Office of the Chief Information Security Officer

Comparison of U-M Security Environment
Under Current and Proposed SPG 601.27

U-M Security Environment Under Current SPG 601.27

● Highly decentralized IT environment; no single high-level official responsible for overall campus IT security.
● Faculty and staff have individual and shared responsibilities to protect U-M information assets, but very limited ability to institutionally verify how well the assets are protected.
● Each university unit is responsible to develop and implement its own information security plan with limited support from a central IT security office.
● Most university units allocate a fraction of 1 FTE to handle unit IT security functions.
● Little insight into unit IT security decisions and user actions.
● Each university unit is responsible to periodically conduct risk assessments of its sensitive information assets and to prioritize risks and appropriate mitigation; due to lack of resources and trained staff as well as pressure on unit priorities, these risk assessments were often not done in a timely manner and mitigation of identified risks was inconsistent or not carried out.
● Unit leadership is able to unilaterally accept risk with regard to sensitive information assets of the unit, even if the risk is ultimately to the entire university.
● Compliance with mandated federal statutes and regulations related to handling of various categories of sensitive data is largely managed at the unit level with limited support from central offices.

U-M Security Environment Under Proposed SPG 601.27

● One comprehensive university-wide IT security and information assurance program that promotes university-wide information assurance culture and capabilities.
● Leadership and direction provided by Chief Information Security Officer who is responsible for operational security of the entire university, including the Health System, and U-M Dearborn and Flint.
● U-M will adopt a NIST-based cybersecurity risk management framework and enterprise security architecture that makes leveraging secure security services straightforward and accessible to faculty and staff.
● Expectation that sensitive data will be maintained in appropriate centrally provided services, or units will need to meet specific documented security requirements.

● U-M will adopt a refined data classification structure and tiered security model. The emphasis will be placed on protecting the most sensitive information first utilizing a more extensive set of security controls.

● U-M units and individuals will generally not unilaterally accept information security and compliance risks that result in the greater university’s vulnerability.

● U-M will monitor on an ongoing basis the security technologies and controls that support the new SPG 601.27 at a level not currently feasible.

December 15, 2015