IS-3 Reviewer FAQs

Questions about IS-3 developed during management consultation and early outreach

1. **Will end users be able to easily understand and follow this policy?**

   We understand that providing clear guidance to end users is a key step in improving cybersecurity at UC. To help clarify this, we created common roles and responsibilities for end users and posted them online. We'll update the website as needed. Providing supporting resources is a key part of the implementation plan.

   Link (look at the left side navigation): https://security.ucop.edu/guides/index.html

2. **What drove the adoption of this structure of the policy?**

   UC, EDUCAUSE and other universities 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, which makes it easier for UC to work with cyber insurance carriers, outside firms and off-the-shelf security tools. It also maps easily to the National Institute of Standards and Technology (NIST) security controls.

3. **Do websites with resources to support Workforce Members in managing security exist?**

   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/guides/index.html there are resources to help guide adoption of the policy. Locations and UCOP both plan to work to meet the needs of the UC Workforce to do their part to manage UC's cyber-risk.

4. **Why is the role of principal investigator (PI) included in this policy?**

   One of policy's top goals is to support research, a pillar of UC's mission. The policy identifies PIs and formally places them in charge of managing security within the parameters set by their Location.

   PIs have three main options:

   1) They can use a pre-approved Risk Treatment Plan provided by the location CISO that tells them what controls to use based on the classification level of the Institutional Information they're handling. Many PIs will likely choose this approach.

   2) They can use a Service Provider (such as a managed academic research computing environment; UCI and UC Davis already are working on prototypes with faculty partners) who will manage security for them. The policy formally provides support for these types of Service Providers.

   3) They can follow the policy to manage security themselves according to the needs of their program. The requirements are listed here: https://security.ucop.edu/guides/researcher.html

5. **Faculty and other researchers share customized code with other researchers. Is that an acceptable practice?**

   Yes—but faculty and researchers need to understand the Institutional Information classification levels and make sure their applications accomplish the mission securely. Researchers should also consider whether their applications introduce additional cyber-risk to others, and then act accordingly.

6. **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 access risk, manage priorities and allocate budget according to Location priorities.

7. **Do Locations control the implementation of this policy?**

   Yes.

8. **What are the standards referenced in the policy?**

   The policy references nine standards, which are approved by the IT Leadership Council (ITLC) in consultation with the UC Academic Senate Computing Committee (UCACC). Standards contain requirements that could change more rapidly than policy allows and/or provide additional details and options (like using passwords, passphrases or multi-factor authentication to gain access). An example draft of the Minimum Security Standard is available here: https://security.ucop.edu/guides/security-controls-everyone-all-devices.html

   These standards are currently in development.

9. **We are concerned about grants and data-sharing agreements that specify the National Institute of Standards and Technology (NIST) 800-171 security controls. Will this policy support our research grants under those requirements?**

   Yes. This is one of the reasons this policy is so important. The new IS-3 was validated against NIST 800-171, and with a few Location specifics like administrative physical access controls and controls that depend on Location technology choices, the policy provides the needed requirements to support research involving Controlled Unclassified Information (CUI).

10. **We are concerned that the Department of Education will start auditing financial aid offices against the Gramm–Leach–Bliley Act (GLBA) safeguard rule and later the National Institute of Standards and Technology (NIST) 800-171 security controls. Will this policy support those requirements?**

    Yes. This is another reason this policy is so important. The new IS-3 was validated against GLBA and NIST 800-171, and with a few Location specifics like administrative controls and controls that depend on Location technology choices, the policy provides the needed requirements to support operations involving Controlled Unclassified Information (CUI) used in Financial Aid offices.