Approved 18 January 2011

Hampton University IT Security Plan

Introduction

"The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements."[1]
This document provides an overview of the Hampton University Information Security Office strategy for providing information assurance at Hampton University. It is a living document and will be subject to updates.

Hampton University Information Security Mission

The Center for Information Technology (CIT) provides direction and guidance to the University community safeguarding the confidentiality, integrity and availability of Hampton University information and computing assets. The Center for Information Technology provides strategy definition, risk assessment, standards development, communication and training, and investigation of threats and incidents. The Assistant Provost for Technology/CIO also serves as the University's Information Systems Security Officer (ISSO).

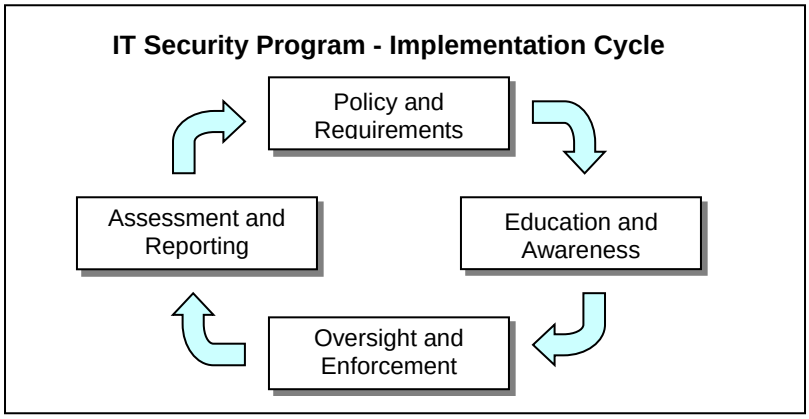
Business Context

Like other universities, Hampton University faces a number of challenges due to its heterogeneous and decentralized information technology services, the need to support three sometimes overlapping user groups (faculty, staff, and students), and the need to provide secure access to information at all times. Key factors/drivers in managing information security at Hampton University include risk tolerance, asset protection, vulnerability management, and threat mitigation.

IT Security Program

It is important to note that establishing an IT Security Program is not a one-time event, but an ongoing venture that follows a cyclical process. The implementation phases (see below) are not cleanly separated processes, but instead represent a flow of activities that yield an ever maturing program. The implementation cycle involves establishing information security requirements, educating people about their responsibilities under those requirements, building governance structures to ensure Program compliance, and monitoring and reporting of progress.

[1] **Swanson, M.** *Guide for Developing Security Plans for Information Technology Systems.* s.l. : NIST Special Publication 800-12, 1998.



Strategic Goals

Goal 1: Develop, Approve, and Promote a Comprehensive IT Security Policy Suite.
In collaboration with all appropriate University representatives the ISSO will lead efforts to develop, approve, and launch a suite of information security policies, based on the ISO 17799 code of best practices for information security[2]. These policies will formally establish the University's IT Security Program and set forth employee responsibility for information protection.

Goal 2: Ensure All Employees are Aware of their Information Security Responsibilities.
Require all employees to participate in information security awareness courses, which serve to inform employees of their responsibilities for protecting the information in their care. To complement employee awareness of responsibility, each campus is to develop a training program to ensure their employees have the knowledge needed to carry out those responsibilities within their campus environment.

Goal 3: Establish Oversight Authority for Information Security at Each Campus.
Designate a person on each campus with information security oversight authority for all IT operations on that campus. Such a person would have the authority to enforce the requirements of University and campus policies for information security. This person would have the authority to make recommendations to the ISSO on the following types of actions: authorizing new IT services, shutting down services that are out of compliance with policy, or transferring management of those services to a department or service provider with the requisite capabilities.

Goal 4: Establish a Process for Regular Progress Reporting to Executive Leadership.

[2] Further information about ISO 17799 (ISO 27000) and its use in security plans may be found at http://www.17799central.com/.

Establish a regular schedule for reporting of campus Program progress to the ISSO. The ISSO will review campus assessments and progress reports and deliver management briefings on a regular basis to the Security Advisory Committee (SAC) and to the Administrative Council, President, and Board of Trustees as required.

Goal 5: Inventory Sensitive Data and Purge Unneeded Data.

Initiate a data inventory process on each campus to identify sensitive data and ensure the data is appropriately protected. Sensitive data no longer needed for business or archival purposes will be promptly purged in accordance with institutional archival policy. Remaining data will be adequately protected, following guidance from campus IT security officers and business owners.

Point of Contact

Keith M. Perkins
Assistant Provost for Technology/CIO/ISSO
Hampton University
(757) 728-6988
keith.perkins@hamptonu.edu

Detailed Policies and Guidelines Available @ Hamptonu.edu

Acceptable Encryption Policy	Email Retention Policy	Remote Access Tools Policy
Analog Line Policy	Email Security Example	Removable Media Policy
Anti-Virus Guidelines	Equipment Disposal Example	Responsible Web Use Example
ASP Policy	Equipment Disposal Policy	Router Security Policy
ASP Standards	Extranet Policy	Security Plan
Audit Policy	Information Sensitivity Policy	Server Security Policy
Auto Forwarded Email Policy	Internal Lab Security Policy	Social Engineering Example
Bluetooth Security Policy	Internet DMZ Equip Policy	Social Engineering Policy
Clean Desk Example	Internet Use Policy	Software Installation Example
Clean Desk Policy	Lab Anti-Virus Policy	Software Installation Policy
Comms Equipment Policy	Mobile Device Encrypt Examp	Virtual Private Network Policy
Dail-in Access Policy	Mobile Device Encrypt Policy	Wireless Comms Policy
Database Credentials Policy	Password Policy	Wireless Comms Standards
Disaster Recovery Guidelines	Personal Comms Device Policy	Workstation Security Example
DMZ Lab Security Policy	Remote Access Policy	Workstation Security Policy
Email Policy		

Definitions

Security Advisory Committee (SAC)
A committee formed to collaborate on the various IT Security issues and policies as they arise. Representatives from (CIT, Campus Police, General Counsel, and Computer Center) make up the core members. Additionally, System Administrators/representatives from the various Schools/Departments serve as auxiliary members.

Risk Tolerance
The residual risk the organization is willing to accept after implementing risk-mitigation and monitoring processes. When evaluating risk, consider the impact (potential consequences of a risk-based event), likelihood of a risk's occurrence, and associated mitigating actions.

Asset
Anything of value to an organization. Assets include information such as enterprise strategies and plans, product information, and customer data; technology such as hardware, software, and IT-based services; supporting facilities and utilities; key personnel with unique knowledge and skills; and items of significant yet largely intangible value such as brand, image, and reputation. Critical assets are those that directly affect the ability of the organization to meet its objectives and fulfill its critical success factors[3]

Asset Protection
Methods, processes, and procedures used by an organization to safeguard its assets

Vulnerability Management
Scanning and Checking for Vulnerabilities, this includes asset inventory, prioritizing and researching the remediation activities as well as the actual act of patching, hardening or reconfiguration. To be effective, it also involves attention to policy and process improvements. In fact, focusing on process and the "softer" side of the vulnerability conundrum will often bring more benefits than a high-tech patch management system.

Threat Mitigation
Identifying threats and taking steps to prevent them. The conventional wisdom is to build a layered defense with security technology such as firewalls, IPS, network access control, anti-x client software, alarm aggregation and event correlation, etc. The systems approach builds upon IT security investment by wrapping it with System Management for policy, reputation and identity that transcend end-points, networks, content and application security.

---

[3] **J. H. Allen**, *How Much Security is Enough?,* https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/566-BSI.html