INFORMATION SECURITY STRATEGIC PLAN

UNIVERSITY OF CONNECTICUT INFORMATION SECURITY OFFICE 4/20/10

MISSION STATEMENT

The mission of the Information Security Office (ISO) is to design, implement and maintain an information security program that protects the University's systems, services and data against unauthorized use, disclosure, modification, damage and loss. The ISO is committed to engaging the University community to establish an appropriate information security governance structure that enables collaboration and support for new information security initiatives.

INTRODUCTION

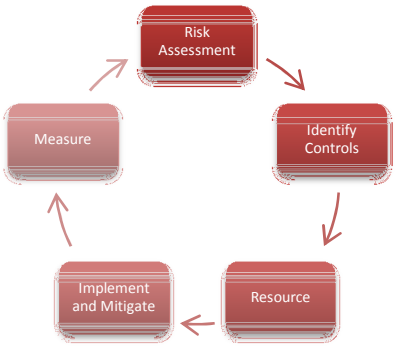
The University of Connecticut recognizes that information is a critical asset and that how information is managed, controlled and protected has a significant impact on the delivery of services. Information assets must be protected from unauthorized use, disclosure, modification, damage and loss. Additionally, information assets must be available when needed, particularly during emergencies and times of crisis.

The decentralized nature of the University's computing environment is inherently difficult to manage and secure. Many departments operate their own systems and applications. In addition, the University has not developed or enforced standards or guidelines to reduce the risks commonly associated with heterogeneous computing environments.

This document is the first University-wide information security strategic plan. It sets priorities for how the University can efficiently and effectively address the management, control and protection of the University's information assets. In addition, this document outlines the strategic objectives that all future initiatives are based on and identifies the components necessary to iteratively improve the security posture of the University.

The Information Security Office will utilize a methodology that establishes information security requirements based on risk assessments. Once risk is determined the mitigation controls are identified and resourced through the governance processes. The controls are then implemented and monitored for their effectiveness. The process continues as periodic risk assessments are done to identify and measure residual risk.

IT SECURITY PROGRAM – IMPLEMENTATION CYCLE



GOVERNANCE

In recognition of the increasing need to protect the University's critical business, intellectual and computing resources, the University has created the Information Security Office and hired a Chief Information Systems Security Officer (CISSO) for the purpose of building an IT Security Program for the University and all branch campuses.

The CISSO will lead the effort to deliver the objectives in this plan. To be successful, the CISSO must align and coordinate resources with the various schools, colleges and departments across the University. These coordinated security efforts must be vetted by all impacted stakeholders through an agreed upon governance process.

Though the governance process is still evolving, we are anticipating the stakeholders that participate in the decision making process will include:

- Chief Information Officer (CIO) – The CIO is responsible for the overall management, direction and security of the University's information assets
- Chief Information Systems Security Officer – The CISSO has delegated authority and is responsible for planning, developing and deploying the University's Security Program
- Executive Security Council – This council is responsible for oversight of security initiatives, policies and processes
- Technical Security Council – This council is responsible for the evaluation and implementation and security initiatives, policies and processes

The Information Security Office will also establish a regular schedule for reporting progress on security initiatives to the CISSO. The CISSO will review campus assessments and progress reports and deliver management briefings on a regular basis to the CIO.

STRATEGIC OBJECTIVES

The strategic objectives outlined below define where the University needs to be to effectively manage security risks to its information technology assets. Assuming that there will be sufficient resources for people, processes and tools, it will take 1 to 3 years to completely implement the following objectives. Each objective has one or more initiatives that need to be completed to achieve the objective.

The Information Security Office's strategic objectives are outlined below:

Data Loss Prevention – Initiatives that support this objective will help the University reduce the likelihood of data loss/disclosure of confidential/Federally protected data.

Improved security of system and network services – Initiatives that support this objective will support a defense in depth architecture and provide increased security of critical University services. Many of these initiatives and supporting projects are required to be in place according to Federal Regulations and various State Laws (HIPAA, GLBA, MA 201CMR 17.00, etc).

Proactive risk management – Initiatives that support this objective will allow data owners and administrators to be more aware of the security risks that their information assets are vulnerable to, identify controls to reduce those risks, and understand what risks remain after any identified controls have been implemented.

Crisis and security incident management – Initiatives that support this objective will help the University recover its information assets in the event of a catastrophic event. Additionally, these initiatives will enable the University to manage security events more efficiently and effectively, thereby reducing or minimizing the damages to the University.

KEY INITIATIVES

Initiative 1 – Security Policy, Standards and Guidelines framework

Enables Objectives – Data loss prevention, improved security of system and network services, proactive risk management and crisis and security incident management

Description - Develop, approve, and launch a suite of information security policies, standards and guidelines based on the ISO/IEC27001 code of best practices for information security. These policies will formally establish the University's IT Security Program and set forth employee responsibility for information protection.

The policy, standards and guideline framework will also take into consideration the multitude of Federal and State regulations that govern the use of personal, financial, student and patient data at the University.

Key Benefits

- Clear security baselines for all departments
- Policy based foundation to measure results
- Consistent application of security controls across the enterprise

Initiative 2 - Information Security Risk Management

Enables Objectives – Data loss prevention, improved security of system and network services and proactive risk management

Description - Create and oversee an IT Risk Management Program that enables the University to appropriately identify and protect its business data, intellectual property, and physical assets. This program also includes a reporting mechanism to alert Deans, Directors, Department Heads and identified Data Owners of the risks and vulnerabilities that the data and systems for which they are responsible for are prone to.

The IT Risk Management Program is the foundation by which all future security and continuity initiatives will be prioritized.

Key Benefits

- Enables the University to identify and proactively manage risks to systems
- Will provide a consistent methodology for identifying and reporting risks throughout the University
- Ensures that risks are being accepted at the appropriate level of management
- Ensures data is identified, classified and appropriately secured

Initiative 3 - Operation Continuity and Disaster Recovery

Enables Objectives – Data loss prevention, crisis and security incident management and proactive risk management

Description – Develop, implement and test plans to ensure that critical University systems are operational and available at all times. Successful completion of this goal will result in a disaster recovery plan and associated implementation strategy.

Key Benefits

- Enables the University to continue to provide critical services in the event of an emergency or disaster
- Ensures that the University is able to recover its systems and services to the user community in an appropriate time frame

Initiative 4 – Identity and Access Management

Enables Objectives – Data loss prevention, improved security of system and network services and proactive risk management

Description – A flexible Identity and Access Management system that is capable of managing the vast heterogeneity of the University community. It will provide authentication and authorization services to enterprise and departmental IT solutions while enabling improved secure collaboration with other Universities and businesses.

A process to maintain the evolution of this system will be developed and implemented to ensure that the products of this initiative continuously evolve as technology and business needs dictate.

Key Benefits

- Better security through uniform and repeatable access control processes
- Reduced potential for security breaches and fines due to non compliance with federal regulations

Initiative 5 – Network and System Security Architecture

Enables Objectives - Data loss prevention, improved security of system and network services and crisis and security incident management

Description - A tiered security architecture that provides the ability to separate resources based on their data, business criticality, and function. Appropriate controls will exist within each level to address the risks to the resources in that tier.

Key Benefits

- Improved security by applying technical safeguards that enforce policies.
- Ability to determine high risk areas and focus security resources where they safeguard the Universities most critical resources.
- Provides a defense system to prevent attacks and locate where attacks may have been successful.

Initiative 6 – Information Security Awareness Training

Enables Objectives – Data loss prevention, improved security of system and network services, proactive risk management and crisis and security incident management

Description – Make available information security awareness training, which serves to inform employees of their responsibilities for protecting the information in their care. To further engage the user community, the security office will work to develop a variety of information-sharing forums to include electronic and live mediums.

Key Benefits

- Better awareness of security threats and their impact on information assets
- Fewer security incidents
- Common knowledge for all staff