Operations and Management Security Policy **Reviewed July 5, 2018**

Purpose

The purpose of this policy is to help ensure the secure operation of ACOM information systems and proper management of ACOM's IT security program and technologies.

Scope

This policy applies to all colleges, departments, administrative units, and affiliated organizations that use college information technology resources to create, access, store or manage College Data to perform their business functions.

Effective Date

This policy became effective on August 1, 2013

Authority

The ACOM Dean’s Committee, Business Contingency Planning, requires all departments, to develop "business continuity plans to ensure that all entities can continue critical operations during any disruption and resume normal operations within a reasonable period of time."

Information Technology Security Self-Assessment Policy, requires all divisions, to complete an annual self-assessment of the status of the security of its information systems.

Policy

1. Business continuity plan - Alabama College of Osteopathic Medicine must have a business continuity plan to guide recovery from disasters or other major disruptions to service in a manner that maintains the security of ACOM’s information systems and ensures timely restoration of services.

2. Configuration management - the configuration of servers, workstations, network devices, firewalls and other enterprise security technologies should be managed in a way that provides consistent setup, documents changes, and ensures security requirements are maintained when the configuration is changed.

3. Data backups - College Data must be backed up regularly and backup media stored securely, commensurate with the classification of the data.

4. Firewalls

- •All connections to networks outside the ACOM campus, such as the Internet, must be protected with a firewall that filters both incoming and outgoing network traffic against common threats.

•All enterprise information systems and any ACOM system hosting confidential data must be protected by a network firewall and a host-based software firewall, both configured in "default deny" mode for incoming traffic and enforcing documented trust relationships for those systems.
•All college computers connected to the college network must have a host-based firewall configured appropriately for the security requirements of the system and the classification of data stored therein.
•Logging should be enabled for all firewalls and periodically reviewed for anomalous events.
•Configuration of network firewalls and host-based firewalls on enterprise information systems should be audited periodically to ensure consistency with the security requirements of the system(s) they protect.

5. Security event logging and auditing

•Audit logs recording user activities, exceptions (i.e., errors or failures), and information security events should be generated commensurate with the security requirements of the system being monitored. Audit logs should be retained for at least 30 days.
•Enterprise information systems must log system administrator activities, such as the use of privileged accounts (e.g., supervisor, administrator, or root).
•Audit logs should be periodically reviewed to detect security violations.
•Security event log data must be protected against unauthorized access and alteration.
•Clocks of systems being monitored should be synchronized regularly from an accurate time source.

6. Security management - ACOM's IT security program and policies must be monitored and periodically assessed to ensure their continued effectiveness. The Director of IS or designee must perform an annual IT security self-assessment and submit a summary report to the ACOM Dean's Committee, as required by ACOM information technology policy.

Definitions

1. Authentication - Process of verifying one's digital identity. For example, when someone logs into Webmail, the password verifies that the person logging in is the owner of the User ID. The verification process is called authentication.

2. 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.

3. Default Deny - a firewall rule set that begins with blocking all network traffic, both incoming and outgoing, then only allowing specific network traffic required for the effective and secure operation of the system(s) protected by the firewall.

4. Enterprise information system - An information system and/or server providing services commonly needed by the College 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.

5. Firewall - A specialized device or software program that controls the flow of network traffic between networks or hosts to enforce security policies and provide protection for the resources on those networks or hosts. For the purposes of this policy, a router with Access Control Lists (ACLs) is not considered a firewall.

6. Trust relationships - A specification of the level of access granted to computer systems and/or applications that are trusted to access resources on a server and its associated data and applications. This applies to access controls between systems, not access rights for individual users or roles.

7. ACOM Computer - Any computer considered to be the property of Alabama College of Osteopathic Medicine.

8. College Data - Any data related to Alabama College of Osteopathic Medicine functions that are a) stored on ACOM 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).

9. College Network - Any part of ACOM's data network physically located on the Dothan campus. This includes devices on the network assigned any routable and non-routable IP addresses, typically 10.X.X.X, and applies to ACOM's wireless network and the network serving ACOM's student apartments at Summer Hill Apartments.

Roles and Responsibilities

1. Director of Information Systems (DIS) - Coordinates the development of guidelines, standards, and/or procedures related to this policy as well as the identification, implementation, and assessment of common security controls needed for this policy; monitors and periodically assesses ACOM's overall IT security program and policies; and ensures completion of an annual IT security self-assessment and report.

2. Information System Security Administrator - Ensures the application of appropriate operational security controls for an information system; coordinates with the DIS in the identification, implementation, and assessment of common security controls; ensures that backups are being performed regularly and stored securely; and ensures that components of an information system have an appropriate system of configuration management in place. This role may be filled by someone directly involved with the development, maintenance, and/or operation of the information system.

Implementing Procedures

1. Security event logging and auditing

a) Audit logs should include the following information, when relevant:

i. User ID or username
ii. Date and time of event
iii. Type of event
iv. Description of the event
v. Network addresses and protocols involved
vi. Files accessed
vii. Commands/processes executed

b) ACOM information systems should consider logging the following events and any others deemed appropriate for tracking important or suspicious actions:

- i. Successful and unsuccessful login or authentication attempts
- ii. Access to confidential data
- iii. Changes to access privileges for confidential data
- iv. Activation and de-activation of security systems such as firewalls, anti-virus systems, and intrusion detection systems, and alerts from these systems
- v. Privileged operations such as the use of privileged accounts (e.g., supervisor, administrator, or root), system start-up and stop, and I/O device attachment/detachment
- vi. System and network alerts and failure messages
- vii. Changes to, or attempts to change, system security settings and controls

Related Laws, Regulations, or Policies

1. Existing ACOM IT security operations and management policies
   - a. Vulnerability management - ACOM's requirements for assessing a system's security controls and identifying and mitigating vulnerabilities is in ACOM's "System Development and Maintenance Security Policy" Other related laws, regulations, or policies.
   - b. 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 Standards Organization http://www.iso.org. This is an international security standard that specifies security requirements for controlling access (see chapter 10, "Communications and operations management") to ensure "the correct and secure operation of information processing facilities."
   - c. NIST Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf, July 2008

Questions/Waivers

The Director of Information Systems is responsible for this policy. The Dean or designee must approve any exception to this policy

Questions relating to this policy should be directed to the Director of IS.