Purpose

The purpose of this policy is to define requirements for system security planning and management to improve protection of College information system resources. Security has to be considered at all stages of the life cycle of an information system (i.e., feasibility, planning, development, implementation, maintenance, and retirement) in order to: a) ensure conformance with all appropriate security requirements, b) protect sensitive information throughout its life cycle, c) facilitate efficient implementation of security controls, d) prevent the introduction of new risks when the system is modified, and e) ensure proper removal of data when the system is retired. This policy provides guidance to ensure that systems security is considered during the development and maintenance stages of an information system's life cycle.

Scope

This policy applies to all university colleges, departments, administrative units, and affiliated organizations that use university information technology resources to create, access, store or manage College Data to perform their business functions. The requirements apply to enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

Effective Date

This policy became effective on August 1, 2013.

Policy

Appropriate security controls should be considered at all stages of an information system life cycle, including the development and maintenance stages.

1.System security plans and documentation - System security plans and documentation must be prepared for all enterprise information systems or other systems under development that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein. Such plans should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements through all stages of the system's life cycle. When the system is modified in a manner that affects security, system documentation must be updated accordingly.

2. Separate development, testing, and production environments - System development, testing, and production should be performed in separate environments.

3. Test data - Testing of enterprise information systems should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any confidential data appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or confidential data must have appropriate security controls employed.

4. Vulnerability management - An assessment of the system's security controls and a vulnerability assessment that seeks to identify weaknesses that may be exploited must be performed on all new enterprise information systems or ones undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures taken to address the risk associated with identified vulnerabilities. Vulnerability notifications from vendors and other appropriate sources should be monitored and assessed for all systems and applications associated with enterprise information system.

5. Vendor acquisitions - If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by K-State or an independent third party, if needed.

Definitions

1. Confidential data - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. See ACOM's Data Classification and Security Policy for an expanded definition and examples.

2. Enterprise information system - An information system and/or server providing services commonly needed by the ACOM community and typically provided by central IT units. Departmental information systems provide services specific to the mission and focus of individual Colleges, departments, administrative units, or affiliated organizations and are typically provided by distributed IT staff in those units.

3. Live data - data accessible to users through systems that are in production (i.e., live).

4. University Data - Any data related to Alabama College of Osteopathic Medicine ("College") functions that are a) stored on College information technology systems, b) maintained by ACOM faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

Roles and Responsibilities

1. Chief Information Security Officer (CISO) - Coordinates the development of guidance for the development, review, and approval of system security plans as well as the identification, implementation, and assessment of common security controls; oversees periodic vulnerability

assessments for enterprise information systems; and coordinates implementation of other assessments as needed with information system security administrators.

2. Information System Security Administrator - Ensures the application of appropriate operational security controls for an information system; coordinates with the CISO in the identification, implementation, and assessment of common security controls; plays an active role in developing and updating a system security plan and coordinating with an information system owner any changes to the system and assessing the security impact of those changes. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

Related Laws, Regulations, or Policies

A. Existing ACOM systems development and maintenance policies

1. Security patches policies

B. Other related laws, regulations, or policies

1. ACOM Data Classification and Security Policy

2. ACOM Information Security Plan

3. ISO/IEC 27002:2005, "Information technology - Security techniques - Code of practice for information security management"http://www.iso.org/iso/catalogue_detail?csnumber=50297, published by the International Security standards Organization http://www.iso.org. This is an international security standard that includes security requirements for development and support processes (see chapter 12, "Information Systems Acquisition, Development and Maintenance") to ensure that "security is an integral part of information systems."

4. NIST Special Publication 800-18, revision 1; Guide for Developing Security Plans for Federal Information Systems, National Institute of Standards and Technology, February 2006.

Questions/Waivers

The Manager of Information Systems - ACOM is responsible for this policy. The Dean or designee must approve any exception to this policy or related procedures.

Questions should be directed to the Chief Information Security Officer.