Weill Cornell
Medicine

15.5

IT Disaster Recovery Policy

Responsible Executive: Chief Information Officer, WCM
Original Issued: July 1, 2010
Last Updated: November 14, 2019

Policy Statement

This policy defines acceptable methods for disaster recovery planning, preparedness, management, and mitigation of IT systems and services of any information system on behalf of Weill Cornell Medicine.

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 (ITS) Department. This policy 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 WCM data by any entity.

Entities Affected by this Policy

The Weill Cornell Medical College and Graduate School of Medical Sciences

Who Should Read this Policy

All individuals responsible for configuring, maintaining, and monitoring information systems on the Weill Cornell Medicine. Individuals may include Weill Cornell Medicine faculty, staff, vendors, contractors, or managed service providers.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

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

• Office:	(646) 962-2768
• Email:	brt2008@med.cornell.edu

Contents

1. Definitions

These definitions apply to institutions and regulations as they are used in this policy.

• WCM	Weill Cornell Medicine
• ITS	Information Technologies & Services Department
• Business Continuity	the complementary process to DR which focuses on business processes and people aspects of recovery. These plans are stored in the Ready tool.
• Business Impact Analysis (BIA)	the process that identifies critical business functions, sets priorities, and determines the impact on the organization if those functions are not performed for a specified period
• Capability Assessment (CA)	an ITS assessment of our estimated recovery time of critical services
• Disaster Recovery (DR)	involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology systems following a disaster
• Emergency Management Team (EMT)	a WCM cross-functional response team that manages potential and/or actual large-scale outages; a published Incident Management Procedure governs the activities of this team
• Information System	any system or service that transport, processes, and/or stores WCM data
• 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
• Risk Assessment (RA)	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	the owner of a service as defined by one of the users

2. Overview

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 Governance

All ITS-managed systems must comply with WCM disaster recovery policies and requirements. 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 as deemed appropriate. The Program will review, update, and coordinate testing of the Policy *at least every other year*. All modifications must be approved by the IT Disaster Recovery Governance Committee and the Information Security and Privacy Advisory Committee (ISPAC).

2.02 Program Development

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

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

At minimum, the Program and Plan 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 the critical business processes, determine standard recovery timeframes, and establish the criticality ratings for each. The results and metrics must be agreed upon by the IT Disaster Recovery Governance Committee. These analyses are required to be updated *at least every other year*.

The Program also includes capability analyses (CA) to determine the department’s capacity to recover critical IT services that support defined critical business process and recovery objectives *at least every other year*.

The Program maintains 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.

Lastly, the Program creates disaster recovery plans for the IT portion—including services, systems and assets-- of critical business processes. These IT services, systems, and assets must be prioritized based upon results of the business impact analysis and ranked according to their Recovery Time Objectives and Recovery Point Objectives. The Program must account for risk assessments *at least every other year* to determine threats to disaster recovery and their likelihood of impacting the IT infrastructure. For each risk or vulnerability identified in the risk assessment, a mitigation or preventive solution must be identified. The Program must include a change management and quality assurance process.

2.03 Emergency Management

The Program will oversee IT disaster recovery-related activities in the event of an emergency (i.e., an unplanned outage where RTO is in jeopardy). The Program should provide input to the institution’s emergency management team.

Each institution’s IT division 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 associates they supervise.

The Program requires that a post-mortem report documenting outages and recovery responses be completed *within 45 days* after the occurrence of an event.

2.04 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 the recovery and restoration effort. During an outage, the Program 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.

3. Implementation

3.01 Plan Objective

The 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 point objectives (RPO); and, recovery time objectives (RTO).

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

3.02 Storage

The Plans must be stored in a single, central, comprehensive application 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 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.

3.03 Plan Attributes

The Plans must address an outage that could potentially last for a period of up to six (6) weeks. It must identify risk exposure and either accept the risk or propose mitigation solution(s).

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*. Recovery strategies must meet recovery objectives defined in accordance with disaster recovery tiers.

Approved recovery strategies must be tested to ensure they meet required recovery time and recovery point objectives. Recovery strategies must be implemented within a previously agreed upon period, generally *not more than 180 days* after management approval.

The Program will provide training and awareness activities on the Plan *at least twice per year.*

4. Maintenance

Several activities are required to maintain the Plans. Plan owners must ensure that plans contain current and accurate information. Revisions must be completed *within 60 days* after a test is completed. To ensure effectiveness, the Plans must be integrated into all phases of the IT 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.

Backup media supporting critical business processes must be tested *semi-annually*. Reviews are required *within 60 days* after a test to correct exposed deficiencies.

The following maintenance activities must be conducted *annually*:

- Updating the documented Plan
- Reviewing the Plan objectives and strategy
- Updating the internal and external contacts lists
- Conducting a simulation/desktop exercise
- Conducting an application recovery test
- Verifying the alternate site technology
- Verifying the hardware platform requirements
- Submitting a DR Status and Recoverability Report
- IT managers are responsible for briefing staff on their roles and responsibilities related to DR planning, including developing, updating, and testing plans.

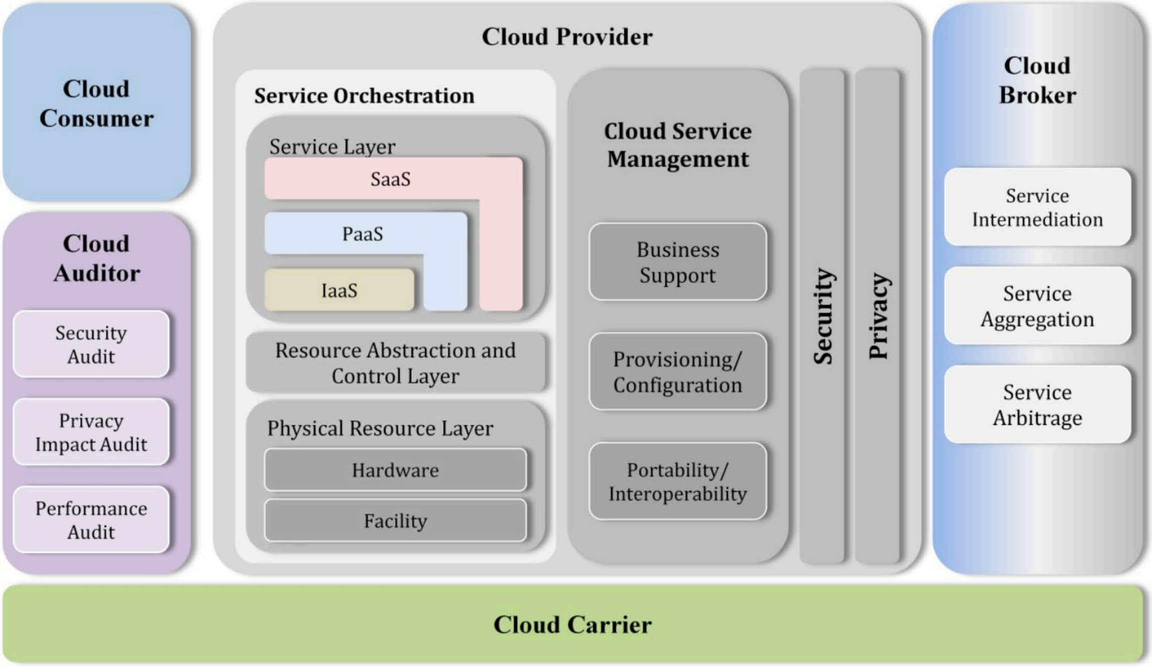
5. Additional Resources

5.01 Services Tier Mapping

Tier	*Time Period*	*Data Loss*	*Technical Solution*
0	Immediate (Active/Active)	Generally synchronous (or semi-synchronous) data replication with no or minimal data loss (PoF)	Redundant remote clustering or load balancing and synchronous replicated – transparent or near transparent recovery.
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 coupled with some form or data replication.
2	< 72 hours (Disk/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 RTO objectives.
3	< 1 week (Disk/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.

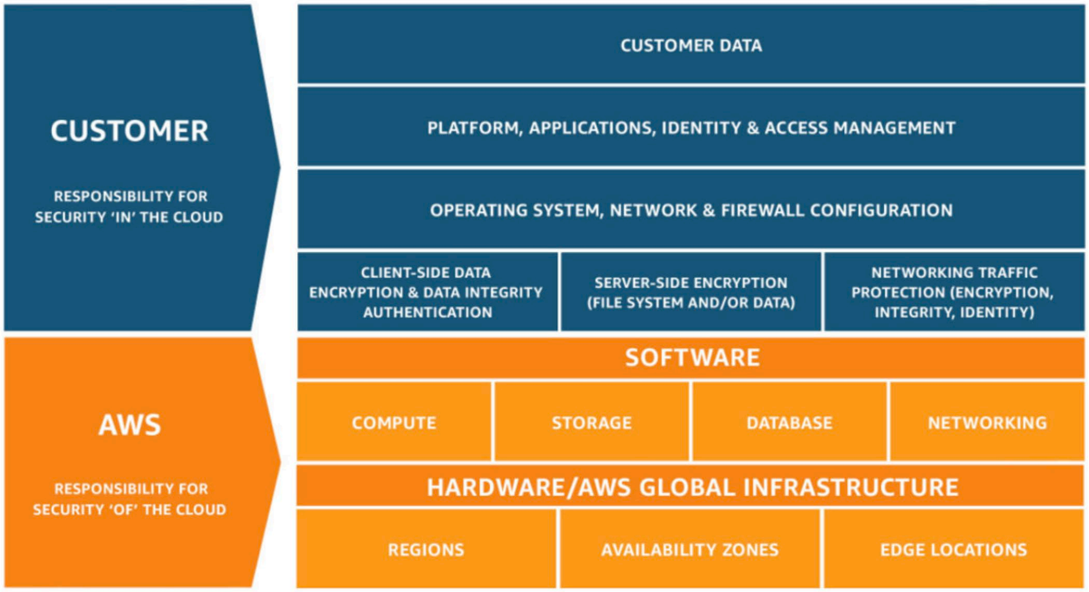
Tier	*Time Period*	*Data Loss*	*Technical Solution*
4	Deferrable	Generally, recovery from last captured backup and data loss is acceptable.	Deferrable apps can be recovered on an as needed basis –i.e., a complete build solution.

5.02 Hosting Model



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

5.03 Shared Responsibility Representative Model


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

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

5.04 Capability Review and Risk Assessment

It is important to periodically vet all ITS and non-ITS service providers on their continuity practices so that WCM data is not at risk. This assessment questionnaire is designed to identify any vulnerability area(s) which is derived from this policy. The completed assessment needs to be shared with the Program for final resolution.

Category	Description	Reference Sections
Recovery Strategy	• What is your recovery strategy? • Are these strategies documented in your contingency plan?	1.02, 2.01, 2.03, 3
Program Policy	• What drives your continuity program—i.e., DR policy or procedure?	1.01
Testing and Audit	• What is your commitment to DR testing? • Is the DR program audited?	1.02, 2.01, 3
Data Recovery	• What are your data backup procedures and storage practices?	2.01, 3
Notification and Escalation	• What is your notification and escalation documented protocol? • Declaration process? • Frequency of updates during a disaster?	1.03, 2.01
Critical Functions Recovery Plans	• Do functional plans exists?	1.02
Teams and Roles & Responsibilities	• What team structure supports your DR program?	1.03
Contact Information	• Does your DR plan identify contact information for key personnel, etc.?	3
Risk Assessment	• Do you perform a risk assessment? • Frequency of assessment? • Top risk concerns?	1.02
Supplier DR Program Information	• Which suppliers do you heavily depend on? • Are you checking their DR program?	1.02