ITSC Briefing Paper

AN ENTERPRISE INFORMATION TECHNOLOGY SECURITY PROGRAM

What is an IT Security Program?

The Program is an 'umbrella' document representing an enterprise policy framework for consolidating Information Technology (IT) security policies and procedures. The Program documents management's commitment to information security, and specifies the scope and applicability of IT security practice.

The Program recognizes the value of information as an asset, and links to the risk assessment process managed by the Risk Management Steering Committee (ERM-SC). The IT Security Program specifies ownership, responsibility and accountability for University information technology security practice.

The Program references a widely-accepted international standard for managing information security, ISO/IEC 27000. The standard provides a structure and guidelines for developing and implementing cost-effective risk-based security processes.

Why Do We Need It?

The University's external auditors (PWC) and external security consultants have strongly recommended the institution articulate and document its management approach to information security, encompassing the three common security practice components: confidentiality, integrity, and availability. The C-I-A triad is the core objective and focus of an information security initiative.

Formalizing IT security into a policy framework (i.e. the Program), is an important step towards achieving a more visible and strengthened security "posture". It will serve to communicate expectations, educate the campus on risk management, business continuity priorities, and enable auditability against approved procedures and practice.

Security Program Components:

The ISO/IEC security standard emphasizes a risk-based approach to identify priority security controls. A risk assessment, identification of critical business processes, and an authoritative IT asset inventory are prerequisites.

The standard provides guidance on a recommended organizational structure for IT policies and recognized good practice for IT security, ranging from clear accountability for information security, managing third-party contractors, physical and environmental security, network management and access control, security incident management, to business continuity planning, compliance and auditing.

It is not expected, nor presumably cost-effective, to implement all 100+ "controls" detailed in the standard, however completion of the information risk assessment, and prioritization of critical business processes, will assist in determining the most effective security controls.

Implementation Strategy:

1. Document our current IT security "posture", using a Report Card of the most recent external security audit. The Report Card summarizes the areas where progress has been made, and where increased attention is required**.** **Complete**

2. ITSC to review and support the draft Program in principle, and recommend the appropriate level of approval for the over-arching Policy Framework**.** **Pending**

3. CIO to work with the Risk Management Steering Committee to complete the IT asset inventory, identify critical business processes, and prioritize risk-mitigating initiatives. **Pending**

4. The CIO's Office/PMO to engage with appropriate stakeholders to finalize the Security Program, build on the Program document to consolidate existing IT policies, move current draft policies through the approval process, initiate new policy statements, and coordinate new information security initiatives as appropriate. **Pending**