Frequently Asked Questions

General questions

1. What drove the adoption of this structure of the policy?

The structure of the policy is based on international standards. UC, other universities and EDUCAUSE have opted to use the International Standards Organization (ISO) standard on security techniques, information security management systems and security requirements. These standards are labeled 27001 and 27002. The ISO standard is in use worldwide. Using this structure thus makes it easier for UC to work with cyber insurance carriers, outside firms and off-the-shelf security and risk management tools. It also maps easily onto the National Institute of Standards and Technology (NIST) security controls, which are relevant to the NIST Cyber-Security Framework (CSF).

2. Does the policy set the bar too high?

No. UC is a complex organization and handles many types of data. The policy sets the minimum requirements that UC must meet due to law, regulation or contract.

Some examples of obligations UC must meet include: Health Information Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act; California's Confidentiality of Medical Information Act (CMIA); Payment Card Industry Digital Security Specification (PCI-DSS); Higher Education Act; Family Educational Rights and Privacy Act (FERPA); Department of Education Dear Colleague letters 2015 and 2016; Student Aid Internet Gateway (SAIG) Enrollment Agreement; Gramm-Leach-Bliley Act; State of California Attorney General minimum security standard; Defense Federal Acquisition Regulations Supplement (DFARS related to NIST 800-171 - Protecting Unclassified Information in Nonfederal Information Systems and Organizations); state regulations/laws; and other federal regulations/laws and agreements. Increasingly, data sharing agreements and research funding agreements include cyber security requirements. The European Union's General Data Protection Regulation also has requirements for data security and data loss prevention. In addition, all members of the UC community expect and trust UC to protect their information.

3. How will implementation of the policy be monitored?

Managing security risk requires an iterative process. The CRE, CIO and CISO will collaborate with UCACC, faculty, administrative leaders, internal audit, UISLs and other interested stakeholders to monitor cyber risk at the Location and make needed adjustments. Shared governance is foundational to successfully managing cyber security risk.

Policy questions

4. Can Part III, Section 1.2.2, "Costs of an Information Security Incident," be used to hold an individual (Workforce Member or faculty) personally liable for an information security incident?

No. Financial responsibility for an information security incident is an organizational concern. UC would not seek to recover costs from an individual due to a significant failure to comply with IS-3 policy. Individuals may, however, still be held liable by an outside party, and may be subject to criminal investigation, criminal charges or civil cases seeking restitution.

Unrelated to this policy, the Health Insurance Portability and Accountability Act (HIPAA) and California privacy laws both list personal liability as a possible outcome of a privacy breach (a determination not made by UC). Regulatory agencies such as Health and Human Services and the California Department of Public Health may opt to levy fines against

individuals when that agency's assessment of the case indicates that an individual or individuals were personally responsible for a breach.

5. In Part III, Section 1.2.2, "Costs of an Information Security Incident," what constitutes a "significant failure to comply" with the policy?

This is a "reasonable person" standard and the same standard set by the State of California and the Office of Civil Rights. The standard defines "significant failure" as "conscious, intentional failure or reckless indifference to the obligation to comply."

Example 1: If a Unit did not encrypt any of its 50 laptops, that would constitute a failure to comply. Conversely, if a Unit encrypted all of its laptops and two new ones were stolen prior to the setup process, that would not constitute a significant failure to comply.

Example 2: If a Unit had two years of history showing the Unit regularly applied software updates (patches), but five systems were missed in the last cycle, that would not constitute a failure to comply. Conversely, if there were no history of patching and recent patching was also incomplete (i.e., most systems were still unpatched), that would constitute a significant failure because there would be a clear pattern of non-compliance.

6. Regarding Part III, Section 1.2.2, how might a Location hold a Unit financially accountable?

Holding a Unit financially accountable is within the purview of the Location. If a Location, after an investigation into an Information Security Incident, discovers that a Unit did not make a reasonable effort to comply with the information security requirements, the Location would be able to charge the Unit with the incident costs related to the failure to comply.

Example: A Unit starts taking credit cards. The Unit is advised of the requirements for their payment card system, yet decides not to comply with those requirements and signs the attestation that they are in compliance. Later, the Unit's credit card processing systems are attacked and the Location's merchant bank requires a forensic investigation costing $50,000 and fines the Location $75,000 for the failure to comply. In addition, there is a cost of $20,000 for consumer notification and credit reporting. The Location may allocate all or part of the incident cost of $145,000 to the Unit.

Rationale: Assigning financial responsibility for the failure to comply with policy standards to non-compliant Units allows Locations to avoid penalizing Units that do comply. It also produces an incentive to follow information security policy. Compliant Units and Locations may avail themselves of UC's cyber insurance protections, which helps manage financial risks related to data loss or other cyber incidents.

7. Regarding Part III, Section 1.2.1, what constitutes a "serious violation" of the policy?

A serious violation occurs when the Workforce Member either knowingly fails to comply with a material requirement (purposeful disregard) or acts with plain indifference.

8. Does Part III, Section 7.1 require faculty to get background checks prior to employment?

No. IS-3 does not impose requirements for faculty background checks.

9. Does Part III, Section 7.2 require teaching assistants, graduate students and undergraduates who handle Protection Level 3 and Protection Level 4 Institutional Information to get background checks prior to employment?

Yes. It has been consistent UC policy to require background checks of individuals assigned these tasks. Previous policy asserted that:

> "Campuses should develop policies and procedures to ensure that candidates for critical positions requiring access to restricted or essential resources undergo applicable background checks as part of the selection process…"
>
> "Background checks shall be conducted for University employees who control and manage encryption keys and key management software and hardware."
>
> "Background checks are required for non-University contractors or consultants engaged to work on restricted or essential electronic information resources."

IS-3 clarifies that Locations create these processes to ensure effective cyber risk management in the context of business needs. See IS-3 Part III, Section 7.5 below:

> **7.5 Background checks**
>
> Location HR must develop and implement pre-employment screening procedures in accordance with university policy and applicable labor agreements for non-academic Workforce Members, including appropriate background checks that anticipate risks stemming from access to Institutional Information or IT Resources. Such cyber risks might include:
>
> - Financial fraud.
> - Identity theft.
> - Medical fraud.
> - Cyber related crimes.
> - Crimes related to the performance of specific job duties.

10. Does IS-3 apply to UC students?

IS-3 only applies to students employed by UC as Workforce Members (which includes research assistants and volunteers). It does not apply to students simply attending the university.

Regarding student user guidelines, the policy does require Locations to:

1. Establish rules for Internet access/use (acceptable use). See IS-3, Part III, Section 8.1.3.
2. Establish Location rules for safe computing on provided networks. See IS-3, Part III, Section 9.1.2.

Implementation questions

11. Do Locations control the implementation of this policy?

Yes.

12. Will end-users be able to easily understand and follow this policy?

Providing clear guidance to end-users is an important part of improving cyber security at UC. To that end, guides outlining the common roles and responsibilities for end-users [https://security.ucop.edu/policies/index.html] have been created and posted online, and will be updated as needed.

Many Locations have already developed similar resources and others plan to do so.

13. Are there websites with resources to support Workforce Members in managing security?

Yes. At https://security.ucop.edu/services/index.html, on the left side of the screen, a list of links points to each Location's resources.

At https://security.ucop.edu/policies/index.html, resources help guide adoption of the policy. Locations and UCOP will both work to meet the needs of UC Workforce Members as they do their part to manage UC's cyber risk.

14. How will Locations allocate additional resources to support the policy?

Each Location's chancellor has appointed a Cyber-risk Responsible Executive (CRE). The CRE is responsible for managing cyber risk and allocating resources. The Location will assess risk, manage priorities and allocate budget according to Location priorities.

15. Are there examples of the shared responsibility, data classification and unit concepts?

Yes. These are from work implemented at UC Berkeley:

- https://security.berkeley.edu/campus-information-technology-security-policy
- https://security.berkeley.edu/departmental-security-contact-policy#related
- https://security.berkeley.edu/data-classification-standard

16. Are there examples of how implementation will look?

Yes. UCI and UCOP have already started user-friendly "How do I … "and "I am …" guides. See:

- https://security.uci.edu/
- https://security.ucop.edu/policies/quick-start-guides-by-role/index.html

UC Davis has developed a user-friendly assessment tool and process to support the new IS-3:

- http://itcatalog.ucdavis.edu/service/risk-assessment

17. Who will ensure that faculty members have the campus support they require?

The Unit Head or the Location CRE.

18. Who is a Unit Head?

Locations determine who is a Unit Head.

For administrative Units, the Unit Head will typically be a senior executive, most often a Director, Sr. Director, AVC or VC.

Academic Unit Heads have administrative responsibility for campus organizational departments (e.g., deans, department chairs) or supervise projects/research involving IT Resources and Workforce Members (e.g., principal investigators).

Faculty who do not supervise Workforce Members or act as IT Resources Proprietors for multiple users are not Unit Heads.

19. How long should documented exception records be kept (Part III, Section 2.2)?

Retain records for 3 years after the end of the fiscal year in which the IT Resource, system, application or website is retired. See BFB-RMP-2.