IT Disaster Recovery

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: July 1, 2010
Last Updated: November 10, 2023
Last Reviewed: November 13, 2023

Contents
Policy Statement ....................................................................................................................................................................... 2
Reason for Policy...................................................................................................................................................................... 2
Entities Affected by this Policy .................................................................................................................................................. 2
Who Should Read this Policy ................................................................................................................................................... 2
Web Address of this Policy ....................................................................................................................................................... 2
Contacts .................................................................................................................................................................................... 2
1. Overview ............................................................................................................................................................................ 3
   1.01 Governance ............................................................................................................................................................. 3
   1.02 Program Development ............................................................................................................................................ 3
   1.03 Emergency Management ........................................................................................................................................ 3
   1.04 Budgeting ................................................................................................................................................................ 4
2. Implementation ................................................................................................................................................................... 4
   2.01 Plan Objective ......................................................................................................................................................... 4
   2.02 Storage .................................................................................................................................................................... 4
   2.03 Plan Attributes ......................................................................................................................................................... 4
3. Maintenance ....................................................................................................................................................................... 4
4. Additional Resources ......................................................................................................................................................... 5
   4.01 Services Tier Mapping Chart ................................................................................................................................ 5
   4.02 Hosting Model ......................................................................................................................................................... 6
   4.03 Shared Responsibility Representative Model ......................................................................................................... 6
   4.04 Capability Review and Risk Assessment for ITS and Non-ITS Supported Services .............................................. 7
Policy Statement
This policy is designed to support disaster recovery planning, preparedness, management, and mitigation of risks to the continuity of information technologies (IT) systems and services used for Weill Cornell Medicine purposes.

Reason for Policy
The disaster recovery standards in this policy provide a systematic approach for safeguarding the vital technology, services, and data managed by both the Information Technologies and Services (ITS) Department and individual departments. This policy also provides a framework for the management, development, implementation, and maintenance of a disaster recovery (DR) program for the systems and services managed by ITS that use Weill Cornell Medicine data.

Entities Affected by this Policy
All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy
All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources. All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy
https://its.weill.cornell.edu/policies/

Contacts
Direct any questions about this policy, 15.5 – IT Disaster Recovery, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu
1. Overview
The IT Disaster Recovery Program (“Program”) is a continuous lifecycle consisting of governance, implementation, and maintenance of the disaster recovery program and plan.

1.01 Governance
All Weill Cornell Medicine information systems and applications (“systems”) must comply with the institution’s disaster recovery policies and standards. The Program is responsible for coordination and project management including, but not limited to, reporting the status of planning, testing, and auditing activity to the IT Disaster Recovery Governance Committee at least twice per year.

The IT Disaster Recovery Governance Committee is responsible for ensuring adequate financial, personnel, and other resources are available to support the Program.

1.02 Program Development
The Program addresses the protection and recovery of Weill Cornell Medicine systems so that critical operations and business services are recovered in a timeframe that ensures the survivability of Weill Cornell Medicine commensurate with patient obligations, business necessities, industry practices, and regulatory requirements.

Disaster recovery plans must be developed, tested, and maintained to support the objectives of the Program, and the plans should include relevant personnel, IT infrastructure, computer systems, network elements, and applications.

At minimum, the Program and the encompassing plans must be updated in the event of a significant organizational change, following the use of the plans in response to a disruptive event, or otherwise reviewed annually.

The Program includes business impact analyses to identify business processes, determine recovery points and timeframes, and establish criticality ratings for each. The results and metrics are subject to modification by the IT Disaster Recovery Governance Committee. These analyses are required to be reviewed and updated, if necessary, during the annual review of the plan.

The Program also includes capability assessments to determine a department’s capacity to recover critical IT services that support defined critical business processes and recovery objectives in a systematic fashion at least annually.

The Program maintains a Recovery Tier Chart, which defines the recovery time objectives (RTO) and recovery point objectives (RPO) of all ITS-managed systems. Service Managers are required to prioritize their IT processes and associated assets based upon the potential detrimental impacts to the defined critical business processes.

Lastly, the Program creates disaster recovery plans for the IT portion—including services, systems, and assets—of critical business processes. These must be prioritized based upon results of the business impact analysis and ranked according to their Recovery Tier and related recovery time objectives and recovery point objectives. The Program must account for risk assessments to determine threats to disaster recovery and their likelihood of impacting IT infrastructure. For each risk or vulnerability identified in the risk assessment, a mitigation or preventive solution must be identified. The Program must include change management and quality assurance processes.

1.03 Emergency Management
The Program will oversee IT disaster recovery related activities in the event of a disruption, emergency or other unplanned outage where RTO is in jeopardy. The Program should provide input to the institution’s emergency management team as defined in the Weill Cornell Medicine Emergency Management Manual.

Each department must develop and maintain a documented emergency plan including notification procedures. The emergency plan shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the staff they supervise.
The Program requires that a post-mortem lessons learned report documenting outages and recovery responses be completed within 45 days after a disruption.

1.04  Budgeting
Budgeting for disaster recovery efforts must be informed annually by requirements gathered in the business impact analysis and capability assessment as well as the ITS budgeting process.

The Program will track and report on planned and unplanned outage spending related to any recovery and restoration efforts. During a disaster-level outage or incident, the Program may incur special recovery and restoration costs that are unbudgeted. For a small outage these costs would be expected to be immaterial, but for a longer outage, these costs could be significant.

2. Implementation

2.01  Plan Objective
Disaster Recovery plans must address the following areas: business impact analysis; data backup and recovery; business resumption; administration and organization responsibilities; emergency response and operations; training and awareness; testing; recovery time objectives; and recovery point objectives.

Technological solutions for data availability, data protection, and application/service recovery must be considered by data gathered by a business impact assessment and capability assessment.

2.02  Storage
The plans must be stored in a single, central, comprehensive repository that is accessible by plan owners and key stakeholders in the event of an emergency.

All backup data must be labeled, logged, and available for use during an emergency within stated recovery time and point objectives. A documented decision-making process will be used to determine what subset of backup data will be additionally encrypted and stored offsite in a secured location outside of the geographical area of the supported system.

2.03  Plan Attributes
The plans must consider outages that could potentially last up to six (6) weeks. They must identify risk exposure and dependencies and either accept the risk or propose mitigation solutions.

Backup strategies and recovery strategies should be designed to meet recovery time objectives and recovery point objectives in accordance with designated disaster recovery tiers. Tests should be designed to ensure recovery times and recovery points can be supported.

The Program will provide training and awareness activities on disaster recovery plans at least annually.

3. Maintenance
Several activities are required to maintain the plans. System owners must ensure that plans contain current and accurate information. New disaster recovery plans and revisions to existing plans should be integrated into all phases of the IT information system life cycle.

Tests that demonstrate recoverability commensurate with the documented plans must be conducted regularly and when warranted by changes in the business and/or information systems environment.

The ability to restore data from backup media should be tested semi-annually. Should these reviews identify deficiencies, corrective actions should be undertaken promptly.
The following maintenance activities are to be conducted annually by the system owner or system manager:

- Review of the plan objectives and strategy, including potential disaster scenarios
- Update of internal and external contact lists
- Recording of known dependencies
- Verification of hardware requirements
- Documentation in support of the completion of a recovery test or simulation/desktop exercise, including test details and a summary of results

System managers are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

4. Additional Resources

4.01 Services Tier Mapping Chart

<table>
<thead>
<tr>
<th>Tier</th>
<th>Time Period</th>
<th>Data Loss</th>
<th>Technical Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Immediate (Active/Active)</td>
<td>Generally synchronous (or semi-synchronous) data replication with no or minimal data loss (point of failure)</td>
<td>Redundant remote clustering or load balancing and synchronous replication; transparent or near transparent recovery</td>
</tr>
<tr>
<td>A</td>
<td>&lt; 3 hours (Active/Passive)</td>
<td>Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is accessible</td>
<td>Recovery within minutes or hours on hot/warm standby server; requires manual intervention to invoke combined with some form of data replication</td>
</tr>
<tr>
<td>1</td>
<td>&lt; 24 hours (Active/Passive)</td>
<td>Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable</td>
<td>Recovery within minutes or hours on hot/warm standby server; requires manual intervention to invoke combined with some form of data replication</td>
</tr>
<tr>
<td>2</td>
<td>&lt; 72 hours (Disk/Virtual Tape Restore)</td>
<td>Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable</td>
<td>May be coupled with hot site or mobile type solution to provide recovery within days; the volume of data required for recovery may push this into a mirroring requirement to meet recovery time objectives</td>
</tr>
<tr>
<td>3</td>
<td>&lt; 1 week (Disk/Virtual Tape Restore)</td>
<td>Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable</td>
<td>May be coupled with hot site or mobile type solution to provide recovery within 1 week</td>
</tr>
<tr>
<td>4</td>
<td>Deferrable</td>
<td>Generally, recovery from last captured backup and data loss is acceptable</td>
<td>May be recovered on an as-needed basis (i.e., a complete build solution)</td>
</tr>
</tbody>
</table>
4.02 Hosting Model

Cloud Provider

Service Orchestration
- Service Layer
  - SaaS
  - PaaS
  - IaaS
- Resource Abstraction and Control Layer
- Physical Resource Layer
  - Hardware
  - Facility

Cloud Service Management
- Business Support
- Provisioning/Configuration
- Portability/Interoperability

Security

Privacy

Cloud Carrier

Cloud Consumer

Cloud Auditor
- Security Audit
- Privacy Impact Audit
- Performance Audit

Cloud Broker
- Service Intermediation
- Service Aggregation
- Service Arbitrage

Note: ITS manages the security and privacy segments that transport, process, and/or store Weill Cornell Medicine data.

4.03 Shared Responsibility Representative Model

### 4.04 Capability Review and Risk Assessment for ITS and Non-ITS Supported Services

It is important to periodically vet all ITS and non-ITS service providers on their continuity practices so that risk to Weill Cornell Medicine data is minimized. This assessment questionnaire is designed to identify vulnerability areas derived from this policy. The completed assessment must be shared with the Program for final resolution.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Strategy</td>
<td>• What is your recovery strategy?</td>
</tr>
<tr>
<td></td>
<td>• Are these strategies documented in your contingency plan?</td>
</tr>
<tr>
<td>Program Policy</td>
<td>• What drives your continuity program—i.e., DR policy or procedure?</td>
</tr>
<tr>
<td>Testing and Audit</td>
<td>• What is your commitment to DR testing?</td>
</tr>
<tr>
<td></td>
<td>• Is the DR program audited?</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>• What are your data backup procedures and storage practices?</td>
</tr>
<tr>
<td>Notification and Escalation</td>
<td>• What is your notification and escalation documented protocol?</td>
</tr>
<tr>
<td></td>
<td>• Declaration process?</td>
</tr>
<tr>
<td></td>
<td>• Frequency of updates during a disaster?</td>
</tr>
<tr>
<td>Critical Functions Recovery Plans</td>
<td>• Do functional plans exists?</td>
</tr>
<tr>
<td>Teams and Roles &amp; Responsibilities</td>
<td>• What team structure supports your DR program?</td>
</tr>
<tr>
<td>Contact Information</td>
<td>• Does your DR plan identify contact information for key personnel, etc.?</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>• Did you perform a risk assessment?</td>
</tr>
<tr>
<td></td>
<td>• Frequency of assessment?</td>
</tr>
<tr>
<td></td>
<td>• Top risk concerns?</td>
</tr>
<tr>
<td>Supplier DR Program Information</td>
<td>• Which suppliers do you heavily depend on?</td>
</tr>
<tr>
<td></td>
<td>• Are you checking their DR program?</td>
</tr>
</tbody>
</table>
## Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 1, 2010</td>
<td></td>
<td>Initial policy issued</td>
</tr>
<tr>
<td>November 14, 2019</td>
<td>Larry Heck</td>
<td>Updated policy language to incorporate cloud service providers</td>
</tr>
<tr>
<td>November 10, 2023</td>
<td>J. M. Rosenbloom, B. Tschinkel, J. Barber</td>
<td>Added new service tier; generalized document to apply to any information system regardless of management; updated policy template and language for branding</td>
</tr>
</tbody>
</table>