IS-12 IT Recovery Policy

Key Features

SUMMARY

ROBERT SMITH

ROBERT.SMITH@UCOP.EDU
Effective Date

**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.

12 Months to move to the new iterative model! Resets the compliance clock!
Limited scope based on Location BCP

Scope:
- All Units and related Institutional Information and IT Resources identified in the Location Business Continuity Plan (BCP).

Location planning and priorities now drive scope and implementation.
New iterative model – based on IS-3/CSF

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.
Robust Location 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.
## Noteworthy Comparison

<table>
<thead>
<tr>
<th>Improvements addressed</th>
<th>Advantages of the Rewritten Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Added new features</td>
<td>• Now aligned with technology.</td>
</tr>
<tr>
<td>• Narrower scope – Location defined.</td>
<td>• Aligns with UC Health Recovery levels.</td>
</tr>
<tr>
<td>• Exception process.</td>
<td>• Now aligned with Cloud and Service Providers.</td>
</tr>
<tr>
<td>• Iterative model for compliance.</td>
<td>• Directly implementable.</td>
</tr>
<tr>
<td>• Clock restarts – 12 months to transition.</td>
<td>• Systemwide consistency.</td>
</tr>
<tr>
<td>• The current policy does not align with UC Health recovery levels. Aligning helps UC Health and:</td>
<td>• Endorsed by systemwide workgroup, including BCP leads</td>
</tr>
<tr>
<td>• UCLA</td>
<td>Sponsored by:</td>
</tr>
<tr>
<td>• UC Davis</td>
<td>◦ UCACC/AS</td>
</tr>
<tr>
<td>• UCI</td>
<td>◦ Risk Services</td>
</tr>
<tr>
<td>• UCSD</td>
<td>◦ Systemwide IT</td>
</tr>
</tbody>
</table>
Old IS-12 Roles map to new!

B. Campus
Chancellors, the Executive Vice President - Business Operations at the Office of the President, and UC managed national laboratory directors are responsible for delegating responsibility for implementation of these guidelines in locations. Information Security Officers are responsible for facilitating compliance with the campus Information Security Program.

C. Divisions and Departments
Division deans, department chairs, and appropriate administrative units are responsible for identifying and establishing procedures to assure compliance with campus implementation.

D. Individuals
All members of the University community are expected to comply with emergency instructions, follow emergency procedures, and report policies and procedures in support of this bulletin and to execute them appropriately to their position and delegated authorities. Each conducts the business of the University in accordance with the

VP Business Ops ➔ CRE

Department Head ➔ Unit Head

Individuals ➔ ITRL
Old blocks mapped to new

<table>
<thead>
<tr>
<th>Current IS-12</th>
<th>New IS-12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identify – roles/people</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Removed from IS-12 – this topic is covered in IS-3 IR Standard</td>
</tr>
<tr>
<td>Technology and Infrastructure</td>
<td>Same</td>
</tr>
<tr>
<td>Preparedness</td>
<td>Same + communication plan</td>
</tr>
<tr>
<td>Response</td>
<td>Same</td>
</tr>
<tr>
<td>Recovery</td>
<td>Same</td>
</tr>
</tbody>
</table>
thank you!

QUESTIONS – CONTACT:
robert.smith@ucop.edu