	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	IT Disaster Recovery
	Policy Number	ITS-520.01
	Department/Office	ITS Security, Identity & Business Continuity
	Effective Date	July 1, 2010
	Last Reviewed	November 25, 2024
	Approved By	Information Security & Privacy Advisory Committee (ISPAC)
	Approval Date	November 25, 2024

Purpose

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 (WCM) data.

Scope

Applies to all members of the WCM community who utilize WCM information technology resources. This includes WCM-Qatar and those responsible for managing and safeguarding WCM data.

Policy

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 WCM purposes.

Procedure

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

The IT Disaster Recovery Program ("Program") is a continuous lifecycle consisting of governance, implementation, and maintenance of the disaster recovery program and plan.

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.

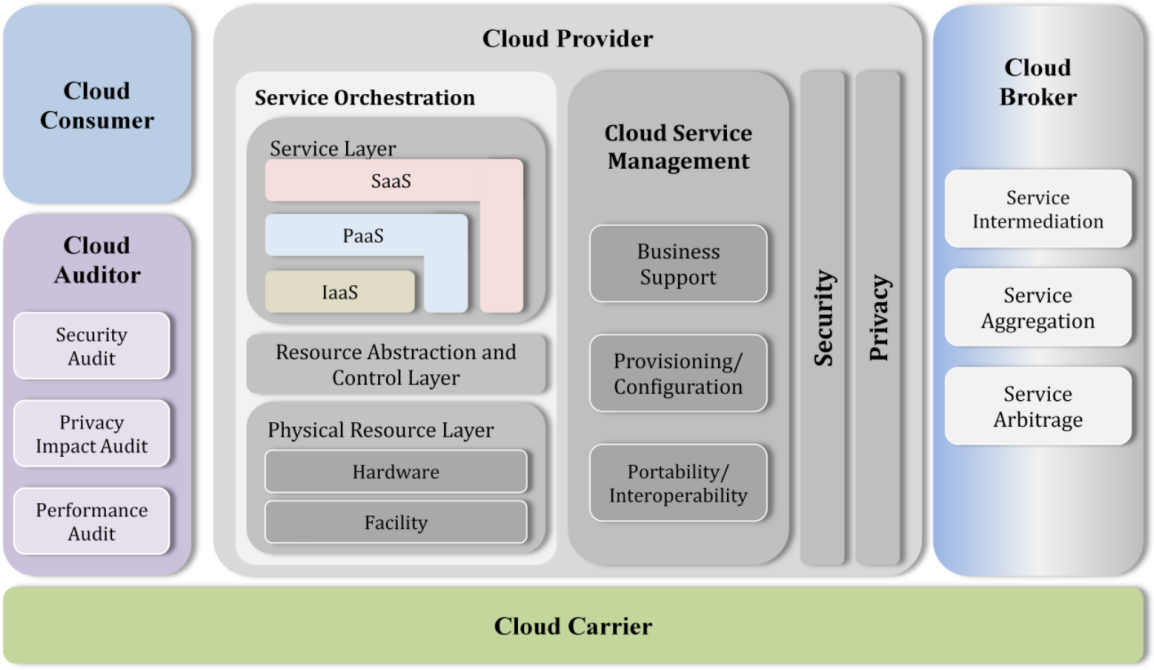
System managers are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

4. Additional Resources

4.01 Services Tier Mapping Chart

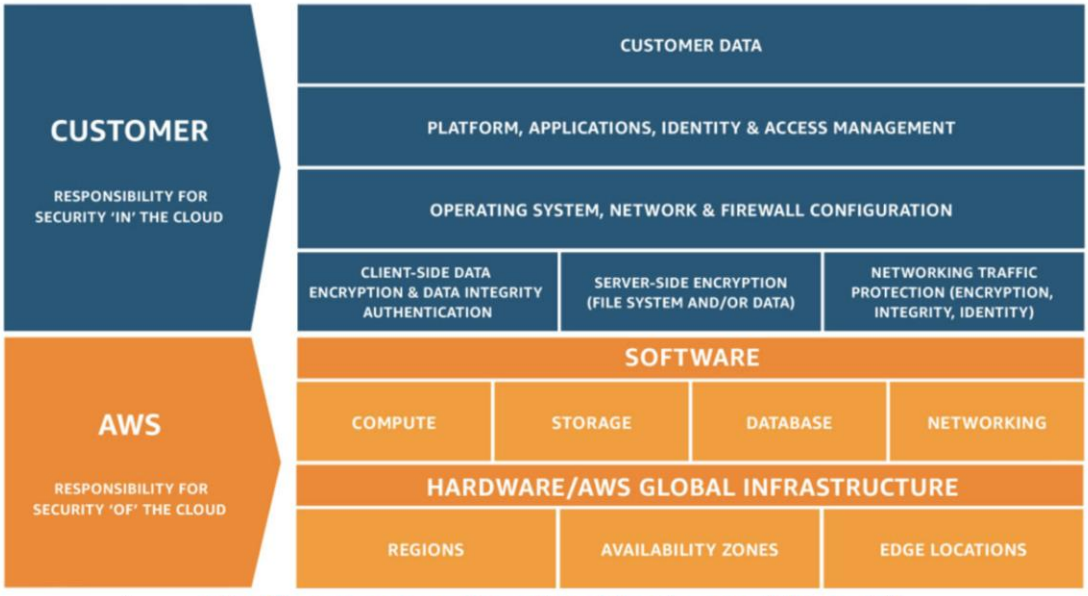
Tier	*Time Period*	*Data Loss*	*Technical Solution*
0	Immediate (Active/Active)	Generally synchronous (or semi-synchronous) data replication with no or minimal data loss (point of failure)	Redundant remote clustering or load balancing and synchronous replication; transparent or near transparent recovery
A	< 3 hours (Active/Passive)	Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is accessible	Recovery within minutes or hours on hot/warm standby server; requires manual intervention to invoke combined with some form of data replication
1	< 24 hours (Active/Passive)	Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable	Recovery within minutes or hours on hot/warm standby server; requires manual intervention to invoke combined with some form of data replication
2	< 72 hours (Disk/Virtual Tape Restore)	Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable	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
3	< 1 week (Disk/Virtual Tape Restore)	Generally asynchronous data replication/snapshot or some other periodic copy function, therefore some data loss is acceptable	May be coupled with hot site or mobile type solution to provide recovery within 1 week
4	Deferrable	Generally, recovery from last captured backup and data loss is acceptable	May be recovered on an as-needed basis (i.e., a complete build solution)

4.02 Hosting Model



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

4.03 Shared Responsibility Representative Model



Source: https://aws.amazon.com/compliance/shared-responsibility-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.

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

Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

Direct any questions about this policy, 520.01 – [IT Disaster Recovery], to the Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-3609
- Email: ciso@med.cornell.edu

Approval

This policy was reviewed and approved by the Information Security and Privacy Advisory Committee (ISPAC).

Version History

Date	Author	Revisions
July 1, 2010		Initial draft completed. Original date of issue.
November 14, 2019	Larry Heck	Updated policy language to incorporate cloud service providers
November 10, 2023	J. Mark Rosenbloom, Brian J. Tschinkel, Justin Barber	Added new service tier; generalized document to apply to any information system regardless of management; updated policy template and language for branding
November 22, 2024	J. Mark Rosenbloom, Thomas Horton	Updated policy template, language & contact information. Assigned new policy number, "ITS-520.01."