IS-12: IT Recovery

Responsible Officer:	Chief Information Officer & VP Information Technology Services
Responsible Office:	Information Technology Services
Issuance Date:	TBD XX, 2021
Effective Date:	The Location must transition planning and execution from the 2007 version of IS-12 to this version of IS-12 no later than twelve (12) months after the Issuance Date.
Last Review Date:	TBD XX, 2021
Scope:	This policy applies to all of the following: • All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories, and all other UC locations (Locations). • All Units and related business processes, Institutional Information and IT Resources identified in the Location BCP. • All Workforce Members, Suppliers, and Service Providers, brought into scope by the Location Business Continuity Plan (BCP) and role assignments made under this policy. Note: This policy does **not** apply to students who are not Workforce Members. This policy is optional for Units not included in the Location BCP, principal investigators, faculty, and researchers. The practices outlined are recommended for: • Units not covered by Location BCP; • Research projects performed at any Location and UC-sponsored research performed by any Location that requires a data management plan.

Contact:	Robert Smith
Title:	Systemwide IT Policy Director
Email:	robert.smith@ucop.edu
Phone:	(510) 587-6244

TABLE OF CONTENTS

I. POLICY SUMMARY

The University of California's Institutional Information and IT Resources should be recoverable in the event of an unavoidable or unforeseen disaster, whether natural or human-made. The ability to recover this Institutional Information and IT Resources requires appropriate governance, funding, design, development, testing, maintenance, protection, and procurement procedures. To guide and prepare for IT Recovery and business continuity, the University has created this policy.

Locations are required by the UC Policy on Safeguards, Security and Emergency Management to have a comprehensive emergency management program. One of the key aspects of emergency management is a continuity of operations plan. UC has commonly adopted the title "Business Continuity Plan" (BCP) as the working name for this plan. This policy follows that convention. BCP is the process for developing procedures to sustain business operations while recovering from a significant disruption.

IT Recovery must align with Location BCP objectives. The Location uses its BCP and Business Impact Analysis (BIA) to determine what business processes (Units) are in scope for IT Recovery planning. The BCP and BIA result from the execution of the Policy on Safeguards, Security and Emergency Management. UC recognizes that a certain level of risk may be accepted through the Location governance processes.

This policy specifies the duties of Workforce Members responsible for the IT Recovery process. Successful execution of an IT Recovery strategy requires commitment and planning involving Location senior management and Unit Heads. The Cyber-risk Responsible Executive (CRE) oversees funding, establishing risk tolerances, and planning for the Location. The Unit Head oversees funding and planning for the Unit.

CREs appoint a Location IT Recovery Lead. Unit Heads appoint Unit IT Recovery Leads (UITRL). Section V. Compliance/Responsibilities highlights roles within this policy.

Additionally, UC has adopted five Recovery Levels (RL1 to RL5) ranging from 30 days (RL1) to 15 minutes (RL5).

The policy includes procedures to create an IT Recovery Plan.

Locations and the Units identified in the Location BCP are in-scope for this policy.

Policy Function

This policy establishes:

- Requirements for Location governance of IT Recovery planning and processes.
- Requirements for appointing IT Recovery Leads for the Location and Units.
- Requirements for identifying IT Recovery Teams.
- Requirements for Location governance of the IT Recovery process.
- Requirements for Recovery Level (RL) Classification.
- Requirements for Location/Unit IT Recovery planning and testing.
- The role of and responsibilities for Location and Unit IT Recovery Leads.
- IT Recovery responsibilities for the existing roles of Risk Manager, Business Continuity Planner, CRE, Unit Head, and Unit Information Security Lead (UISL).

Existing roles used in this policy

As part of executing the Policy on Safeguards, Security and Emergency Management and in compliance with other obligations, Locations have already established key roles used by this policy, most importantly the Risk Manager and Business Continuity Planner.

The CRE is responsible for approving the IT Recovery Plan. Some roles, including the CRE, Unit Head, and UISL, also have key responsibilities described in the UC policy, IS-3 Electronic Information Security.

Role responsibilities used in this policy

The CRE is the top-level executive for the Location's overall IT Recovery lifecycle. This includes overseeing governance, funding, and establishing risk tolerances.

The CRE is responsible for appointing one or more Location-wide IT Recovery Leads (LITRL) and ensuring the creation of the Location IT Recovery Team. The Location Recovery Team coordinates with Units for IT Recovery planning.

Unit Heads are responsible for Unit IT Recovery Planning, appointing Unit IT Recovery Leads, and ensuring the creation of Unit IT Recovery Teams. Unit IT Recovery Leads (UITRL) ensure that IT Recovery planning and testing take place. They communicate requirements to key parties and coordinate the execution of the Plan in the event of an emergency.

Unit Information Security Leads (UISLs) ensure that the planning and execution of IT Recovery includes meeting security requirements.

Role responsibilities are summarized in Section V. Compliance/Responsibilities.

II. PURPOSE

The IT Recovery requirements in this policy provide a systematic approach for planning the recovery of Institutional Information and IT Resources managed by Units, including Units that have Location-wide responsibility, such as central IT departments. This policy

provides a framework for the governance, management, development, implementation, maintenance, and testing of an IT Recovery program.

IT Recovery strategies must meet the needs of the business. Unit IT Recovery Plans must be developed in accordance with the Location BCP. Priorities and recovery time objectives (RTO) for Institutional Information, including identification of Vital Records and key IT Resources, must align with the Location's Business Impact Analysis (BIA).

Successful execution of an IT Recovery strategy requires commitment and planning involving Location senior management, the CRE, and Unit Heads.

Properly funded and organized IT Recovery is essential to successfully regain normal operations after interruption. Funding and planning must align with:

- Recovery Level (RL) – There are five levels defined, RL1 (low) to RL5 (high).
- Recovery Time Objective (RTO).
- Recovery Point Objective (RPO).
- Maximum Tolerable Downtime (MTD).

Given limited Unit IT budgets, Unit Heads may experience gaps in their IT Recovery solution. In these cases, CREs and Unit Heads must use an iterative risk-based approach, making improvements over time/budget cycles, and ensuring that Location executives understand the remaining risks.

This policy must be used in conjunction with Business and Finance Bulletin IS-3 Electronic Information Security, which identifies protective controls.

III. DEFINITIONS

Business Continuity Plan (BCP): documented procedures that guide organizations on how to respond, recover, resume, and restore business to a pre-defined level of operation following disruption. BCP is also known as a "continuity plan" in the UC Ready tool and, in other tools, Continuity of Operations (COOP).

Cyber-risk Responsible Executive (CRE): an individual in a senior management or academic position who reports to the Location chancellor or top Location executive. The CRE is accountable for all information risk assessments, security strategies, planning and budgeting, incident management, and information security implementation.

Institutional Information: a term that broadly describes all data and information created, received, and collected by UC. (See also the UC IT Policy Glossary.)

IT Recovery: a term that includes all activities needed to enable access to Institutional Information and enable business functions. This includes:

IT Disaster Recovery – recovering the operating state of IT Resources and access to Institutional Information (information systems or cloud services) that support identified business functions.

IT Service Continuity – restoring or making available equivalent functional IT Resources and access to Institutional Information, whether temporary or durable, that support identified business functions.

IT Resource: a term that broadly describes IT infrastructure, software, and hardware with computing and networking capability. These include, but are not limited to: portable computing devices and systems, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, cloud services, cloud or virtually hosted services/applications/infrastructure, backup systems, electronic media, Logical Media, biometric and access tokens, and other devices that connect to any UC network. (See also the UC IT Policy Glossary.)

Maximum Tolerable Downtime (MTD): the amount of time a mission/business process can be disrupted without causing significant harm to the Unit or Location's mission.

Recovery Point Objective (RPO): the amount of data that can be lost before significant harm to the business occurs. The objective is expressed as a time measurement from the loss event to the most recent backup preceding the event.

Recovery Time Objective (RTO): the length of time allowed for the restoration of business processes and the achievement of a stated level of service following a disruption.

Vital Records: Institutional Information essential for a Unit to continue business-critical functions, both during and after a disaster or emergency condition. (See also Business and Finance Bulletin, RMP-4.)

IV. POLICY TEXT

In carrying out its mission of teaching, research, patient care, and public service, UC's Workforce Members and affiliates create, receive, transmit, and collect many different types of Institutional Information. UC also maintains significant investments in IT Resources, which include information technology (IT) infrastructure, computing systems, network systems, industrial control systems, and cloud services.

In the event of a disaster, either natural or human-made, UC must be able to either continue or appropriately resume its mission in a timely manner. This section describes the baseline requirements for IT Recovery to serve this need.

1. Governance

Location Business Continuity Planning and Business Impact Analysis (BIA) is the overarching controlling process for a Location's IT Recovery plans.

1.1. Management direction for IT Recovery

The Location's Cyber-risk Responsible Executive (CRE), a senior executive appointed under the IS-3 Electronic Information Security policy, has broad authority and responsibility to oversee the implementation of this policy.

1.1.1. CREs must identify or appoint an IT Recovery Lead. A Location may designate one or more people/roles to meet this provision and must make the appointment(s) to ensure that scope and responsibility are understood.

1.1.2. CREs may create additional roles and assign responsibilities in order to implement this policy. Locations must establish governance and processes to support the IT Recovery requirements stated in this policy.

1.1.3. CREs must ensure the regular testing of IT Recovery Plans and the use of the testing results to improve plan effectiveness. CREs must evolve IT Recovery testing to tackle a broader scope with ever fewer resources and less disruption to ongoing activities. Testing must include failover and failback scenarios.

1.1.4. CREs must review and approve significant IT Recovery related gaps and risks requiring mitigations. CREs must review IT Recovery related gaps that result in mission risks with Location officers and associated Unit Heads.

1.1.5. CREs must review with the Chancellor or Laboratory Director the state of Location readiness to perform IT Recovery at least once every two (2) years.

1.2. Follow a risk-based approach

Locations must allocate funding to meet a wide range of priorities. The CRE makes decisions regarding funding for risk reduction.

UC uses a risk-based approach to IT Recovery, which allocates resources to protect Institutional Information and IT Resources based on their value, risk factors, likelihood, and severity of the impact of potential events causing an adverse outcome. This approach balances UC's IT Recovery goals with its other values, obligations, and interests. It also supports an iterative process for compliance.

1.2.1. The CRE must allocate funding to support the Location's IT Recovery Plan while balancing IT Recovery goals with other funding priorities.

1.2.2. The CRE must approve the IT Recovery risk that remains after funding is prioritized. (See also: 1.3 Compliance and the iterative approach.)

1.2.3. The CRE must establish and approve the risk tolerances for IT Recovery.

1.3. Compliance and iterative approach

There are two methods of complying with this policy.

1.3.1. Full compliance method

CREs and Unit Heads meet all the requirements of this policy.

1.3.2. Iterative method

To plan for IT Recovery, the Location's CRE may use an iterative model guided by the requirements of this policy. The iterative model must:

- Assess an initial state of IT Recovery preparedness/readiness.[1]
- Review and accept risks based on the Location BCP and BIA.
- Ensure that risk be accepted by a role with a level of authority corresponding to the level of risk.
- Include a review of regulatory compliance.
- Plan improvements to reach the target state, typically based on risk and resource availability.
- Implement improvements in IT Recovery to reach the target state.
- Assess the progress of policy implementation, IT Recovery plans and implementation, and the state of IT Recovery readiness.
- Repeat the process as needed, with a minimum frequency of once per fiscal year.

1.4. Appointing IT Recovery Leads

[1] State of IT Recovery - The organization identifies its business/mission objectives and high-level organizational priorities for IT Recovery. With this information, the organization makes strategic decisions regarding the readiness of IT Recovery using this policy and other UC policies to assess implementations and determine the scope of Workforce Members, plans, tools, and other resources that support the selected business line or process.

The responsible official (CRE or Unit Head) appoints respective IT Recovery Leads.

1.4.1. The CRE must appoint one or more Location IT Recovery Lead(s).

1.4.2. Unit Heads must appoint one or more Unit IT Recovery Lead(s).

1.5. IT Recovery Plan approval

IT Recovery Plans are fundamental to a Location's ability to carry out its mission and thus oversight is key.

1.5.1. The CRE must approve the Location IT Recovery Plan.

1.5.2. The CRE must establish and approve the Location process for approving Unit IT Recovery Plans.

1.5.3. The process must include Unit Head approval.

1.6. Plan activation

Unit Heads, in consultation with the Risk Manager and CRE, are responsible for activating their Unit IT Recovery Plan.

The CRE, in consultation with the Risk Manager and Chancellor, is responsible for activating their Location IT Recovery Plan.

1.7. Violations and sanctions

The following disciplinary sanctions are authorized for confirmed and serious violations of this policy.

1.7.1. Confirmed serious violations of this policy by Workforce Members may result in sanctions, which are governed by:

- Policies Applying to Campus Activities, Organizations and Students (PACAOS) if the student is part of the Workforce (see "Workforce Member" in the IT Policy Glossary).
- Personnel Policies for Staff Members (PPSM) 3, 62, 63, 64, and II-64 pertaining to disciplinary and separation matters.
- As applicable, the Faculty Code of Conduct (APM - 015), University Policy on Faculty Conduct and the Administration of Discipline (APM - 016) and Non-Senate Academic Appointees/Corrective Action and Dismissal (APM - 150).
- As applicable, collective bargaining agreements.
- As applicable, non-faculty medical staff disciplinary action policies.
- Other applicable policies.

1.7.2. Confirmed serious violations of this policy by Workforce Members may result in employment or educational consequences, up to and including:

- Informal verbal counseling or a written counseling memo and education.
- Mandatory education and/or supplemental training.
- Adverse performance appraisals.
- Corrective or disciplinary actions.
- Termination.

1.8. Insurance coverage

A significant failure to comply with this policy may affect the Unit's or the Location's ability to seek cyber insurance reimbursement under Business and Finance Bulletin BUS-80 – Insurance Programs for Information Technology Systems.

2. Exceptions

While exceptions to an IT Recovery policy or standard may weaken the Location's ability to withstand a disaster, they are occasionally necessary and permitted.

Units must follow a risk-based approach when requesting an exception to the controls specified in Part IV, V, and VI. Exception requests must be submitted to the Risk Manager and follow the Location-approved exception process.

2.1. Exception process requirements

2.1.1. Location exception process approval

The CRE is responsible for approving the Location exception process.

2.1.2. Required circumstances for exception

An exception to this policy may be granted under these circumstances:

- When immediate compliance would disrupt a critical operation;
- When compliance would adversely impact the business process;
- When another acceptable solution with equivalent protection is available and implemented/implementable; or
- When compliance would cause a major adverse financial impact to the Unit that would not be offset by the risk reduction achieved by compliance.

2.1.3. Exception request documentation

The exception request must document all of the following:

- The specific policy/standard for which an exception is being requested.

- The specific business process, IT Resource, and Institutional Information for which the exception is being requested.
- The impact on the MTD, RTO, and RPO of the exception requested.
- Why an exception is required (e.g., what business need or situation exists that prevents/limits compliance, alternatives that were considered, and why alternatives were not appropriate).
- Assessment of the potential risk posed by non-compliance.
- Plan for managing or mitigating risks (e.g., compensating controls, alternative approaches, etc.).
- Anticipated length of the exception.
- How any proposed compensating controls mitigate IT recovery risks that this policy would otherwise address; and
- Additional information as needed, including any specific conditions or requirements for approval.

2.1.4. Unit requirements

At the Unit level, the following is required for all exceptions:

- The Unit Head of the requesting Unit must review and approve exception request.
- UITRL must identify compensating controls when required by external obligations or situations involving IT Resources or Institutional Information classified at RL 3 or above.

2.1.5. Exception approvals

Exceptions are approved based on the RL.

- The Risk Manager must approve all requests for exceptions to this policy involving Institutional Information and IT Resources classified from RL1 to RL5.
- Additionally, the CRE or designee must approve all requests for exceptions to this policy involving Institutional Information and IT Resources classified from RL4 and RL5.

Exception requests and decisions must be documented, periodically reviewed based on risk, and retained by the Risk Manager.

3. IT Recovery teams

The IT recovery teams are groups of Workforce Members who are tasked with developing, documenting, and executing processes and procedures for the Location's or Unit's IT Recovery in the event of a disaster or failure.

3.1. Location Recovery Team

The CRE must identify a role (e.g., Location IT Recovery Lead, Risk Manager, Business Continuity Manager, or other suitable role) that will collect Location-wide recovery team contact information and share it with appropriate Units.

3.1.1. Identification of IT Recovery teams

These teams include, but are not limited to:

- Data Center Recovery Team.
- Location IT Infrastructure Recovery Team.
- Website Recovery Team.
- Application Recovery Team.
- Telecommunications, Network, and Internet Services Recovery Team.
- Academic Computing, Instructional Systems, and Classroom Recovery Team.
- Other Location-wide identified/required teams.

3.1.2. Contact information

Contact information includes, but is not limited to:

- Name.
- Title.
- Role (e.g., IT Recovery Lead).
- Primary phone and alternate phone number.
- Primary email and alternate email.
- Other communication method (e.g., team collaboration, web or phone conferencing, messaging, or radio).

Note: When possible, identify the primary and secondary contacts.

3.2. Unit Recovery Team

The Unit Head must identify a role (e.g., UITRL, UISL, or other suitable role) that will collect Unit recovery team contact information and share it with the Location IT Recovery Lead and Risk Manager.

3.3. Recovery Plan activation

Plan activation responsibility for Location and Unit are as follows:

- CREs are responsible for activating the Location IT Recovery Plans in consultation with the Risk Manager and other Location officials as designated in the Location IT Recovery Plan.

- Unit Heads are responsible for activating the Unit IT Recovery Plans in consultation with the Risk Manager.

4. Asset management

Asset management identifies assets (Institutional Information and IT Resources) subject to IT Recovery requirements and defines appropriate recovery levels. The identification of Vital Records in electronic format/media is part of IT Recovery planning.

4.1. Inventory of assets

When in scope of the Location BCP, the Unit IT Recovery Lead (UITRL) must maintain an inventory for the lifecycle of Institutional Information and IT Resources procured or managed by the Unit and classified at any Recovery Level. At a minimum, the inventory record must contain:

- An identification of the asset (name, asset tag, service tag, or other unique identifier);
- Identity of the Institutional Information Proprietor;
- Recovery Level (RL);
- Location of the Institutional Information or IT Resource;
- Configuration or security documentation; and
- Notation that identifies Vital Records.

This can be the same inventory as required by Business and Finance Bulletin IS-3 – Electronic Information Security, III. 8.1.1 Inventory of Assets, recording Protection Level and Availability Level.

4.2. Recovery Level classification

The Institutional Information and IT Resources associated with the Location BCP must receive an appropriate level of IT Recovery planning and preparation in accordance with the assigned Recovery Level (RL) classification.

4.2.1. Recovery Level Classifications

UITRLs must assign in-scope Institutional Information and IT Resources a Recovery Level Classification using the following levels.

Recovery Level (RL)	Description of IT Resources and Institutional Information	Recovery Time Objective (RTO)
RL5	Core technology and infrastructure	15 Minutes
RL4	Critical 1 - Life/safety/alternatives not sustainable	Up to 6 hours

RL3	Critical 2 - Alternatives sustainable up to 24 hours	Up to 24 hours
RL2	Necessary	Up to 5 days
RL1	Deferrable	Up to 30 days

4.2.2. Recovering other assets

Unit Heads have discretion in planning for and addressing IT Recovery needs for IT Resources and Institutional Information supporting business processes not identified in the Location BCP. When planning for these other IT Recovery needs, Unit Heads should follow this policy.

5. Lifecycle Management

UITRLs must ensure IT Recovery requirements are addressed during the design/specification of in-scope information processing systems and throughout the lifecycle of in-scope IT Resources and Institutional Information.

5.1. Lifecycle planning for IT Recovery – design/acquisition

Planning for IT Recovery starts during system design/acquisition and must include:

- Choosing physical or virtualized IT Resources (e.g., servers, storage, networks, etc.) and services (e.g., on premise, cloud, hybrid, micro-services/service mesh, etc.) to accelerate and simplify IT Recovery.
- Leveraging virtualization, workload migration, and orchestration to automate IT Recovery, when applicable.
- Selecting Suppliers that can meet Location and Unit IT Recovery requirements.

5.2. Lifecycle considerations

Lifecycle considerations must include at least:

- Selection of Suppliers.
- Architecture of the system.
- Selection of IT Resources and their likely availability during a widespread or regional disaster.
- Selection and availability of tools, contractors, and Supplier resources during a disaster.
- Single points of failure.
- Required updates and technology.

- Post-event analysis (i.e., actual use of the IT Recovery Plan) after terminating the declared IT Recovery operation.
- Changes in needs.

6. Unit IT Recovery planning

The IT Recovery Plan is a formally documented, structured approach that describes how work can quickly resume after a disruption or disaster.

6.1. Ensuring IT Recovery Plan adherence to policy requirements

The following roles are responsible for ensuring plans follow procedural policy requirements:

- The LITRL must ensure the Location IT Recovery Plan is developed per the requirements in section VI Procedures.
- The UITRL must ensure the Unit IT Recovery Plan is developed per the requirements in section VI Procedures.

6.2. IT Recovery Plan updates

LITRLs and UITRLs must review or update their respective IT Recovery Plan:

- Annually;
- When required by modifications to the Location BCP; and
- In response to major changes made by the Unit.

6.3. Access to Unit IT Recovery Plans

LITRLs and UITRLs must ensure their:

- IT Recovery Plans are stored in the UC-approved centralized repository or a CRE-approved alternative for storage location.
- IT Recovery Plan methods of access are recorded with the Location Business Continuity Planner.
- IT Recovery Plans are highly available and accessible (e.g., redundant, geographically dispersed, etc.) in the event of a major disaster or adverse event.
- IT Recovery Plans are securely stored.

7. IT Recovery Plan testing

IT Recovery Plan testing identifies potential issues or gaps in plans, allowing corrective action in advance of a disruption or disaster.

7.1. IT Recovery Plan testing requirements

LITRLs and UITRLs must ensure IT Recovery Plan testing:

- Includes a method to inform Location stakeholders of planned testing and any impact to operations.
- Is performed at least annually or on a Location schedule approved by the CRE.
- Reflects mission risk and include a mix of:
    - Appropriately scoped tabletop exercises.
    - Live recovery drills that include fail-over testing and fail-back testing.
- Includes a representative set of IT Resources and Institutional Information.
- Analyzes the results obtained from testing the IT Recovery Plan and make required adjustments based on lessons learned, identified gaps, or errors.
- Is tested according to a schedule based on risk (e.g., Recovery Level and Availability Level).
- Produces documented test results.
- Records of lessons learned and required changes.
- Includes the CRE as a participant at least once every three (3) years.

7.2. Actual disruption or disaster

An actual disruption or event does **not** constitute an IT Recovery Plan test unless the event is representative of mission risk (e.g., the same scale as the risk area that would have been tested).

7.3. Backup location and testing

Consistent backup testing lessens the risk of losing the data, applications, systems, and workloads that backups contain. Testing verifies backups will perform as expected in a disaster or disruption scenario.

7.3.1. The CRE must approve the frequency of backup testing. RL4 and above require backup testing of at least once a year.

7.3.2. LITRLs and UITRLs must anticipate adverse events when choosing the location and connection of their respective backups (e.g., backup stored away from physical or logical area(s) of possible loss).

- For RL3 and above, a separate copy of Institutional Information and applications/tools must be stored off-site (i.e., not another location on-site).

- For the purposes of this policy, a live transactional/operational copy at the Location is not considered a backup (i.e., a geographically and logically separated second copy is required).

7.3.3. UISLs and ITRLs/UITRLs must ensure the isolation and protection of their respective backups reflect and anticipate modern cyber risks (e.g., ransomware, wipers, sabotage). This includes the protection of:

- Logical/virtual backups.
- Physical backups from unauthorized access, theft, tampering, or destruction.

7.3.4. LITRLs and UITRLs must ensure backup and tool strategies are tested independently from IT Recovery Plans.

7.3.5. LITRLs and UITRLs must ensure testing of IT Recovery related backups includes:

- Retrieval of identified backups;
- Ensuring the MTD, RPO, and RTO objectives are met;
- Integrity of the backup; and
- Recovery/restoring the Institutional Information and IT Resources, including having emergency access to secrets (e.g., keys and passphrases) so that operations can continue.

7.3.6. LITRLs and UITRLs must ensure backup media retrieval planning includes:

- The specific method to retrieve off-site backup media in support of the RTO requirements.
- Supplier contact information used for media retrieval.

7.3.7. For RL3 and above, LITRLs must review the results from testing of IT Recovery related backups with the CRE at least annually.

8. Service Providers

Heads of Units that are Service Providers must plan for the IT Recovery needs of client Units, communicate clearly to client UITRLs concerning the response priority, and respond to supported client Units during disasters or disruptions.

9. Security requirements for IT Recovery

The following security requirements for IT Recovery planning, execution, and communication apply.

9.1. Security requirements during planning and execution of IT Recovery

9.1.1. UISLs and LITRL/UITRLs must plan for and comply with IS-3 security requirements in the planning and execution of IT Recovery. This includes ensuring security is maintained during a disaster or disruption.

9.1.2. UISLs must ensure security requirements are communicated to the LITRL/UITRL.

9.1.3. LITRLs/UITRLs must ensure backups are protected using IS-3 controls.

9.2. Communicating changes

9.2.1. UISLs must communicate changes in security requirements for Institutional Information and/or IT Resources to the UITRL and/or LITRL.

9.2.2. UISLs must communicate changes in security requirements for Institutional Information and/or IT Resources to affected Suppliers.

See also the References and FAQ sections of this policy.

10. Lesson learned post-event analysis

IT Recovery Leads conduct lessons learned to collect documented information that reflects both the positive and negative experiences from an IT Recovery event or IT Recovery Plan test.

10.1. IT Recovery Lessons Learned

10.1.1. LITRLs and UITRLs must conduct a lessons learned review after a major event or testing of the IT Recovery plan and supporting processes.

10.2. Updating IT Recovery plans and other supporting processes

10.2.1. LITRLs and UITRLs must ensure IT Recovery Plan updates that result from testing or from the use of the IT Recovery Plan (e.g., lessons learned) are made and presented for approval by the Unit Head within forty-five (45) calendar days of test completion or event/use.

10.2.2. LITRLs and UITRLs should update IT Recovery supporting processes as determined in the lessons learned review.

V. COMPLIANCE / RESPONSIBILITIES

Role	Responsibilities	Notes
Cyber-risk Responsible Executive (CRE)	Identifying a role (e.g., Location IT Recovery	

Role	Responsibilities	Notes
	Lead, Risk Manager, Business Continuity Manager, or other suitable role) that will collect and share recovery team contact information with Units Location-wide. Approving: ● The Location IT Recovery Plan. ● The Location process of approving IT Recovery Plans. ● The exception process. ● Risk exceptions that impact the Location mission or IT Resources classified at RL4 and RL5. ● Ensuring the testing frequency of IT Recovery Plans is adequate to addresses risk ● The storage location(s) for IT Recovery Plans. ● The frequency of IT Recovery Plan testing. ● The frequency of backup recovery testing. Participating in Location Recovery Plan testing once every three (3) years. Ensuring testing the frequency of the IT Recovery Plans adequately addresses mission risk related to BCP. Allocating funding to meet organization risk tolerances.	

Role	Responsibilities	Notes
	Approving the governance process and managing the overall Location risk tolerance related to IT Recovery. Reviewing and approving significant gaps and risks requiring mitigations and evaluating associated mission risks with Location officers/Unit Heads. Reviewing with the Chancellor or Laboratory Director the state of Location readiness to perform IT Recovery.	
Unit Heads	Activating the Unit IT Recovery Plan in consultation with the Risk Manager. Reviewing and approving the Unit IT Recovery Plan. Allocating sufficient funding to meet IT Recovery objectives. Reviewing and approving exceptions before they are presented to the Risk Manager or CRE for approval. Identifying and establishing procedures to achieve Unit compliance with Location implementation of the BCP. This task can be delegated. Appointing one or more IT Recovery Leads for the Unit.	Unit Heads are the same as defined and identified in IS-3.

Role	Responsibilities	Notes
	Assigning, or designating a delegate to assign, IT Recovery related training. Assigning one or more Workforce Members to develop the Unit IT Recovery Plan.	
Business Continuity Planners	Facilitating access to a UC-approved centralized repository for recovery plans or the CRE-approved alternative (e.g., UC Ready). Facilitating communication and sharing BCP between stakeholders. Facilitating communication and sharing BIA between stakeholders. Training UISLs, IT Recovery Leads, and other Workforce Members on the Location BCP and procedures.	Often the administrator to UC Ready or Location-approved alternative to the UC Ready tool.
Unit IT Recovery Lead (UITRL) Location IT Recovery Lead (LITRL)	Overseeing the development of assigned (Location or Unit) IT Recovery Plans in accordance with this policy. Briefing Unit Heads on the progress of IT Recovery Planning. Overseeing the testing of assigned IT Recovery Plans. Ensuring IT Recovery Plan updates that result from testing or from use of the IT Recovery Plan (e.g., lessons learned) are made	

Role	Responsibilities	Notes
	and presented for approval by the Unit Head within forty-five (45) calendar days of test completion. Ensuring an accurate inventory. Overseeing the execution of the IT Recovery Plan. ● Monitoring IT Recovery reporting progress. ● Overseeing the restoration of normal operations. ● Reviewing the IT Recovery Plan and participating in updates. ● Briefing Unit Heads on the progress of IT Recovery. ● Performing post-event analysis (i.e., actual use of the IT Recovery) after terminating the declared IT Recovery operation and updating the IT Recovery Plan based on the lessons learned. At least annually and when major changes occur, reviewing the Unit's deployed IT Resources and Institutional Information for changes and ensuring the IT recovery Plan is up-to-date by requesting appropriate action to close any identified gaps. Ensuring proper storage, documentation, and access of IT Recovery Plans and sharing that information	

Role	Responsibilities	Notes
	with the Location Business Continuity Planner. Assigning Recovery Level (RL) Classification. Reviewing and updating the IT Recovery Plan. Ensuring protection of backups, including testing of backup and tool strategies. Planning for and complying with IS-3 security related requirements. Complying with requirements in this policy. Completing assigned training.	
Risk Manager	Advising on the use of the Location Business Continuity Plan (BCP). Approving and documenting exceptions using the Location-approved process. Consulting in the decision to activate the Unit IT Recovery Plan(s). Completing assigned training.	
Unit Information Security Leads (UISL)	Ensuring security requirements are communicated to the Unit IT Recovery Lead. Sharing changes in IT Resources and Institutional Information with the Unit IT Recovery Lead.	This policy relies on the IS-3 definition of UISL.

Role	Responsibilities	Notes
	Ensuring security is maintained during a disaster or disruption. Ensuring backups are protected using IS-3 controls. Ensuring the isolation and protection of backups reflect and anticipate modern cyber risks. Planning for and complying with IS-3 security related requirements. Completing required training.	
Workforce Members	Cooperating with Location emergency instructions. Following business continuity procedures. Complying with Location procedures in support of this policy. Exercising responsibility appropriate to their position and duties. Completing assigned training.	In this policy. the only obligations are to those Workforce Members that are assigned specific duties in support of IT Recovery.

VI. PROCEDURES

Units that the Location Business Continuity Planner identifies as being in-scope under the Location Business Continuity Plan (BCP) must develop plans that address the requirements listed in this section. The objective is that Location and Unit IT Recovery plans support the Location BCP.

1. IT Recovery Plan requirements for in-scope Units

To support the Location BCP, in-scope Units developing their IT Recovery Plan must:

1.1. Identify and develop procedures to implement temporary processes (physical or logical), fail over to another Location, use of a Supplier/Alternate-Supplier, or recovery in another physical location.

1.2. Identify the Unit IT Recovery Lead (i.e., one or more Workforce Members who fill this role).

1.3. Identify Workforce Members assigned responsibility for responding in emergencies, including their primary and secondary contact information.

1.4. Document communication plans in accordance with the Location-wide communication plan and strategy (e.g., alternate phone numbers, conferencing systems, email, messaging, document repositories, etc.).

1.5. Identify IT Recovery actions to be taken to facilitate both short-term recovery (e.g., loss of power) and long-term recovery (e.g., loss of: Workforce Members, buildings, IT Resources, Institutional Information, and Location operational capability).

1.6. Ensure response procedures anticipate the need for alternative Workforce Members to address the inability of assigned personnel to participate in response efforts.

1.7. Identify deployment procedures to relocate or replicate IT Resources and Institutional Information (e.g., alternate Locations).

1.8. Support provisions for remote worksites/locations.

1.9. Identify IT Recovery actions to be taken to facilitate return of IT Resources, Institutional Information, and Location operational capability to the primary site (e.g., failback, swing-back, flip-back).

1.10. Identify dependencies on other services, key services, and IT Resources:

- Service Providers.
- Central IT services.
- Supplier services and/or Supplier managed IT Resources.

Examples of dependencies might include network access, active directory/LDAP, and basic assumptions about other IT capabilities, such as wireless network and security tool availability.

1.11. Identify recovery sites, including:

- UC.

- Non-UC.
- Supplier alternative sites or zones.

1.12. Plan for the acquisition of IT Resources for recovery, including:

- Identification of sources to provide replacement IT Resources.
- Pre-staging of specialized equipment and software not generally available.

1.13. Establish procedures that ensure authorized access to recovery sites (e.g., primary, secondary, or tertiary as applicable) and supporting resources (e.g., media storage, equipment storage, tools, and other required items) in support of MTD, RTO, and RPO.

1.14. Identifying and planning to acquire required backup equipment.

1.15. Establish procedures to retrieve, recover, and restore backups that consider:

- Location of virtual, on-site, and off-site storage.
- Cloud, SaaS, and PaaS Suppliers.

1.16. Establish procedures that ensure coordination with the Location's CIO office (central IT) and the CISO office (security office).

1.17. Securing Institutional Information during IT Recovery.

1.18. Ensuring provisions in Agreements (e.g., contracts) with external Suppliers that ensure their preparedness for emergency response and business recovery.

1.19. Establishing emergency access to secrets (e.g., passwords/passphrases, digital keys, certificates, physical keys, etc.).

1.20. Addressing the loss of a Supplier and/or Supplier Zone/Region.

1.21. Identifying Suppliers specifically needed to support IT Recovery and contacts at those Suppliers.

1.22. Meeting external contractual commitments related to IT Recovery Requirements (e.g., contracts, grants, other agreements).

1.23. Identifying Service Providers' capabilities to support IT Recovery, including:

- SLAs to meet Unit requirements.

- Redundancy.
- Mitigations and migration tools.

1.24. Developing and conducting IT Recovery training, including:

- Training specified for Workforce Members responsible for IT Recovery.
- Cross-training requirements for IT Recovery.

VII. RELATED INFORMATION

1. University of California Resources

Policy on Safeguards, Security and Emergency Management: https://www.ucop.edu/enterprise-risk-and-resilience/_files/crisis-management/ssempolicy.pdf (Linked on this page: https://www.ucop.edu/enterprise-risk-and-resilience/resilience/crisis-management.html.)

Business and Finance Bulletin BUS-80 – Insurance Programs for Information Technology Systems.

IS-3 Electronic information security policy and standards: https://security.ucop.edu/policies/
(See X. Appendix A for additional information.)

Records Management Policies (RMP): https://www.ucop.edu/information-technology-services/policies/records-management-policies.html

Enterprise Risk and Resilience: https://www.ucop.edu/enterprise-risk-and-resilience/resilience/crisis-management.html

2. External Resources

NIST 800-34 Contingency Planning Guide: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

Ready.GOV - IT Disaster Recovery Plan: https://www.ready.gov/business/implementation/IT

VIII. FREQUENTLY ASKED QUESTIONS

1. What is the difference between IS-3's Availability Level and IS-12's Recovery Level?

IS-3's Availability Levels assign additional security controls to help ensure access to and use of Institutional Information and IT Resources. Availability is one of the

traditional elements of the information security triad – Confidentiality, Integrity, and Availability.

IS-12's Recovery Level designates how fast the Institutional Information or IT Resource should be restored after a disaster or disruption. This relates primarily to the RTO for the IT Resources and Institutional Information.

2. How will IS-12 impact faculty and researchers?

IS-12 might impact faculty, for example, if a Location decides to include certain academic and/or instructional technology business processes in the Location Business Continuity Plan (BCP). This might involve plans to recover the use of an online classroom or instructional technology that supports instruction when facilities are not available.

Another example might be a Unit that operates a lab where research is performed as a service. The Unit would use IS-12 to develop the lab's IT Recovery plan. The researchers would be involved in IT Recovery planning and, if required, the implementation of that plan.

3. To whom would the sanctions outlined in Section IV.1.7 apply?

IS-12 is a policy designed to cover a specific topic. The policy is applied according to a Location's business continuity planning and prioritization. Therefore, this section would only apply to the roles defined in this policy as assigned by the Location. The section would not apply to other Workforce Members.

4. Who determines what a Vital Record is?

The Location Records Manager should be consulted to make this determination. This determination should be made narrowly.

5. Is there an example for how Locations perform BCP and BIA?

Yes – from UC Berkeley: Through questionnaires, surveys, interviews, and other forms of information gathering, a Business Continuity Planner will work with various functional Units at the Location to determine what essential/critical functions and processes those Units support for daily operations, including information like MTD, RPO, RTO, and Vital Records they create and are responsible for, and the impacts to the Location if those functions are disrupted. They will also identify acceptable minimum operations, within what timeframes, what resources are dependencies / necessary, and acceptable risks. This information is documented in a BIA report. Functional Units will then work with the Business Continuity Planner to create a BCP, which documents the plans and strategies for resumption to minimum operations initially, and full operations eventually, incorporating that information into the BIA.

IX. REVISION HISTORY

TBD, 2021: Major rewrite to comply with academic research/grant requirements, conform to cyber insurance underwriting, conform to the Office of Civil Rights guidance on HIPAA compliance, adapt to changes in security landscape (ransomware and wipers), and adopt a standards-based approach to IT Recovery. Updated to align with UC's overall business continuity and disaster preparedness planning. The name was changed from "Continuity Planning and Disaster Recovery" to "IT Recovery." Additional features were added to support Location governance, budgeting and risk management.

April 20, 2012: The policy was reformatted into the standard University of California policy template and to support web accessibility guidelines.

July 27, 2007: The policy was updated.

X. APPENDIX A

This Appendix lists some of the relevant controls from Business and Finance Bulletin, IS-3 Electronic Information Security.

Section	Topic	IS-3 Control
12.3	Backup/ Recovery	Units must ensure that Institutional Information classified at Availability Level 3 or higher is backed up and recoverable.
12.3	Backup/ Recovery	Units must comply with UC Records Retention Schedule for retention of backups.
12.3	Backup/ Recovery	Units must protect backups according to the Protection Level of the Institutional Information they contain.
12.3	Backup/ Recovery	Units must ensure that portable backup media meet the portable media requirements outlined in this policy.
12.3	Backup/ Recovery	Units must document and execute a plan to test restoration of Institutional Information from backups.
12.3	Backup/ Recovery	Units must maintain a backup catalog that shows the location of each backup and retention requirements.
14.1	Security requirements of information systems	Units must identify system security and management requirements in the planning phase and prior to development or acquisition of a system. System security requirements must include: • The elements described in the UC Secure Software Configuration Standard. • The Risk Assessment or Risk Treatment Plan. • The Protection Level and Availability Level. • The UC Minimum Security Standard. Units must ensure that software developed in-house that stores, processes or transmits Institutional Information classified at Protection Level 2 or higher is developed in compliance with the UC Secure Software Development Standard.

Section	Topic	IS-3 Control
		For Institutional Information and IT Resources classified at Protection Level 4, Units must conduct penetration testing at a minimum: • Once every three years. • After a major change occurs.
15.2.1	Unit responsibilities when using suppliers	Units must work with their central Procurement departments to ensure that agreements and other arrangements with persons or Suppliers conform to the requirements of this policy. (See the policy section for a list of requirements. These requirements are met by UC's Appendix Data Security.)
17.1	Information security and business continuity	Units must plan, implement, test and review the continuity of information security as an integral part of the Unit's business continuity and disaster recovery plans. Units must include IT Resources classified at Availability Level 4 in emergency and disaster recovery planning.

In addition, the following UC information security standards are relevant to the overall IT Recovery program:

- Minimum Security Standard.
- Secure Software Development Standard.
- Secure Software Configuration Standard.