Executive Board

(Systemwide Senate Review) Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Table of Contents

Generated 7/1/2025 5:59 PM

UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

Mary Gauvain
Telephone: (510) 987-0887
Email:mary.gauvain@ucop.edu

Chair of the Assembly of the Academic Senate
Faculty Representative to the Regents
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200

March 8, 2021

SUSAN CARLSON, VICE PROVOST
ACADEMIC PERSONNEL

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Susan,

As requested, I distributed for systemwide Senate review the proposed revisions to Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Nine Academic Senate divisions and three systemwide committees (UCACC, UCORP, and UCFW) submitted comments. These comments were discussed at Academic Council's February 24 meeting and are attached for your reference.

We understand that the IS-12 policy describes requirements and procedures around the recovery of UC data and other IT resources following a disaster, and details the planning, oversight, and implementation of an IT recovery program at each UC location. The revisions update the existing policy to reflect contemporary technology concerns and issues; provide guidance to UC locations on data recovery; ensure compliance with requirements related to HIPAA, insurance underwriting, and research grants; provide for local governance of IT recovery, budgeting, and risk management; and outline a standards-based approach to IT recovery. Finally, the policy defines the responsibilities of the personnel who will be assigned to IT recovery functions at each location, including the Cyber-risk Responsible Executive (CRE), Unit Head, Unit and Location Leads, Risk Manager, Business Continuity Planner, and others.

In general, Senate reviewers believe the policy includes reasonable and practical requirements that will help UC locations prepare for disasters and IT recovery, while giving individual campuses control over local implementation. However, reviewers also raise a number of concerns and questions that warrant additional consideration. One of the dominant concerns is that the policy text is overly complex and uses technical jargon and concepts that make it inaccessible to a non-expert audience. We encourage the authors to consider suggestions in our comments to provide or clarify definitions of key terms and concepts, policy implementation criteria, communication processes, and management reporting structures, and to add specific examples to the policy to help readers without a specialized background more easily understand the basic provisions and implications of the policy, particularly its impact on faculty in their roles as researchers and educators.

Senate reviewers are also concerned that a costly new bureaucracy may be needed to implement the policy, forcing a significant unfunded mandate onto campuses already bracing for budget cuts. One budget-related suggestion is to include a cost-benefit analysis outlining the fiscal implications of the policy. Another is for the University to review the IT recovery services included in UC's cloud technology contracts, and identify gaps between the contracts and the revised policy as well as opportunities for additional linkages.

There was also concern about who on the campus will provide oversight of these activities and how well they are working. The working groups or committees charged with this responsibility should include members from the campus faculty, possibly from computer science departments. This will help ensure that the rights and activities of faculty will be considered in any proposed practices or decisions. In the Council discussion, members commented that IT managers on the campuses often want to make changes quickly and, in their urgency, bypass consultation with faculty because it is seen as too difficult or slow. Some clear and direct communication processes need to be established so that urgent matters can be dealt with in a consultative and timely manner. Finally, while faculty need to be made aware of their data security responsibilities, the administration needs to understand and address faculty concerns regarding academic freedom and privacy when IT changes are proposed, for example, in wanting to install software, such as malware, on faculty computers.

The enclosed letters make several other suggestions for further developing the policy, including clarifying its impact on faculty research data; how IT recovery mechanisms will be tested and evaluated for vulnerabilities; how recovery priorities will be established and recovery efforts funded; contingencies to address if a campus is unable to recover its data; and the provision of sanctions and discipline to individuals and teams found out of compliance.

We appreciate the opportunity to comment and also appreciate the ongoing consultation by Systemwide IT Policy Director Robert Smith with the University Committee on Academic Computing and Communications during the development of the policy.

Please do not hesitate to contact me if you have additional questions.

Sincerely,

Mary Gauvain

Mary Gauvain, Chair
Academic Council

cc: Systemwide IT Policy Director Smith
Academic Council
Senate Division Chairs
Executive Director Baxter

Encl.

ACADEMIC
SENATE
BERKELEY

320 STEPHENS HALL
UNIVERSITY OF CALIFORNIA

February 17, 2021

MARY GAUVAIN
Chair, Academic Council

Subject: Systemwide Review of Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair Gauvain;

On February 8, 2021, the Council of the Berkeley Division (DIVCO) discussed the proposed replacement for the Presidential Policy, Business and Finance Bulletin, IS-12, informed by comments from our local committees on Academic Planning and Resource Allocation (CAPRA) and Computing and Information Technology (CIT). The committee comments are appended in their entirety.

The Berkeley Division generally supports the proposed replacement policy, and found the policy to be reasonable. Four points were brought up during the meeting:

1. The number of mandatory roles in the policy could be difficult to fill, especially in the current resource-constrained environment.
2. The need for clarity in the area of UC "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."
3. More clarification for Recovery Time Objectives (RTOs).
4. Conflated cost of downtime with cost of permanent loss

I draw your attention specifically to a point made by our Committee on Computing and Information Technology (CIT):

> While there is a tool with pointers to various resources to help individuals understand their compliance obligations, the Committee would like information to be woven into processes where that information is of vital necessity to compliance.

CIT also provided recommendations for communications strategies. Please refer to the enclosures.

Thank you for the opportunity to comment.

Sincerely,

Jennifer Johnson-Hanks

Jennifer Johnson-Hanks
Professor of Demography and Sociology
Chair, Berkeley Division of the Academic Senate

Enclosures

cc: Ronald Cohen, Vice Chair, Berkeley Division of the Academic Senate
Paul Fine, Chair, Committee on Academic Planning and Resource Allocation
Deirdre Mulligan, Chair, Committee on Computing and Information Technology
Jocelyn Surla Banaria, Executive Director, Berkeley Division of the Academic Senate
Deborah Dobin, Senate Analyst, Committee on Academic Planning and Resource Allocation

ACADEMIC
SENATE
BERKELEY

320 STEPHENS HALL
UNIVERSITY OF CALIFORNIA

February 3, 2021

PROFESSOR JENNIFER JOHNSON-HANKS
Chair, Berkeley Division of the Academic Senate

Re: CAPRA comments on Proposed Presidential Policy, Business and Finance Bulletin,
IS-12: IT Recovery

At today's meeting, CAPRA discussed the proposed *Presidential Policy, Business and Finance Bulletin, IS-12: IT Recovery*. This memo addresses issues of academic planning, budget, and resource allocation, consistent with the charge of CAPRA.

The IS-12 policy describes, at a very broad level, "appropriate governance, funding, design, development, testing, maintenance, protection, and procurement procedures" to ensure IT recovery and business continuity for the university in the event of a large-scale disruption. The last major update to the policy, prior to this one, was almost 15 years ago (July 2007).

Overall, CAPRA found the policy to be very reasonable. While it is necessarily prescriptive, it balances that need with pragmatic concerns. For example, while the goal is for each location and unit to achieve compliance quickly, it recognizes that this may not be immediately possible in many cases, and it defines an iterative process to work towards implementing the policies. In addition, it has a well-defined procedure to allow for exceptions, and it delegates much of the responsibility to the local institution (e.g. the campus).

The policy is defined at a sufficiently broad level that the committee does not have a lot of questions or comments about specifics. Nevertheless, the following comments/questions arose in reviewing the document:

1. The number of mandatory roles in the policy could be difficult to fill, especially in the current resource-constrained environment. It was not clear to us how many of these roles would represent new FTEs, as opposed to delegation to existing FTEs. What is the estimated annual cost to fulfill the mandatory roles as stated?
2. Section 1.2 states that UC "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." But it was unclear to us who exactly

determines value. Is there consultation with faculty, staff, and others who rely on these resources?

3. Section 4.2 lists RTOs (Recovery Time Objectives) for each of the five Recovery Levels (RL), ranging from 15 minutes (RL5) to 30 days (RL1). Presumably these RTOs represent scenarios under which most/all of our other services remain up — it would be unrealistic to envision that all RL5 resources could be recovered in 15 minutes (as the policy specifies) in the event of a major catastrophe that shut down everything. Perhaps the policy should make this clear by giving specific examples, such as the 2019 PG&E shutdown for fire prevention.
4. In Section 7.3, it appears that the RLs conflate the cost of downtime with the cost of permanent loss; only RL3 and above require off-site backup. Some resources, however, might be valuable but not immediately necessary. These resources could receive a low RL and thus not be backed up off site. (Note: it’s possible that IS-3, which we did not review, addresses this issue.)

Thank you for the opportunity to review the proposed policy. CAPRA finds it responsive to the university's needs in this changing and challenging technology environment, and endorses it.

With best regards,

Paul Fine, Chair
Committee on Academic Planning and Resource Allocation

Committee on Information Technology
Berkeley Div. of the Academic Senate

February 1, 2021

Division Chair Jennifer Johnson-Hanks
Berkeley Division of the Academic Senate
University of California

Re: Systemwide Review of Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Division Chair Jennifer Johnson-Hanks,

Thank you for the opportunity to comment on the New IS-12 policy. The Committee invited Allison Henry, Chief Information Security Office, and Professor Anthony Joseph, the campus Cyber-risk Responsible Executive, to discuss IS-12 and it's interaction to IS-3 at our December 14, 2020 meeting.

Many of the questions and concerns raised by the Committee focused on making sure faculty and students were provided with information about their new responsibilities and new workflows at relevant points. For example because IS-12 covers any project that has a data management plan the Committee discussed the need to provide information to researchers when they are applying for federally sponsored research, and when they are going through the human subjects research approval process at OPHS. While there is a tool with pointers to various resources to help individuals understand their compliance obligations, the Committee would like information to be woven into processes where that information is of vital necessity to compliance. For example, during grant proposals PIs should be alerted to the fact that their data management plan must conform with IS-12, that there are resources available on campus for IS-12 compliant storage so that they can build this into the proposal. Researchers should also be aware of charges and migration options. Sponsored projects and OPHS may both play an important role in providing "just in time" information to researchers that will ease the transition, maximize compliance and minimize confusion and labor. We also discussed the possibility of making sure IS-12 is discussed in PhD seminars, and in research labs and groups. The Committee wants to make sure faculty and researchers as a whole understand their responsibilities *and* the availability of tools to ease compliance.

The Committee offered a few concrete recommendations for communication, however, we expect that others on campus will be better able to develop detailed and effective communication strategies.

- Include information about IS-12 and compliant data management resources in the faculty newsletter about funding opportunities.
- Build awareness of IS-12 obligations and resources into the grant process and research approval process.
- Provide clear points of contact to help faculty members.
- Provide training to help faculty understand their new obligations and risk. We discussed an IS-12 awareness month; communications highlighting consequences flowing from compromises of research data.
- Educate students. Student Affairs could include information about IS-12 and resources as part of their onboarding.

The Information Security Office has been very quick to respond to issues that arose in our conversation. Allison Henry, CISO, recently shared a set of new resources and processes including the Draft Roles and Responsibility Policy which we are now reviewing. The Information Security Office also incorporated additional responsibilities that came up during a separate review of the IS-3 requirements which they summarized below.

Responses to Feedback:

- Updated and clarified the definition of a Unit, and added it to the Policy
- Developed a one-page Faculty guide - linked from the Policy
- Published a resource page for Unit Heads and Security Leads (UISLs) - linked from the Policy
- Compiled a UISL "job description" (one-page and expanded versions), including estimated time commitment - linked from the above resource page.
- Reviewed and updated data classification resources including "How to Classify Research Data", linked from the campus Data Classification Standard

Policy Additions:

1. Added UC's Minimum Security Standards to the list of information security standards that Workforce Members must follow. These will eventually be incorporated into our local Minimum Security Standards (MSSND and MSSEI).
2. Added links for guidance and clarification to Proprietor and Security Lead sections regarding record retention and classification, respectively;
3. Highlighted documentation requirements for Workforce Managers;
4. Clarified that all Users are responsible for responding to official reports of security incidents involving their systems or accounts;
5. Added resources to the "Related Documents and Policies" section.

The CIT will review these next week and provide any additional feedback.

Sincerely,
Deirdre K. Mulligan, Chair, Professor, School of Information
Michael Eisen, Professor, Mollecular and Cell Biology
Michael Laguerre, Professor, African American Studies
Kimiko Ryokai, Associate Professor, School of Information
Paul Schwartz, Professor, School of Law
Matthew Welch, Professor, Mollecular and Cell Biology
Avideh Zakhor, Professor, Electrical Engineering and Computer Science, UCACC rep
Parth Nobel, Representative, Associated Students of the University of California
Jenn Stringer, Chief Information Officer & Associate Vice Chancellor Information Technology (ex-officio)

UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

DAVIS DIVISION OF THE ACADEMIC SENATE
ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8502
(530) 752-2220
academicsenate.ucdavis.edu

February 17, 2021

Mary Gauvain
Chair, Academic Council

RE: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Mary,

The proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery was forwarded to all standing committees of the Davis Division of the Academic Senate. The Committee on Information Technology (CIT) responded.

CIT did not have any comments or concerns about the proposed policy. The Davis Division appreciates the opportunity to comment.

Sincerely,

Richard P. Tucker, Ph.D.
Chair, Davis Division of the Academic Senate
University of California, Davis

Enclosed: Davis Division Committee Responses

c: Hilary Baxter, Executive Director, Systemwide Academic Senate
Michael LaBriola, Assistant Director, Systemwide Academic Senate
Edwin M. Arevalo, Executive Director, Davis Division of the Academic Senate

UC DAVIS: ACADEMIC SENATE
COMMITTEE ON INFORMATION TECHNOLOGY

January 28, 2021

Richard Tucker
Chair, Davis Division of the Academic Senate

RE: Request for Consultation – Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Richard:

The Committee on Information Technology has reviewed the RFC – Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery and did not have any comments regarding this new policy.

Sincerely,

Matt Bishop

Matt Bishop
Chair, Committee on Information Technology

c: Edwin M. Arevalo, Executive Director, Davis Division of the Academic Senate

UCI University of California, Irvine

Academic Senate
Council on Research, Computing & Libraries
307 Aldrich Hall
Irvine, CA 92697-1325
(949) 824-7685
www.senate.uci.edu

February 2, 2021

JEFFREY BARRETT, CHAIR
ACADEMIC SENATE, IRVINE DIVISION

RE: Systemwide Review of Proposed Presidential Policy Business and Finance Bulletin IS-12 on IT Recovery

At its meeting on January 21, 2021, the Council on Research, Computing, and Libraries (CORCL) reviewed the proposed presidential policy business and finance bulletin IS-12 on IT Recovery.

The main objective of IS-12 requires IT resources to be recoverable regardless of the source of failure, whether natural or man-made. The policy includes guidance on governance, funding, design, development, testing, maintenance, protection, and procurement procedures. IS-12 follows the Business Continuity Plan (BCP) of the UC which was developed for safeguarding, security, and emergency management situations. This policy also defines the duties of workforce members responsible for the IT Recovery.

The policy designates five Recovery Levels for response time (RL1-RL5), ranging from 30 days for RL1 to 15 minutes for RL5. Additionally, it describes how the funding must be planned to meet recovery levels, recovery time objectives, recovery point objectives, and maximum tolerable downtime. The document details the responsibilities of Cyber-risk Responsible Executives (CRE), managers, unit leaders and other relevant individuals for implementation.

Overall, the Council observed that the IS-12 has important policy points for IT Recovery and has made substantial refinements to the previous policies. However, the Council identified a number of issues that warrant additional consideration:

- It is unclear how CREs will be appointed. Information on who is responsible for this process of selection, recruitment, and appointment is needed.
- Faculty involvement in the development of the policy and oversight of the operation is minimal. There should be more in-depth consultation with research faculty whose work may rely on this policy in case of disaster.
- The policy should include an organization chart. An organization chart will convey the operation and duties of each level of management in a succinct way.
- The policy does not consider how testing of the IT Recovery mechanisms proposed in IS-12 will be done. There should be clear guidance for having external review of policies by IT external security firms, including mock cyber-attacks to evaluate the vulnerability of the system.
- There should be a more coordinated systemwide effort to address cyber risk. This academic year alone, the Council will have reviewed three separate items relating to systemwide online issues. A more integrated approach would ensure that policies relate itself to other existing policies and should articulate how it fits in with the new environment.

Given the concerns above, the Council advises a reconsideration of the proposed policy.

On behalf of the Council,

Michele Guindani, Chair

c: Kate Brigman, Executive Director
Gina Anzivino, Assistant Director
Michelle Chen, CORCL Analyst
Brandon Haskey-Valerius, Senate Analyst

UCLA Academic Senate

February 9, 2021

Mary Gauvain
Chair, UC Academic Senate

Re: (Systemwide Senate Review) Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair Gauvain,

The Divisional Executive Board, councils, and committees appreciate the opportunity to review the proposed revision to (Systemwide Senate Review) Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery.

After discussion, members unanimously endorsed a motion to support the proposal as written with caveats about possible unintended consequences for privacy and security, as expressed in the attached committee statements.

Sincerely,

Shane White
Chair, UCLA Academic Senate

Encl.

Cc: Jody Kreiman, Vice Chair/Chair Elect, UCLA Academic Senate
Michael Meranze, Immediate Past Chair, UCLA Academic Senate
April de Stefano, Executive Director, UCLA Academic Senate

UCLA Academic Senate
Faculty Welfare Committee

January 26, 2021

Shane White, Chair
Academic Senate

Re: Systemwide Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12, IT Recovery

Dear Chair White,

At its meeting on January 19, 2021, the Faculty Welfare Committee discussed the Business and Finance Bulletin Proposed Policy on IT Recovery. Committee members offered the following comments.

Members agreed that data recovery is an issue related to faculty welfare. However, the committee was unable to assess the potential impact of the proposal because it was challenging to understand. Members are concerned over privacy, security, and data ownership, as well as access to faculty files which could lead to privacy violations when recovering data.

If you have any questions, please contact us via the Faculty Welfare Committee's interim analyst, Elizabeth Feller, at efeller@senate.ucla.edu.

Sincerely,

Huiying Li, Chair
Faculty Welfare Committee

cc: Jody Kreiman, Vice Chair/Chair Elect, Academic Senate
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Interim Analyst, Faculty Welfare Committee
Members of the Faculty Welfare Committee

UCLA Academic Senate
Committee on Teaching

January 12, 2021

To: Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12IT Recovery

Dear Chair White,

The Committee on Teaching discussed at its meeting on January 12, 2021, the Proposed Presidential Policy, Business and Finance Bulletin, IS-12IT Recovery. COT does not wish to opine, as the inaccessibility of the report for a general audience made it difficult to review effectively.

If you have any questions, please do not hesitate to contact me at collett@soc.ucla.edu or Academic Senate Policy Analyst Renee Rouzan-Kay at rrouzankay@senate.ucla.edu.

Sincerely,

Jessica L Collett

Jessica L. Collett, Chair
Committee on Teaching

cc: Shane White, Academic Senate, Chair
Jody Kreiman, Academic Senate, Vice Chair/ Chair- Elect
Michael Meranze, Academic Senate, Immediate Past Chair
April de Stefano, Academic Senate, Executive Director
Members of the Committee on Teaching

UCLA Academic Senate
Council on Planning & Budget

December 15, 2020

Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 7, 2020, the Council on Planning and Budget (CPB) had an opportunity to review and discuss the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members offered the following comments.

Members expressed some frustration at the language and acronyms on the policy, which they described as dense, not useful for non-experts, and hard to understand. Members wondered what would be involved in carrying out these new requirements. How much of that already exists and is being done at UCLA? What does this policy mean for faculty at UCLA who teach and do research on and off-campus? What would it mean for them to recover their information? Much of what faculty do may come late in the recovery process.

Based on the information provided, it is difficult to discern whether it would be fiscally burdensome to face the costs. Will UCLA need to increase its IT services to carry out this policy? Additionally, how does it interact with research? It might be an added complication in addition to existing rules about privacy. It would be helpful to understand the scope and breadth of this policy. Moreover, the centralization of systems and operations may cause them to fail. Members also mentioned that we should make sure that we are thinking of the technology infrastructure to pursue goals that we are interested in at the UCLA campus.

If you have any questions for us, please do not hesitate to contact me at groeling@comm.ucla.edu or via the Council's analyst, Elizabeth Feller, at efeller@senate.ucla.edu.

Sincerely,

Tim Groeling, Chair
Council on Planning and Budget

cc: Jody Kreiman, Vice Chair/Chair-Elect, Academic Senate
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Principal Policy Analyst, Council on Planning and Budget
Members of the Council on Planning and Budget

UCLA Academic Senate
Committee on Academic Freedom

December 14, 2020

To: Shane White, Chair
Academic Senate

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 10, 2020, the Committee on Academic Freedom reviewed and discussed the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 Recovery.

Committee members were supportive of the policy, but had some follow-up questions:

- Would the proposed IT recovery policy require faculty to store research data on UCLA servers? If so, would there be exceptions, for instance if faculty doing research about the university want to store data on a non-UCLA server? What about faculty using national secrets data that needs to be kept on specially secured servers, or faculty doing clinical work, in which they want to keep the data secure for client confidentiality reasons?
- How would the proposed IS-12 IT Recovery policy interact with the data security requirements imposed by Institutional Review Boards (IRBs) and, specifically when the data includes human subjects?

Thank you for the opportunity to review and comment on this proposal. If you have any questions, please do not hesitate to contact me at volokh@law.ucla.edu or the Committee on Academic Freedom Analyst Taylor Lane Daymude at tlanedaymude@senate.ucla.edu.

Sincerely,

Eugene Volokh

Professor Eugene Volokh, Chair
Committee on Academic Freedom

UCLA Academic Senate
Council on Research

December 11, 2020

Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 2, 2020, the Council on Research (COR) had an opportunity to review the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members were in support of the policy and offered no additional comments.

If you have any questions for us, please do not hesitate to contact me at julianmartinez@mednet.ucla.edu or via the Council's analyst, Elizabeth Feller, at efeller@senate.ucla.edu,or x62470.

Sincerely,

Julian Martinez, Chair
Council on Research

cc: Jody Kreiman, Vice Chair/Chair-Elect,
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Principal Policy Analyst, Council on Research
Members of the Council on Research

UCLA Academic Senate

Committee on Data, Information Technology, and Privacy

December 4, 2020

To: Shane White, Chair
Academic Senate

From: Susan Cochran, Chair
Committee on Data, Information Technology, and Privacy

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

At its meeting on December 3, 2020, the Committee on Data, Information Technology, and Privacy (CDITP) reviewed and discussed the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members found the proposed revisions to the policy to be straightforward and offered no additional comments.

Thank you for the opportunity to review and comment.

UNIVERSITY OF CALIFORNIA, MERCED

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

OFFICE OF THE ACADEMIC SENATE, MERCED DIVISION
ROBIN DELUGAN, CHAIR, DIVISIONAL COUNCIL

UNIVERSITY OF CALIFORNIA, MERCED

February 17, 2021

To: Mary Gauvain, Chair, Academic Council

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

The Merced Division Senate and School Executive Committees were invited to comment on the proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Comments were received from the Committee on Academic Planning and Resource Allocation (CAPRA). They are appended for your consideration.

The UC Merced Division sees the importance of updating IS-12 to reflect up-to-date technology references, a uniform method to meet UC's current recovery needs and a method for local governance; and for providing guidance to help UC locations plan for IT recovery.

For clarification, the policy could address how IT recovery priorities are established, the allocation of funding to recovery efforts, who sets the funding priority for the campus, what happens when the Cyber-Risk Responsible Executive does not receive the necessary funds, and what occurs if a campus is unable to recover its systems. The policy points to necessary discussions about how IT priorities are established on campus.

The Merced Division thanks you for the opportunity to review and offer comments on this policy.

Sincerely,

Robin M. DeLugan

Robin DeLugan
Chair, Divisional Council
UC Merced

Cc: DivCo Members
Hilary Baxter, Systemwide Senate Executive Director
Michael LaBriola, Systemwide Senate Assistant Director
UCM Senate Office

Encl. 2

UNIVERSITY OF CALIFORNIA, MERCED

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

ACADEMIC SENATE, MERCED DIVISION
COMMITTEE ON ACADEMIC PLANNING AND RESOURCE ALLOCATION
PATTI LIWANG, CHAIR
pliwang@ucmerced.edu

UNIVERSITY OF CALIFORNIA, MERCED
5200 NORTH LAKE ROAD
MERCED, CA 95343

December 3, 2020

To: Robin DeLugan, Chair, Division Council

From: Patricia LiWang, Chair, Committee on Academic Planning and Resource Allocation (CAPRA) Patricia J. LiWang

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

CAPRA has reviewed the proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. CAPRA appreciates that the proposed policy allows each campus to determine the scope and procedures for IT recovery. Each campus is to appoint a Cyber-risk Responsible Executive (CRE) who will be responsible for leading the effort to recover systems following an interruption.

However, CAPRA is concerned that the policy is unclear on the following points: the allocation of funding to recovery efforts, who sets the funding priority for the campus, what happens when the CRE does not receive the necessary funds, and occurs if a campus is unable to recover its systems.

As a general comment, CAPRA recommends that campus leadership address how IT priorities are established at UC Merced.

We appreciate the opportunity to opine.

cc: Senate Office

UNIVERSITY OF CALIFORNIA, RIVERSIDE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED• RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

CHAIR, ACADEMIC SENATE
RIVERSIDE DIVISION
UNIVERSITY OFFICE BUILDING, RM 225

JASON STAJICH
PROFESSOR OF MICROBIOLOGY & PLANT PATHOLOGY
RIVERSIDE, CA 92521-0217
TEL: (951) 827-6193
EMAIL: JASON.STAJICH@UCR.EDU

February 16, 2021

Mary Gauvain, Chair, Academic Council
1111 Franklin Street, 12th Floor
Oakland, CA 94607-5200

RE: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair Gauvain,

The Riverside Division discussed the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery and I transmit the comments provided by the Senate committees' review.

Sincerely yours,

Jason Stajich
Professor of Microbiology & Plant Pathology and Chair of the Riverside Division

CC: Michael LaBriola, Assistant Director of the Academic Senate
Hilary Baxter, Executive Director of the Academic Senate
Cherysa Cortez, Executive Director of UCR Academic Senate

UC RIVERSIDE

Academic Senate

COMMITTEE ON FACULTY WELFARE

December 17, 2020

To: Jason Stajich
Riverside Division Academic Senate

From: Patricia Morton, Chair
Committee on Faculty Welfare

Re: [Systemwide Review] Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

The Committee on Faculty Welfare met on December 15, 2020 to consider the proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. CFW sees a tremendous impact on faculty welfare if the campus does not have a fully implemented IT recovery plan. Otherwise CFW feels this is not within the committee's purview and has no further comment.

UC RIVERSIDE

Academic Senate

January 29, 2021

To: Jason Stajich, Chair
Riverside Division

From: Alejandra Dubcovsky, Chair
Committee on Library and Information Technology

RE: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

The committee reviewed the proposal and received input from different members of the IT department. Overall, the committee supports the policies recommended by the report and seeks to underscore the importance of a systemwide Recovery Plan. Since the policy is sound and an IT recovery plan seems essential to the functioning of a research university, it is important to emphasize the issue of funding. Sufficient funding should be allocated for this policy to succeed and that funding should take into account the different revenues/staff needs/support of ITS services across the UC's.

UC RIVERSIDE

Academic Senate

PLANNING & BUDGET

January 22, 2021

To: Jason Stajich, Chair
Riverside Division

From: Katherine Kinney, Chair Katherine Kinney
Committee on Planning and Budget

RE: [Systemwide Review] Proposed Policy: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

The Committee on Planning & Budget (P&B) discussed the proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery at their January 19, 2021 meeting. P&B agreed the IT security is a crucial issue but were concerned that the scale of this proposal would likely be prohibitively expensive given that no new funding appears to be attached to the initiative and recommended a cost/benefit analysis of the proposal be conducted.

UC SANTA BARBARA

Academic Senate
Susannah Scott, Chair
Shasta Delp, Executive Director

1233 Girvetz Hall
Santa Barbara, CA 93106-3050
http://www.senate.ucsb.edu

February 19, 2021

To: Mary Gauvain, Chair
Academic Senate

From: Susannah Scott, Chair
Santa Barbara Division Susannah L Scott

Re: Systemwide Review of the Proposed Presidential Policy – Business and Finance Bulletin,
IS-12 IT Recovery

The Santa Barbara Division distributed the Proposed Presidential Policy to the Council on Planning and Budget (CPB), Committee on Research Policy and Procedures (CRPP), and the Committee on Information Technology (CIT). Both reviewing groups raised a number of serious concerns regarding the generic nature of the proposed policy, the absence of a cost-benefit analysis, and the budgetary implications of a new unfunded mandate. The attached responses are included for your consideration.

We thank you for the opportunity to opine.

UNIVERSITY OF CALIFORNIA
ACADEMIC SENATE
SANTA BARBARA DIVISION
Council on Planning & Budget

December 21, 2020

To: Susannah Scott, Divisional Chair
UCSB Academic Senate

From: Douglas Steigerwald, Chair
Council on Planning & Budget

Doug Steigerwald

Re: Proposed IT Recovery Policy, Business & Finance Bulletin, IS-12

The Council on Planning & Budget (CPB) has reviewed the Proposed UCOP Presidential Policy on Information Technology (IT) Recovery, Business & Finance Bulletin, IS-12, the aim of which is to provide an iterative model for IT Disaster Recovery. IS-12 is based on the policy IS-3 /CSF, which is concerned with data security and storage but not specifically with disaster recovery.

The IS-12 policy provides a framework for IT recovery that, once ratified, all campuses will be required to comply with. Specifics on the implementation of IS-12 are, however, the decision of individual campuses. CPB particularly welcomes the new policy measures to enable the provision of cloud-based data back-up but is concerned that the policy contains no language focused on faculty research and archiving.

The implementation of IS-12 will place an additional workload on IT management, which is already stretched in complying with IS-3. It is likely that additional staff/funding will be required. A document describing "best practices" to serve as role models that campus teams can model from, would be especially useful.

CPB supports policy IS-12: IT Recovery

cc: Shasta Delp, Academic Senate Executive Director

Academic Senate
Santa Barbara Division

February 8, 20201

To: Susannah Scott, Divisional Chair
Academic Senate

From: Forrest Brewer, Chair Forrest Brewer
Committee on Research Policy and Procedures

James Frew, Chair
Committee on Information Technology

Re: Proposed Presidential Policy - Business and Finance Bulletin, IS-12 IT Recovery

The Committee on Research Policy and Procedures (CRPP) reviewed this policy at its meeting of 1/22/21 and the Committee on Information Technology reviewed this policy at its meeting, joined by the Chair of CRPP, on 1/29/21.

While the committees acknowledge the need to back up vulnerable and critical research information, they jointly feel that this policy leaves out or poorly defines some rather significant variables, specifically the amount of unprotected or poorly protected data on campus and the appropriate recovery level. They felt that more data was needed to produce a rigorous cost benefit analysis in order to offer deeper insights.

Both committees are concerned with the level of jargon involved in the policy and the vague details it offers regarding the impacts to faculty. They felt it would be helpful for subsequent drafts to provide more detailed information or examples, particularly for those that are not IT experts. The document describes generic response policy without any attempt to identify specific UC policy or organizational requirements that make it specific to UC. In particular, in a document of such size, specific data set types might be identified as examples for the currency evaluation on campus. Cost/benefit analysis is at the core of risk abatement, so such a policy ought to at least template data census and currency evaluations.

Both wanted to see more details related to a strategy for data collection and retention. They are concerned this is a significant unfunded mandate coming to campuses that are already bracing for cuts to their operating budgets, though the groups note and appreciate that an exception process, which allows for cost-benefit justification, exists to exclude specific data sets from the mandate.

Additionally, input from the acting CIO indicates that much of the policy duplicates what is contained in IS-3. The committee members noted that the role of CIO is absent from this policy and felt the leadership designations could be clearer.

CC: Shasta Delp, Executive Director, Academic Senate

UNIVERSITY OF CALIFORNIA, SANTA CRUZ

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

1156 HIGH STREET
SANTA CRUZ, CALIFORNIA 95064

Office of the Academic Senate
SANTA CRUZ DIVISION
125 CLARK KERR HALL
(831) 459 - 2086

February 12, 2021

Mary Gauvain, Chair
Academic Council

Re: Systemwide Review of Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Mary,

The Santa Cruz Division has reviewed and discussed the proposed replacement for the Presidential Policy, Business and Finance Bulletin, IS-12. Our Committees on Information Technology (CIT), Planning and Budget (CPB), and Rules, Jurisdiction, and Elections (RJE) have responded. Overall, the majority of responding committees saw the proposed replacement as positive, in that it provides individual campuses with the ability to have control over implementation, and will encourage the UC community to prepare for recovery and business continuity. However, questions and concerns were raised about the policy's implementation, particularly with regards to roles and responsibilities.

The need to further clarify roles and communication processes is clear. The replacement policy references Units and Unit heads. However, it is not clear whether the location business continuity plan would use academic divisions, or academic departments, as the natural notion of "Units." Further, it is not clear to whom Unit heads should report in an emergency situation. Responding committees suggested that divisions might be a better designation for units than departments, as deans have more authority to allocate funds and personnel in support of this policy than department chairs.

Concerns were additionally raised about the role and workload of the Cyber-risk Responsible Executive (CRE). The proposed policy places the bulk of responsibility on the CRE, including the responsibility of appointing duties, governance, planning, testing, and securing funding. As such, there is a question as to whether the CRE can be successful in recovering IT properties in an emergency situation. Further, the exception process noted in the revision vests much authority in the CRE. Responding committees questioned whether a Unit head such as a dean might be better positioned to make such decisions.

Further clarification is also needed with regards to terms and implementation criteria for new features in the policy. The terms "immediate" and "critical" used throughout the document should be differentiated, as should the major differences between the full compliance method in 1.3.1 and the iterative method in 1.3.2. Also, implementation criteria for the iterative approach should be further clarified, such as expected timelines for implementation, whether there will be any differences in timelines based on different Recovery Levels, and whether the CRE is the proper person to have jurisdiction over iterative processes. Clarification may also be needed on whether UC-managed national laboratories will be subject to the same policy as the campuses and Office of the President.

The Santa Cruz Division further notes that unlike the recently revised IS-13: Electronic Information Security policy, the proposed IS-12 IT Recovery replacement policy does not specifically speak to research data, other than in Section VIII. Frequently Asked Questions. As research is a cornerstone of both the faculty profession and the UC mission, the Division encourages the consideration of research data in all policies regarding IT recovery and business continuity.

Thank you for the opportunity to comment on this proposed revision.

Sincerely,

David Brundage, Chair
Academic Senate
Santa Cruz Division

cc: Brent Haddad, Chair, Committee on Information Technology
Dard Neuman, Chair, Committee on Planning and Budget
Kenneth Pedrotti, Chair, Committee on Rules, Jurisdictions, and Elections

UNIVERSITY OF CALIFORNIA, SAN DIEGO UCSD

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

OFFICE OF THE ACADEMIC SENATE

9500 GILMAN DRIVE
LA JOLLA, CALIFORNIA
92093-0002

TELEPHONE: (858) 534-364
FAX: (858) 534-4528

January 20, 2021

Professor Mary Gauvain
Chair, Academic Senate
University of California
VIA EMAIL

Re: UC Presidential Policy, Business and Financial Bulletin, IS-12, IT Recovery

Dear Professor Gauvain,

The proposed revisions to UC Presidential Policy, Business and Financial Bulletin, IS-12, IT Recovery, were distributed to San Diego Divisional Senate standing committees and discussed at the January 11, 2021 Divisional Senate Council meeting. Senate Council had no objections to the proposed revision.

Suggestions for improvement to policy text include providing clearer definitions and examples for keywords such as *Unit Head*, *IT recovery teams* and *serious violations and consequences*, as well as providing clarification on which party is responsible for recovery under the new policy and the Chancellor's review in this process. While adopting cloud technologies creates opportunities for increased IT recovery, this can substantially increase costs to the campus if they are not disciplined in utilizing a risk-based approach or if policy is over-interpreted over time, and this also creates additional contract and IT architecture complexity. The policy does not appear to address cyber-attacks or industrial espionage on the University. The iterative approach may be considered too lax, especially since there is no set time limit to use this approach.

Further follow-up regarding the need for campuses to identify the linkages between cloud technology contracts and IS-12 is recommended. UCOP IT (or a working group of the CIO Committee, the ITLC) should review these contracts and identify gaps between them and the revised IS-12 policy and generate the necessary documentation to fulfill the related campus IS-12 policy requirements.

The responses from the Divisional Committee on Academic Information Technology and the Committee on Planning and Budget are attached.

Sincerely,

Steven Constable

Steven Constable
Chair
San Diego Divisional Academic Senate

Attachments

cc: Tara Javidi, Vice Chair, San Diego Divisional Academic Senate
Ray Rodriguez, Director, San Diego Divisional Academic Senate
Hilary Baxter, Executive Director, UC Systemwide Academic Senate

ACADEMIC SENATE: SAN DIEGO DIVISION
UCSD, LA JOLLA, CA 92093-0002
(858) 534-3640
FAX (858) 534-4528

January 4, 2021

PROFESSOR STEVEN CONSTABLE, Chair
Academic Senate, San Diego Division

SUBJECT: UC IS-12 IT Recovery Policy

Dear Chair Constable,

At its December 3, 2020 meeting, the Committee on Academic Information Technology (CAIT) reviewed the UC IS-12 IT Recovery Policy. A sub-committee of CAIT was formed to review the policy more in-depth. The CAIT sub-committee and CAIT have no major objections to the proposal. We have several suggestions for improvement.

Some of the policy text can be improved:

- Unit Head should be more clearly defined, perhaps with concrete examples, or linkages to the definition in IS-3 provided in place or in the appendix.
- The policy asks for review with the campus Chancellor. The purpose of that review and the Chancellor expectations should be clarified.
- In sections 3.1.and 3.2 the distinction between IT recovery teams, local recovery team and unit recovery team could be made clearer, perhaps with concrete examples either in place or in the appendix.
- In section 1.7.2, the policy could me improve with clearer definitions or concrete examples for serious violations and consequences, particularly the differences between educational and employment consequences, since student workers may fall into both categories.

We have recommendations regarding possible follow-up actions once the policy is in place.

With regard to cloud technologies most of the topics of practical concern in the policy, including recovery levels, are addressed by cloud providers as expressed in contract terms including but not limited to Microsoft, Amazon, Google, Oracle, Instructure and others. Some these contracts are managed out of the Office of the President. While campuses use these services from these providers under these contracts, campuses will need to identify the linkages between those contracts and IS-12, OP IT (or a working group of the CIO Committee, the ITLC) should review these contracts and identify gaps between them and the revised IS-12 policy and generate the necessary documentation to fulfill the on related campus IS-12 policy requirements.

In addition, in theory and in practice, cloud technologies provide many options for IT recovery, and much more so than most on-premise IT environments. While we can and should improve IT recovery, adopting cloud options creates an opportunity and some challenges. The opportunity is that we can 'raise the bar' on IT recovery and improve an institutions recovery capability. The challenge is two-fold. First, raising the bar can substantially increase costs to the institution if the campus is not disciplined in utilizing a risk-based approach or if policy is over-interpreted over time. Second, raising the bar creates additional contract and IT architecture complexity requiring tight coordination between the Office of the President and campuses. For example, in a cloud-only environment, on-premise risk rapidly shrinks (since on-premise systems are reduced or eliminated). However, risk now moves to regional and national network architecture risk. Regional network planning will play a more important role in IT recovery.

Future revisions of, or addendums or additional work products added to this policy should contain further guidance regarding how OP contracts and IS-12 compliance are addressed and should further elucidate how adoption of cloud technologies may require policy revisions or FAQ additions. We recommend a work group of some kind, perhaps from the ITLC, be tasked to address these issues.

Sincerely,

Ian Galton, Chair
Committee on Academic Information Technology

cc: T. Javidi
R. Rodriguez
B. Simon

December 17, 2020

STEVEN CONSTABLE, CHAIR
Academic Senate, San Diego Division

SUBJECT: UC IS-12 IT Recovery Policy

The Committee on Planning and Budget (CPB) reviewed the UC IS-12 IT Recovery Policy at its December meeting. The CPB endorsed the proposed plans. However, with minimal budgetary information, the committee cannot provide a more specific assessment. Additional contextual information is necessary to fully understand how the campus is preparing for these programs and how this information may be used in the future.

The plan does not appear to directly address cyber-attacks or industrial espionage on the university. Certainly, as recent events at UCSF demonstrate, this is an area of increasing concern.

Would the allowed use of an iterative approach be considered too lax in view of the recent events? Furthermore, there's no set time limit for the use of the iterative approach. Units facing financial constraints might choose to adopt the approach indefinitely.

The definitions of "unit" and "unit head" follow the 2018 document "Insurance Programs for Institutional Information Technology Resources." It appears the new revision shifts responsibility for recovery from departments to unit heads? Is this correct and could responsibility be clarified?

Sincerely,

Kwai Ng, Chair
Committee on Planning & Budget

cc: T. Javidi

UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

UNIVERSITY COMMITTEE ON ACADEMIC COMPUTING
AND COMMUNICATIONS (UCACC)
David Robinowitz, Chair
Email: David.Robinowitz@ucsf.edu

ACADEMIC SENATE
University of California
1111 Franklin Street, 12th Floor
Oakland, California 94607

February 17, 2021

MARY GAUVAIN, CHAIR
ACADEMIC COUNCIL

Re: UCACC's Comments on IS-12: IT Recovery Policy

Dear Chair Gauvain,

UCACC was first introduced to plans to revise the IS-12, IT Recovery policy (previously known as Business and Finance Bulletin, Continuity Planning and Disaster Recovery), in February, 2019. Systemwide Policy Director Robert Smith has joined each UCACC meeting since then to provide updates on the revision plan and progress – a total of nine meetings over two years. 2019-20 UCACC Chair Anthony Joseph (UC Berkeley) was one of the policy revision's three "executive sponsors."

The IS-12 revision is described as a 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, and adopt a standards-based approach to IT Recovery. The name was changed from "Continuity Planning and Disaster Recovery" to "IT Recovery" to align with UC's overall business continuity and disaster preparedness planning. Additional features were added to support local governance, budgeting, and risk management. The policy addresses UC's ability to recover data and supporting systems due to power loss, floods, fires, earthquakes, and pandemics, as well as to cyber threats like ransomware. The revised policy provides guidance to help UC locations plan for IT recovery in all of these situations. The policy was also updated to align with the recent revision of IS-3, the Electronic Information Security Policy.

Although IS-12 is primarily directed toward IT professionals, there are some implications for faculty, for example when a PI sets up an IT recovery plan for a research laboratory. In general, UCACC feels that faculty need to be aware of their data security responsibilities, but with the support, resources, and backing of the local administration.

UCACC greatly appreciates the conscientious and consultative process undertaken by ITS in revising this policy.

Sincerely,
/s/
David Robinowitz, Chair
University Committee on Academic Computing and Communications

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

UNIVERSITY COMMITTEE ON FACULTY WELFARE (UCFW)
Shelley Halpain, Chair
Shalpain@ucsd.edu

Assembly of the Academic Senate
1111 Franklin Street, 12th
Oakland, CA 94607-5200

February 17, 2021

MARY GAUVAIN, CHAIR
ACADEMIC COUNCIL

RE: Proposed Revisions to Presidential Policy, Business and Finance Bulletin, IS-12: IT Recovery

Dear Mary,

The University Committee on Faculty Welfare (UCFW) has discussed the proposed revisions to Presidential Policy, Business and Finance Bulletin, IS-12: IT Recovery, and we have several concerns. While we appreciate the need to update policies given the rapid pace of change in the technology realm, these proposed revisions go too far in non-technical areas. We note that the proposed revisions now include penalties for supervisors whose team may be found to be in violation. This prescription of penalties by the administration requires clarification, as it may contradict established Senate disciplinary processes and policies. Guidelines should include specific scenarios, as well.

We also note that there may be several unfunded mandates implied by the new regulatory requirements. Where will back-up data be stored, and at whose cost; will costs be transferred to individual investigators or research groups? How much will new CRE staff cost, and where will they be housed? Importantly, the compliance onus and time spent are also lost costs that impact the productivity of faculty, trainees, and staff.

UCFW looks forward to a more targeted policy draft that includes recognition of Senate processes and addresses issues of cost and time.

Sincerely,

Shelley Halpain, UCFW Chair

Copy: UCFW
Hilary Baxter, Executive Director, Academic Senate
Robert Horwitz, Academic Council Vice Chair

UNIVERSITY OF CALIFORNIA, ACADEMIC SENATE

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

UNIVERSITY COMMITTEE ON RESEARCH POLICY (UCORP)
Richard Desjardins, Chair
Email: desjardins@ucla.edu

University of California
Academic Senate
1111 Franklin Street, 12th Fl.
Oakland, California 94607

February 17, 2021

MARY GAUVAIN
CHAIR, ACADEMIC COUNCIL

RE: Academic Planning Council Faculty Salary Scales Task Force Report and Recommendations

Dear Mary,

UCORP discussed the **Proposed Revisions to Presidential Policy on IT Recovery** at its meeting on February 8th. Committee members felt that the policy is primarily aimed at IT professionals, who presumably would have more insight into some of its more opaque directives. Nevertheless, UCORP members had the following comments based on conversations with their local committees:

- The section on roles and responsibility is overly complex, including the need to identify recovery and security leads
- The policy is unclear about remedies for cyberattacks and lacks a unified framework regarding IT recovery systemwide
- There is no mention of overlap with other initiatives at the systemwide level
- It is not clear whether there are penalties for not following the policy
- The policy does not include information about how to determine the cost of violations
- There should be faculty input in the oversight of this policy

UCORP appreciates the opportunity to comment on this policy.

Sincerely,

Richard Desjardins
Chair, University Committee on Research Policy

UCLA Academic Senate

February 9, 2021

Mary Gauvain
Chair, UC Academic Senate

Re: (Systemwide Senate Review) Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair Gauvain,

The Divisional Executive Board, councils, and committees appreciate the opportunity to review the proposed revision to (Systemwide Senate Review) Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery.

After discussion, members unanimously endorsed a motion to support the proposal as written with caveats about possible unintended consequences for privacy and security, as expressed in the attached committee statements.

Sincerely,

Shane White
Chair, UCLA Academic Senate

Encl.

Cc: Jody Kreiman, Vice Chair/Chair Elect, UCLA Academic Senate
Michael Meranze, Immediate Past Chair, UCLA Academic Senate
April de Stefano, Executive Director, UCLA Academic Senate

UCLA Academic Senate
Faculty Welfare Committee

January 26, 2021

Shane White, Chair
Academic Senate

Re: Systemwide Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12, IT Recovery

Dear Chair White,

At its meeting on January 19, 2021, the Faculty Welfare Committee discussed the Business and Finance Bulletin Proposed Policy on IT Recovery. Committee members offered the following comments.

Members agreed that data recovery is an issue related to faculty welfare. However, the committee was unable to assess the potential impact of the proposal because it was challenging to understand. Members are concerned over privacy, security, and data ownership, as well as access to faculty files which could lead to privacy violations when recovering data.

If you have any questions, please contact us via the Faculty Welfare Committee's interim analyst, Elizabeth Feller, at efeller@senate.ucla.edu.

Sincerely,

Huiying Li, Chair
Faculty Welfare Committee

cc: Jody Kreiman, Vice Chair/Chair Elect, Academic Senate
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Interim Analyst, Faculty Welfare Committee
Members of the Faculty Welfare Committee

UCLA Academic Senate
Committee on Teaching

January 12, 2021

To: Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12IT Recovery

Dear Chair White,

The Committee on Teaching discussed at its meeting on January 12, 2021, the Proposed Presidential Policy, Business and Finance Bulletin, IS-12IT Recovery. COT does not wish to opine, as the inaccessibility of the report for a general audience made it difficult to review effectively.

If you have any questions, please do not hesitate to contact me at collett@soc.ucla.edu or Academic Senate Policy Analyst Renee Rouzan-Kay at rrouzankay@senate.ucla.edu.

Sincerely,

Jessica L Collett

Jessica L. Collett, Chair
Committee on Teaching

cc: Shane White, Academic Senate, Chair
Jody Kreiman, Academic Senate, Vice Chair/ Chair- Elect
Michael Meranze, Academic Senate, Immediate Past Chair
April de Stefano, Academic Senate, Executive Director
Members of the Committee on Teaching

UCLA Academic Senate
Council on Planning & Budget

December 15, 2020

Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 7, 2020, the Council on Planning and Budget (CPB) had an opportunity to review and discuss the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members offered the following comments.

Members expressed some frustration at the language and acronyms on the policy, which they described as dense, not useful for non-experts, and hard to understand. Members wondered what would be involved in carrying out these new requirements. How much of that already exists and is being done at UCLA? What does this policy mean for faculty at UCLA who teach and do research on and off-campus? What would it mean for them to recover their information? Much of what faculty do may come late in the recovery process.

Based on the information provided, it is difficult to discern whether it would be fiscally burdensome to face the costs. Will UCLA need to increase its IT services to carry out this policy? Additionally, how does it interact with research? It might be an added complication in addition to existing rules about privacy. It would be helpful to understand the scope and breadth of this policy. Moreover, the centralization of systems and operations may cause them to fail. Members also mentioned that we should make sure that we are thinking of the technology infrastructure to pursue goals that we are interested in at the UCLA campus.

If you have any questions for us, please do not hesitate to contact me at groeling@comm.ucla.edu or via the Council's analyst, Elizabeth Feller, at efeller@senate.ucla.edu.

Sincerely,

Tim Groeling, Chair
Council on Planning and Budget

cc: Jody Kreiman, Vice Chair/Chair-Elect, Academic Senate
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Principal Policy Analyst, Council on Planning and Budget
Members of the Council on Planning and Budget

UCLA Academic Senate
Committee on Academic Freedom

December 14, 2020

To: Shane White, Chair
Academic Senate

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 10, 2020, the Committee on Academic Freedom reviewed and discussed the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 Recovery.

Committee members were supportive of the policy, but had some follow-up questions:

- Would the proposed IT recovery policy require faculty to store research data on UCLA servers? If so, would there be exceptions, for instance if faculty doing research about the university want to store data on a non-UCLA server? What about faculty using national secrets data that needs to be kept on specially secured servers, or faculty doing clinical work, in which they want to keep the data secure for client confidentiality reasons?
- How would the proposed IS-12 IT Recovery policy interact with the data security requirements imposed by Institutional Review Boards (IRBs) and, specifically when the data includes human subjects?

Thank you for the opportunity to review and comment on this proposal. If you have any questions, please do not hesitate to contact me at volokh@law.ucla.edu or the Committee on Academic Freedom Analyst Taylor Lane Daymude at tlanedaymude@senate.ucla.edu.

Sincerely,

Eugene Volokh

Professor Eugene Volokh, Chair
Committee on Academic Freedom

UCLA Academic Senate
Council on Research

December 11, 2020

Shane White, Chair
Academic Senate

Re: Systemwide Senate Review: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Chair White,

At its meeting on December 2, 2020, the Council on Research (COR) had an opportunity to review the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members were in support of the policy and offered no additional comments.

If you have any questions for us, please do not hesitate to contact me at julianmartinez@mednet.ucla.edu or via the Council's analyst, Elizabeth Feller, at efeller@senate.ucla.edu,or x62470.

Sincerely,

Julian Martinez, Chair
Council on Research

cc: Jody Kreiman, Vice Chair/Chair-Elect,
Michael Meranze, Immediate Past Chair, Academic Senate
April de Stefano, Executive Director, Academic Senate
Elizabeth Feller, Principal Policy Analyst, Council on Research
Members of the Council on Research

UCLA Academic Senate

Committee on Data, Information Technology, and Privacy

December 4, 2020

To: Shane White, Chair
Academic Senate

From: Susan Cochran, Chair
Committee on Data, Information Technology, and Privacy

Re: Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

At its meeting on December 3, 2020, the Committee on Data, Information Technology, and Privacy (CDITP) reviewed and discussed the Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery. Members found the proposed revisions to the policy to be straightforward and offered no additional comments.

Thank you for the opportunity to review and comment.

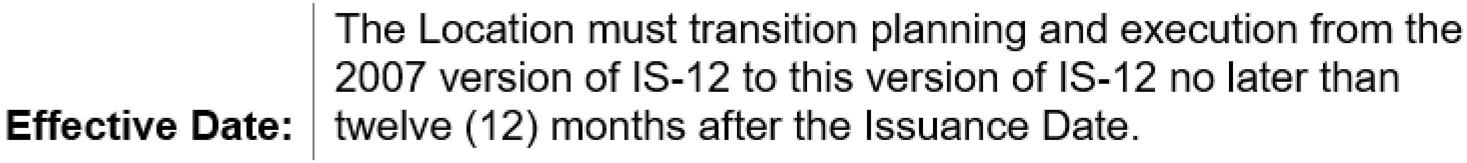
IS-12 IT Recovery Policy Key Features

SUMMARY

ROBERT SMITH

ROBERT.SMITH@UCOP.EDU

Effective Date

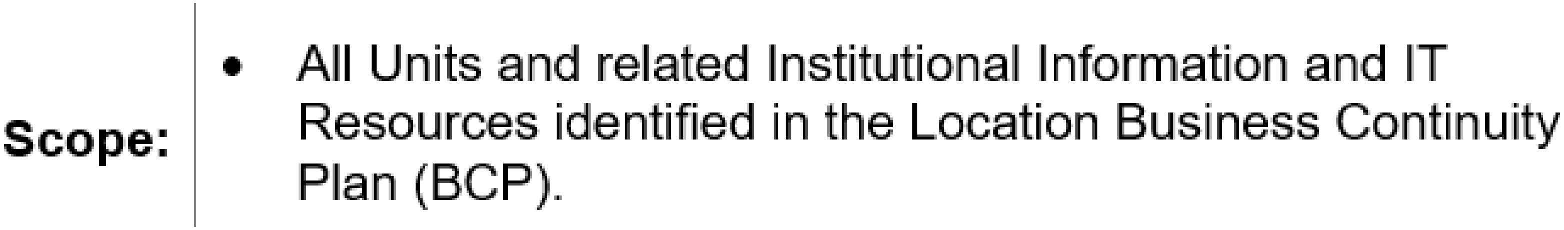


Effective Date: The Location must transition planning and execution from the 2007 version of IS-12 to this version of IS-12 no later than twelve (12) months after the Issuance Date.

12 Months to move to the new iterative model!

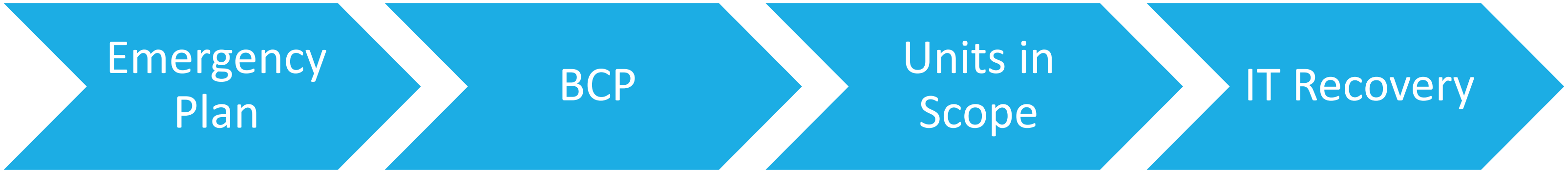
Resets the compliance clock!

Limited scope based on Location BCP



Scope:

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



Emergency Plan

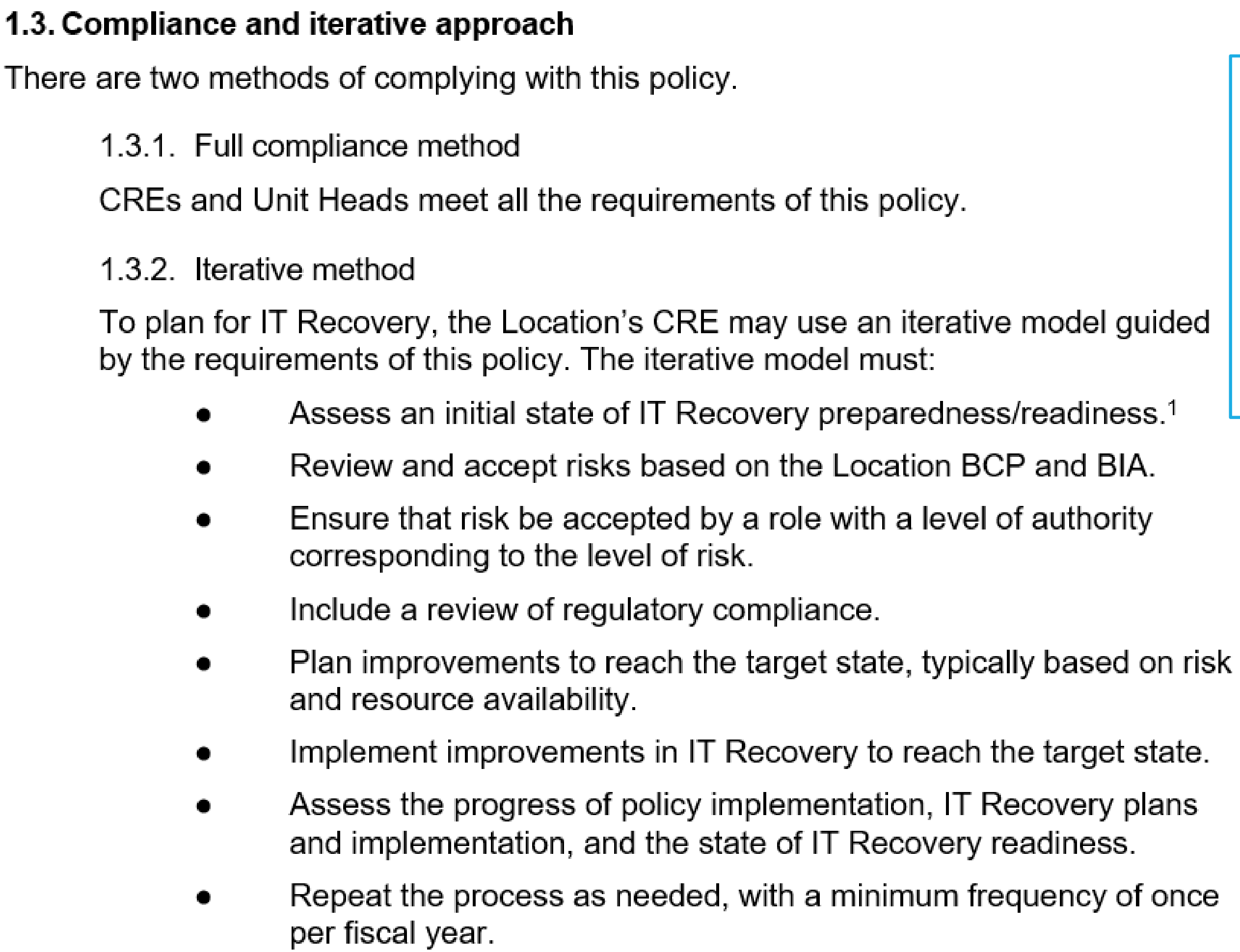
BCP

Units in Scope

IT Recovery

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

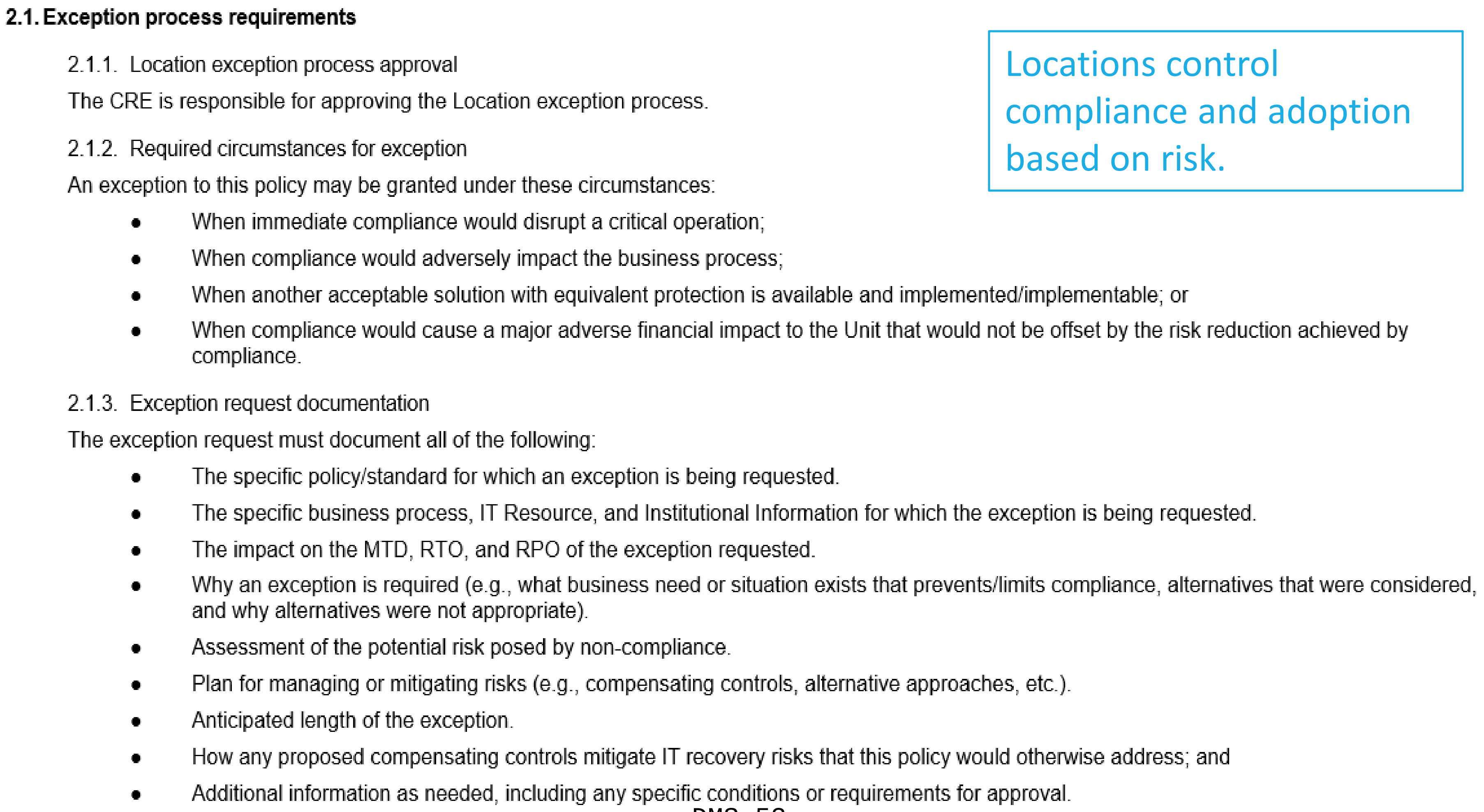
To plan for IT Recovery, the Location's CRE may use an iterative model guided by the requirements of this policy. The iterative model must:

- 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.

These methods allow the Location to iterate over years to fully address IT Recovery risk and manage to a desired level.

Robust Location Exception Process

Locations control compliance and adoption based on risk.



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

Improvements addressed

- Added new features
  - Narrower scope – Location defined.
  - Exception process.
  - Iterative model for compliance.
- Clock restarts – 12 months to transition.
- The current policy does not align with UC Health recovery levels. Aligning helps UC Health and:
  - UCLA
  - UC Davis
  - UCI
  - UCSD

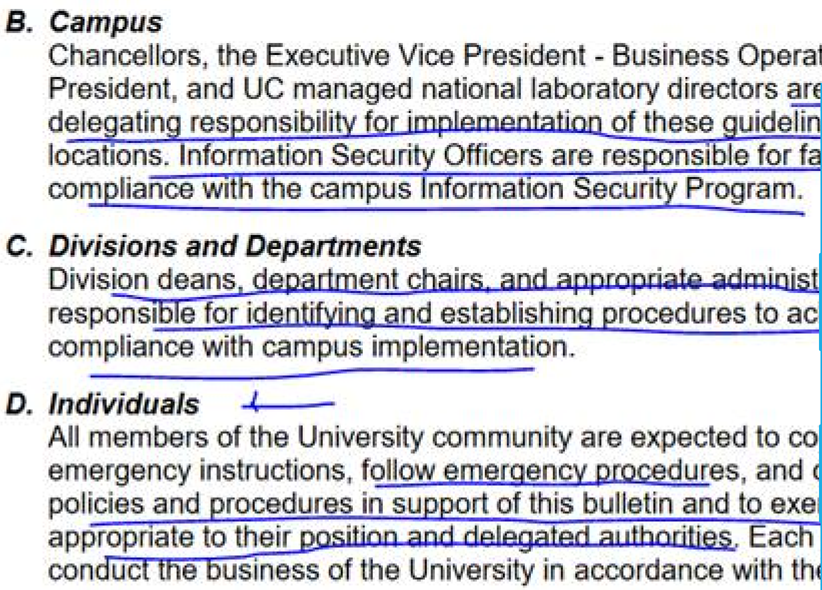
Advantages of the Rewritten Policy

- Now aligned with technology.
- Aligns with UC Health Recovery levels.
- Now aligned with Cloud and Service Providers.
- Directly implementable.
- Systemwide consistency.
- Endorsed by systemwide workgroup, including BCP leads

Sponsored by:

- ◦ UCACC/AS
- ◦ Risk Services
- ◦ Systemwide IT

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

delegating responsibility for implementation of these guidelin

locations. Information Security Officers are responsible for fa

compliance with the campus Information Security Program.

C. *Divisions and Departments*

Division deans, department chairs, and appropriate administ

responsible for identifying and establishing procedures to ac

compliance with campus implementation.

D. *Individuals* ←

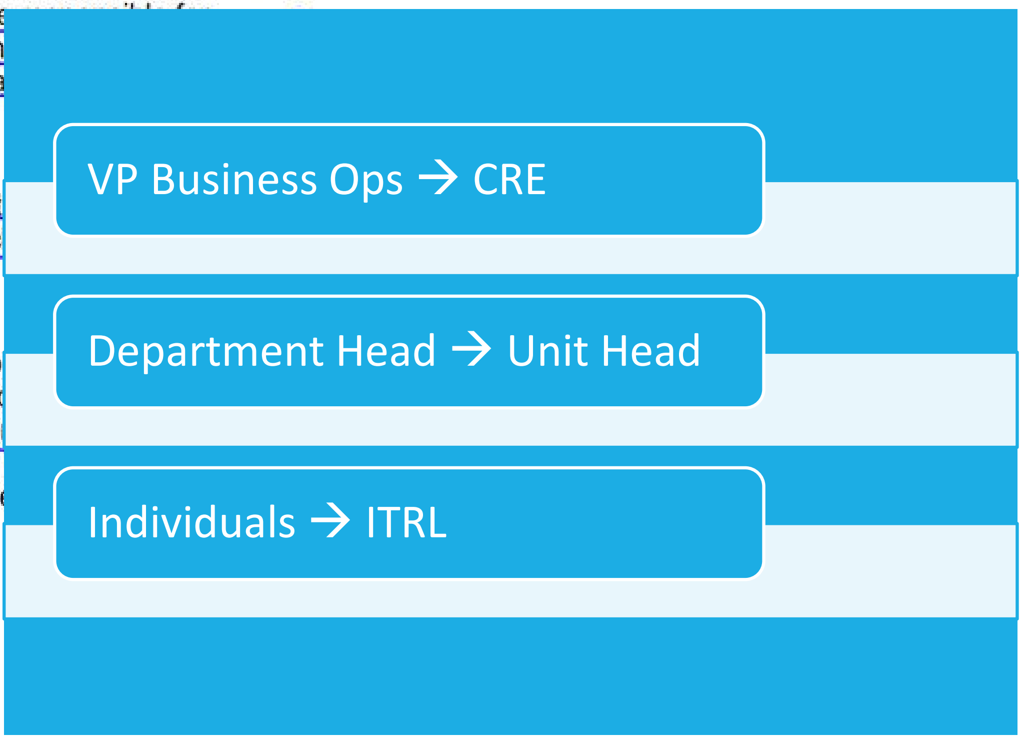
All members of the University community are expected to co

emergency instructions, follow emergency procedures, and

policies and procedures in support of this bulletin and to exe

appropriate to their position and delegated authorities. Each

conduct the business of the University in accordance with the



VP Business Ops → CRE

Department Head → Unit Head

Individuals → ITRL

Old blocks mapped to new

Current IS-12	New IS-12
	Identify – roles/people
Mitigation	Removed from IS-12 – this topic is covered in IS-3 IR Standard
Technology and Infrastructure	Same
Preparedness	Same + communication plan
Response	Same
Recovery	Same

thank you!

QUESTIONS – CONTACT: robert.smith@ucop.edu

University of California – Policy **DRAFT**

IS-12: IT Recovery

Systemwide Review Draft

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.

Systemwide Review Draft

Systemwide Review Draft

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.

Systemwide Review Draft

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.)

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

Systemwide Review Draft

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

Systemwide Review Draft

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.

Systemwide Review Draft

- 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:

Systemwide Review Draft

- 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).

Systemwide Review Draft

- 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

Systemwide Review Draft

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.

Systemwide Review Draft

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.	

Systemwide Review Draft

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.

Systemwide Review Draft

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	

Systemwide Review Draft

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

- 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.

Systemwide Review Draft

- 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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide Review Draft

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.

Systemwide

UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

OFFICE OF THE VICE PRESIDENT AND
CHIEF INFORMATION OFFICER
Information Technology Services

OFFICE OF THE PRESIDENT
1111 Franklin Street, 7th Floor
Oakland, California 94607-5200

November 3, 2020

CHANCELLORS
ACADEMIC COUNCIL CHAIR GAUVAIN
LABORATORY DIRECTOR WITHERELL
ANR VICE PRESIDENT HUMISTON

Re: Systemwide Review of Proposed Presidential Policy, Business and Finance Bulletin, IS-12 IT Recovery

Dear Colleagues:

Enclosed for systemwide review is a proposed replacement for the Presidential Policy, Business and Finance Bulletin, IS-12.

IS-12 was last updated in 2007 and was called Continuity Planning and Disaster Recovery (now called IT Recovery.) However, it lacked crucial details to keep it relevant for the current times. Some examples include up-to-date technology references, a uniform method to meet UC's current recovery needs, and a method for local governance.

UC's ability to recover data and supporting systems is critical in order to recover from or operate through power loss, floods, fires, earthquakes, pandemics, and cyber threats like ransomware. The revised policy provides guidance to help UC locations plan for IT recovery, and utilizes the IT recovery knowledge and experience that UC Health has been putting into practice.

A systemwide workgroup under the sponsorship of Risk Services, the UC Academic Computing Committee (UCACC is a subcommittee of the systemwide Academic Senate), and the Systemwide Chief Information Security Officer was formed to revise the policy. The workgroup consisted of fourteen representatives from various functions (IT operations, IT recovery, security, business continuity leads/planners, IT policy and analysts) and representing the following locations:

- ANR
- UC Berkeley
- UC Davis
- UC Davis Health
- UCLA
- UCLA Health
- UCOP
- UC Merced
- UCSF
- UC Santa Cruz

The workgroup collected requirements in late 2019 and early 2020, and drafted revised policy. Two drafts were widely circulated, one in April 2020 and another in July 2020, to the UCACC, UC Legal, campus representatives, and other systemwide departments. The workgroup made adjustments based on the feedback from both rounds of review.

Given UC's fiscal limitations both pre and post COVID, the revised policy allows locations to manage IT recovery in accordance with their budgetary priorities and provides for the following:

- Location ability to determine what units are in scope
- Location-governed exception process
- Iterative model for adoption and compliance
- Delayed effective date

Systemwide Review

Systemwide review is a public review distributed to the Chancellors, the Chair of the Academic Council, the Director of the Lawrence Berkeley National Laboratory, and the Vice President of Agriculture and Natural Resources requesting that they inform the general University community, especially affected employees, about policy proposals. Systemwide review also includes a mandatory, 90-day full Senate review.

Employees should be afforded the opportunity to review and comment on the draft policy. Attached is a Model Communication which may be used to inform non-exclusively represented employees about these proposals. The Labor Relations Office at the Office of the President is responsible for informing the bargaining units representing union membership about policy proposals.

We would appreciate receiving your comments no later than **March 5, 2021**. Please submit your comments to Robert Smith, robert.smith@ucop.edu. If you have any questions, please contact Robert Smith at 510-587-6244 or robert.smith@ucop.edu.

Sincerely,
Mark A. Ci
Mark Cianca
Interim Vice President and Chief Information Officer
Associate Vice President, Operational Services

Enclosures:

1. Presidential Policy IS-12 IT Recovery
2. Supporting PowerPoint in PDF format outlining some key features of IS-12
3. Model Communication

cc: President Drake
Provost and Executive Vice President Brown
Executive Vice Chancellors/Provosts
Executive Vice President and Chief Operating Officer Nava
Senior Vice President Bustamante
Vice President and Vice Provost Gullatt
Interim Vice President Lloyd
Vice President Maldonado
Vice Provost Carlson
Deputy General Counsel Woodall
Vice Provosts/Vice Chancellors of Academic Affairs/Personnel
Assistant Vice Provosts/Assistant Vice Chancellors/Directors – Academic Personnel
Executive Director Baxter
Executive Director Chester
Executive Director and Chief of Staff Henderson
Chief of Staff and Chief Policy Advisor Kao
Chief of Staff Levintov
Chief of Staff Peterson
Director Grant
Director Lee
Director Smith
Manager Crosson
Manager Smith
Analyst Durrin
Policy Advisory Committee
Executive Sponsor, Joseph, UC Berkeley
Executive Sponsor, Rusting, UCOP
Executive Sponsor, Samuels, Risk Services