**Purpose**

Access controls are the rules that an organization applies in order to control access to its information assets. The risks of using inadequate access controls range from inconvenience to critical loss or corruption of data. This policy defines access control standards for system use notices, remote access, and definition and documentation of trust relationships for Alabama College of Osteopathic Medicine information systems.

**Scope**

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

Effective Date

This policy became effective on August 1, 2013.

**Policy**

Access control standards for ACOM information systems are to be established in a manner that carefully balances restrictions that prevent unauthorized access to information and services against the need for unhindered access for authorized users.

1. System use notice - Before a user gains access to an ACOM computer, a general system use notice must be displayed that welcomes users and identifies it as an ACOM system, warns against unauthorized use of the computer, and indicates that use of the system implies consent to all relevant ACOM policies. The general system use notice should also be displayed before a user gains access to an ACOM information system, where practical.

   The system use notice must state the following:

*Welcome to ACOM's information technology resources. Access to this system and all other electronic resources at ACOM is restricted to employees, students, or individuals with legitimate educational interest and are authorized by the College or its affiliates. Use of this system constitutes agreement to abide by all relevant ACOM policies. Do not continue unless you are authorized to do so and are informed about the Family Educational Rights and Privacy Act (FERPA).*

   Employee Acknowledgement:

*I understand that I may have access to information and data which contain individually identifiable information and acknowledge that the disclosure of this information to unauthorized persons or for un-official use may result in limitation or revocation of use privileges and/or administrative, civil, or criminal penalties. I understand that by my sign-on, I accept full responsibility for complying with these regulations.*

Remote access - Remote access control procedures must provide appropriate safeguards through appropriate identification, authentication, and encryption techniques. Direct log-on to campus computers from off-campus locations is not allowed. A remote user must first authenticate to an authorized campus remote access service with strong encryption, such as ACOM's VPN service or a departmental Windows Terminal Services (aka Remote Desktop Services) or connect.acomedu.org, before logging into a campus computer. This restriction does not apply to authenticated user access to web applications like SEAMED, Portal, Webmail, or to systems designed for public access.

For additional security controls for remote access, see "Data Security Standards," in ACOM's Data Classification and Security Policy.

2. Trust relationships - Trust relationships for centrally-managed College information systems or any system with confidential data must be defined and documented, approved by an appropriate authority, and periodically reviewed and revised as needed. Security controls, such as firewall rule sets, must be configured to enforce the trust relationships.

**Definitions**

1. Authentication - Process of verifying one's digital identity. For example, when someone logs into a workstation or server with their User ID, 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 College 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. ACOM Computer - Any computer considered to be the property of Alabama College of Osteopathic Medicine.

4. Local Network - Any segment of ACOM's data network physically located on the Dothan, Alabama campus. This includes devices on the network assigned any routable and non-routable IP addresses, typically 10.100.X.X, respectively, and applies to the wireless network and the network serving ACOM's student residence at Summer Field Apartments.

5. Remote Access - Accessing an ACOM local network from any physical location outside the Dothan, Alabama campus. This includes access from off campus using ACOM's VPN service.

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’s Data - Any data related to Alabama College of Osteopathic Medicine ("ACOM") 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).

8. VPN - Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

**Roles and Responsibilities**

1. Manger of Information Systems - is responsible for developing guidance on documentation and approval of trust relationships.

**Implementation Procedures**

1. The System Use Notice should be passively displayed such that no user action is required to view it before logging into the ACOM computer or information system.

**Related Laws, Regulations, or Policies**

A. Additional ACOM access control policies

1. Data access controls - access controls based on data classifications are specified in ACOM's Data Classification and Security Policy

2. Password security - Passwords are commonly used in conjunction with an identifying username to control access to information and information systems. ACOM's password requirements are listed in ACOM's "Security for Computing, and Network Resources" policy.

3. Unattended computers - security controls for preventing unauthorized access to unattended computers are defined in ACOM's "Security for Computing, and Network Resources" policy.

4. Vendor access - access controls for vendors or other third parties who need to access ACOM information systems for business reasons are defined in ACOM's Data Classification and Security Policy.

B. Other related laws, regulations, or policies

1. Alabama College of Osteopathic Medicine Data Classification and Security Policy

2. 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 11, "Access control") to ensure that access to information and information systems is limited to authorized users.

**Questions/Waivers**

The Dean of the Alabama College of Osteopathic Medicine 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 Manager, Information Systems - ACOM.