.

Recovery Time Objective (RTO) represents the maximum amount of time an institution can tolerate the loss of an application or, conversely, how quickly an application must be restored to working order in the event of a disaster.

Recovery Point Objective (RPO) represents the maximum amount of data loss an institution can tolerate for a given application in the event of a disaster.

Recovery Tier Chart ranks IT services by business-defined recovery requirement during the Business Impact Analysis process (see below for WCMC Recovery Tier Chart:

Tier	*Criticality*	*RTO*	*RPO*	*Type of DR HW*	*Replicate Or Tape?*	*DR Plan*	*Config*
0	Self-Healing	Immediate	PoF	Dedicated	Replicate	Yes	Hot/Hot
1	Mission Critical	< 24 hrs	PoF or Intra-Day	Dedicated	Replicate	Yes	Hot/Warm
2	Highly Critical	< 72 hrs	Intra-Day or SoD	Dedicated	Replicate or Tape	Yes	Hot/Cold
3	Critical	< 7 days	SoD	QuickShip	Tape	Yes	N/A
4	Non-Critical	< 2 Weeks	LC	Determined ATOD	Tape	Yes	N/A
5	Deferrable	> 2 weeks	LC	Determined ATOD	Tape	No	N/A

Risk Assessment (RA) is the initial steps of Risk Management which analyzes the value of the IT assets to the business, identifying threats to those IT assets, and evaluating how vulnerable each IT asset is to those threats.

Service Manager is the owner of a service as defined by one of the user or technical catalogs.

`Technical Service Catalog` maps technical activities of the User Services Catalog to select ITS systems and applications. This mapping helps understanding of how changes in these services impact the users.