Information security landscape

UC is a target. Cyber bad actors target our university for many reasons. They steal electronic deposits, credit cards, identities, medical records and research. They encrypt files hoping to get paid a ransom. They gather human intelligence. Regardless of the type of threat, the public and UC community trust our policies and procedures to protect their data and privacy.

Government expects UC to practice sound security methods in all that we do. The California legislature, California Attorney General, Office of Civil Rights, Department of Education, Department of Energy and Department of Defense all have one thing in common. They are raising the bar for information security, and UC must meet it.

The Department of Education is also moving to require a higher level of information security. Beginning December 2017, many faculty research contracts with the department of defense will include new, more stringent requirements (DFARS 252.204-7008(c)(1), NIST 800-171). IS-3 must be revised to meet these new requirements.

At the same time, we're becoming more collaborative across the UC system and with other researchers from around the globe. UC requires a uniform approach to information security that can work across the university system, support UC's mission, and meet the expectations and requirements of the public and UC's partners. IS-3 was drafted with systemwide collaboration to meet the challenge of remaining both a trusted holder of information and a premier open research university.

The new version of IS-3 aligns with many key initiatives already under way. These include systemwide cybersecurity governance, cyber risk management, the escalation protocol and collaborating across locations.

Local control

The new version of IS-3 puts each location in charge of risk management, risk trade-offs and the exception process. Each location has a Cyber-risk Responsible Executive (CRE) who will balance local needs, risk tolerances, budget and implementation of policy requirements.

Easing adoption

The old version of IS-3 requires each campus to develop policies following guidance. This approach led to inconsistent adoption and makes it hard to answer the question: "What do I need to do?" The new IS-3 is a single policy that was developed to work across the system. This approach allows us to develop guides to help specific roles answer that question. These are published on the website on the guide page. They provide an overlay to the policy, helping to guide staff and faculty to the most important policy provisions.

The policy creates a pre-approved risk treatment plan that's scalable and easy to adopt. This template-based approach allows for quick and scalable handling of routine scenarios and allows us to focus our scarce resources on higher-risk areas (Section III, Subsection 6.1.)

Standards-based approach

IS-3 uses an accepted standard as the basis for security controls. The standards are ISO 27001 and 27002. IS-3 used a subset of the controls that fit UC's mission of research, teaching and public service.

The policy also considers the requirements of HIPAA, the Payment Card Industry (PCI) and other state and federal regulations. These include requirements needed to qualify for certain grants that are essential to UC research funding (NIST 800-171). This approach has many benefits, including lower-cost engagement with vendors, vendor product support, alignment with cyber insurance carriers and alignment with regulations.

New roles

Unit Head: A generic term for Dean, Vice Chancellor or similarly senior role who has the authority to allocate budget and is responsible for Unit performance. At a particular location or in a specific situation the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers.

Unit Information Security Lead: A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities including, but not limited to: implementing security controls;

reviewing and updating Risk Assessment and Risk Treatment plans; devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights.

Service Provider: A UC internal organization that offers IT services to Units. Identifying this role allowed the policy to clarify accountability and ease adoption through clear responsibility assignment.

IS-3 outline

The policy has five key goals focused on the mission of the university. Unit Heads are responsible for planning and implementing information security risk management. The policy text is in Section III. Subsections 1 to 6 outline the overall governance, security management, risk management and planning processes. Subsection 7 specifies the requirements for recruiting and managing the workforce. Subsection 8 deals with the classification of electronic institutional information and IT Resources. Subsections 9 to 18 deal with specific controls and requirements, covering key topics like encryption, logging, access controls and supplier controls. They are scoped based on availability needs, protection requirements and risk.

A separate glossary defines key terms and gives examples to help illustrate the definitions. The most important terms have summary definitions in Section III.

Security Management Program principles

UC is adopting five key principles in developing electronic information security programs:

1. A goal-based approach is best.
2. Units are accountable for driving information security.
3. Decision-making rights correspond to risk level.
4. Security is a shared responsibility.
5. Security is embedded into the entire lifecycle.

Information classification

UC's electronic information now has four protection levels. The first level, P1, is public information. Here UC's concerns relate to integrity and availability. The next level is P2, where we find information that UC does not to intend to be public. At P2 we a start to become concerned with confidentiality, ensuring only those who are intended to access the information can do so. At P3, we are very concerned with confidentiality. P3 information includes student educational records and staff records. At P4, the highest level, UC has a statutory or contractual obligation to protect the data with the highest level of care. (Section 3, Subsection 8.2.)

The policy has a special classification called Critical IT Infrastructure. These systems have a shared fate. They contain information or provide access that, if compromised, would give the attacker broad access across multiple systems and information classifications types. Think of these systems as "keys to the castle." (Section III, Subsection 6.1.2.)

Risk-based approach

A risk-based approach is applied throughout the policy. This approach helps guide decisions on allocation of resources by evaluating the risk, the costs of addressing those risks, and the benefits of addressing the risks. The risk-based approach is a cornerstone to scoping controls and making intelligent investment decisions.

Other changes

The new IS-3 simplifies electronic information security at UC. It replaces the existing IS-3 and retires two other policies: IS-2 Inventory, Classification, and Release of University Electronic Information; and IS-10, Systems Development Standards.

The policy also formalizes the method of adoption for systemwide electronic information security standards (procedures). Consultation with the Academic Senate's UC Academic Computing Committee is now a required step in the process. This change integrates faculty into the governance process. (Section III, Subsection 2.3 Standards.)