WHAT DO THE NEW INFORMATION SECURITY POLICIES MEAN FOR ME?

Full policies are available for reference at **policy.arizona.edu** (currently via the link to proposed policies).
Here is a brief guide based on your role at the UA.

DEANS, DIRECTORS & DEPARTMENT HEADS

Because the UA is a highly distributed environment, information security risk is also distributed in a shared responsibility model. The new policies define the role of **Information Resource Owner** as those with operational authority for making risk tolerance decisions. This is often at the Dean or unit Director level. During the annual information security risk management cycle, the information security risk manager should consult with the information resource owner regarding the risks revealed by the assessment, provide the information resource owner with the necessary information to understand the risks, and receive guidance on priorities for security planning and remediation.

ALL FACULTY & STAFF

General security awareness training is required for all faculty, staff (including student workers) and DCCs. Training is available through UAccess Learning (security.arizona.edu/content/all-employee-security-awareness) and takes just under 40 mins to complete. There are 4 modules, so the training can be completed in ten minute increments.

Systems with regulated data (such as data protected by FERPA) must be **encrypted**. Full-device encryption is also a good practice to protect your personal information. Ask for assistance from your IT staff to ensure your computing devices are encrypted. This includes laptops, desktops, mobile devices, and external storage devices. Establishing a PIN or biometric access control such as fingerprint or facial recognition enables encryption on most smartphones and tablets.

INFORMATION SECURITY RISK MANAGERS

Individuals identified as information security risk managers for their departments are responsible for participating in the **information security risk management cycle**, using tools provided by the ISO (or a substantially similar process). They will then review the risks with appropriate leadership (Information Resource Owners) and develop a security plan. Particularly for the first annual cycle, Campus IT Partnerships and the ISO will provide hands-on assistance for this process.

RESEARCHERS

If you work with **regulated or confidential data**, you need to understand the regulatory requirements governing your data and comply with regulations. For data that is governed by NIST 800-171, (research on Controlled, Unclassified Information), UITS has a purpose-built environment that meets the technical standards required. Contact cui-support@list.arizona.edu for more information about the use of this environment.

INFORMATION TECHNOLOGY PROFESSIONALS

You must follow security policy and guidelines for **vulnerability management**, **logging and monitoring**, **access controls**, **contingency planning**, and **appropriate media life cycle management**. The guidelines supporting the new policies are under development through the spring and summer of 2019. There is a campus working group involved in this process; please reach out to the security office (security@arizona.edu) if you would like to contribute to the development of guidelines.

Information Security