ACOM Security for Information, Computing and Network Resources Reviewed July 5, 2018

Purpose

To establish and maintain security requirements necessary to protect College information, computing and network resources, and minimize susceptibility to attacks on ACOM resources or from ACOM locations against other sites.

Scope

This procedure and accompanying requirements apply to all College locations and all system users at any location, including those faculty, students and staff using privately owned computers or systems to access College information, computing and network resources.

Security requirements shall be in place for the protection of the privacy of information, protection against unauthorized modification of information, protection of systems against the denial of service, and protection of systems against unauthorized access. Users are reminded that all usage of ACOM's information technology resources is subject to all College policies including the Information Technology Usage Policy.

General Policy

College information, computing and network resources may be accessed or used only by individuals authorized by the College. The College encourages the use of computing and network resources and respects the privacy of users. Nonetheless, the College may access information stored on the College's network of computers for the following purposes:

The extent of the access will be limited to what is reasonably necessary to acquire the information and/or resolve the issue.

1. Troubleshooting hardware and software problems,
2. Preventing unauthorized access and system misuse,
3. Retrieving University business related information, *
4. Investigating reports of violation of ACOM policy or local, state or federal law, *
5. Complying with legal requests for information, *
6. Rerouting or disposing of undeliverable mail,
7. Addressing safety or security issues

* The system administrator will need approval from the Director of Information Systems and the Dean of Student Services or the appropriate designee to access specific mail and data for these purposes.

To the greatest extent possible in a public setting individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on College-owned equipment.

Consequences for Noncompliance to Requirements

Systems that are found to pose a threat to the integrity of the information, computing and network resources may have their access to these resources suspended with the Director of Information Systems or the appropriate designee. The suspension of services will continue until the problem has been remedied and the system validated by the Dean of Student Services for operation within the ACOM information, computing and network resources environment. The College reserves the right to invoke emergency suspension of services without prior notification if the situation poses a serious threat to the information technology environment.

Requirements for Information, Computing and Network Security

The following system requirements represent the minimum standard that must be in place in order to establish and maintain security for College information, computing and network resources.

Initial Network Hook-up:

Each system must be capable of passing a test for vulnerabilities to hacker attacks and relaying of unsolicited email prior to being attached to ACOM's information, computing and network resources. System testing will be the responsibility of the Departmental/Unit or ACOM IS Staff.

Password Specification:

Password Policy: All passwords on any system, whether owned by ACOM or by an individual, directly connected to Alabama College of Osteopathic Medicine network must adhere to the following standards when technically possible. This includes devices connected to the campus network with a direct wired connection, wireless, dial-in modem, remote access software (e.g., Windows Remote Desktop), use of a Virtual Private Network (VPN), and the like. This policy applies to all passwords – User ID, system, user, database, application, etc. Any system that does not comply may have its network access blocked without prior notification. The password standards are maintained by the Manager of Information Systems - ACOM or designee. Exceptions must be approved by the Dean or designee.

Password Standards:

1. Passwords must have a minimum of 7 characters.
2. Passwords must contain characters from 3 of the 4 following categories:
    a. Uppercase letters
    b. Lowercase letters
    c. Numbers
    d. Special Characters (for example: !,@,#,$,%,^,&,*, etc. But be aware if traveling outside the U.S. that some symbols, like the U.S. dollar sign, may not be available on international keyboards)
3. Passwords cannot be the same as the ACOM User ID and not easily guessed (for example: no variants of the ACOM User ID, dictionary words, family names, pet names, birthdates, etc.).

4. Passwords must be changed at least twice a year (User ID password changes are during a designated time at the beginning of the fall and spring semesters).

5. Passwords must be changed significantly and cannot repeat more frequently than every two years.

6. Passwords that are written down or stored electronically must not be accessible to anyone other than the owner and/or issuing authority.

7. The same password used to access Alabama College of Osteopathic Medicine Systems (for example, your User ID password) must not be used for accounts or other forms of access to non-ACOM systems or applications such as online shopping, banking, etc.

8. Passwords must not be shared unless explicitly permitted by the issuing authority. User ID passwords must not be shared under any circumstances.

9. Anyone who believes their password has been compromised must immediately notify their departmental or college IT support, or the IT Help Desk to evaluate possible risks.

10. Default passwords in vendor-supplied hardware or software must be changed during initial installation or setup.

11. The User ID password must never be transmitted over the network in clear text (i.e., it must always be encrypted in transit). It is also strongly recommended that other types of passwords be encrypted in transit.

Unattended Computers

To protect against unauthorized access to data on computers left unattended, the following precautions are required:

1. Enable password protection on the screen saver for all college computers with the exception of special-purpose computers designed for public access, such as information or registration kiosks, public computers in the library, or computer labs where locking is undesirable due to the risk of a user monopolizing a shared computer. The length of time before the password-protected screen saver comes on should be set to 30 minutes or less. For lab situations, it is recommended that computers be set to automatically logout after at the most 30 minutes of idle time.
2. Never leave your computer unattended and unprotected. Before leaving your computer, lock the display or log out in a manner that requires a password to gain access.

Protection from Malicious Software and Intrusions:

Malicious software, or "malware", comes in many forms - viruses, worms, Trojan horses, denial of service attacks, botnets, spyware, adware, spam relays, etc. All pose a security risk, some of which are a very serious threat to the confidentiality, integrity, or availability of ACOM's information and technology resources. Appropriate precautions must be taken to protect ACOM systems and information from compromise by malware. To that end, ACOM may require the installation of essential security software on computers connected to the ACOM campus network or accessing ACOM information and technology resources. The following sections define specific requirements for antivirus, spyware/adware, personal

firewalls, and e-mail. Assuring the validity of malware protection software is the responsibility of each user, the department/unit representative, and the ACOM Information Systems Staff.

Virus Protection

1. The following computers must use the college-supplied antivirus software configured in a managed mode ("managed mode" allows a server to monitor and configure the antivirus protection on the client computer and push updates to the client on demand):

   a. Any college-owned computer

   b. Student-owned computers in ACOM residence halls (Connected to the “wired ACOM network”)

   c. Users of ACOM's Virtual Private Network (VPN) or connect.acomedu.org

   d. Users of ACOM's wireless or wired network if it is a college-owned computer or one that belongs to a current ACOM faculty, staff, or student.

2. All other computers accessing the ACOM campus network or information technology resources must be running active, up-to-date virus protection software. Current faculty, staff, and students may run the ACOM-supplied antivirus software on their home computers at no cost to meet this requirement.

3. Antivirus software must be activated when the computer boots up and remain active at all times during its operation.

4. Real-time file scanning must be enabled where files are scanned for malicious anomalies before they are written to the hard drive.

5. The version of the antivirus software (i.e., the antivirus program or engine) must be no more than one version behind the current version offered by the vendor or the version endorsed by ACOM, and must be supported by the vendor.

6. Virus definition files (i.e., the database in the antivirus software that identifies known malware) must be up-to-date with the most current version available from the vendor.

7. Checking for and installing updates to virus definition files and antivirus software must be automated and performed at least daily.

8. Comprehensive virus scans of all local hard drives must be performed at least weekly.

Spyware/Adware Protection

1. All computers connected to the campus network must run active spyware/adware protection software.
2. Spyware/adware definition/detection rules must be up-to-date with the most current version available from the vendor.
3. Scans of all local hard drives for spyware/adware must be performed at least weekly.

Personal Firewall Protection

1. All computers using the college-supplied security software (which includes virus, spyware, intrusion, and firewall protection) must have the firewall enabled.
2. Any other computer connected to the campus network must run a personal firewall. Microsoft Windows Firewall is an acceptable personal firewall.

E-mail Protection

1. All campus e-mail servers must provide antivirus protection that detects and mitigates infected e-mail messages.
2. Infected messages must be discarded or quarantined, not returned to the sender.

Security Patches

All systems connected to the campus network and the applications and databases running on those systems must have the latest security patches available from the respective vendors applied. Any system or application with known vulnerabilities for which a patch is not available must take appropriate measures to mitigate the risk, such as placing the system behind a firewall. Alabama College of Osteopathic Medicine may block access to the network for systems that have not been patched.

College/Departmental Systems

Colleges, departments, or other ACOM units may institute their own distributed computing system, as these provide valuable specialized services to users. These servers, in order to protect the College resources to which they are connected, must be kept no more than one version behind the current vendor-supported version of the operating system and application software and comply with all security requirements and standards set forth in this policy.

Assurance of server protection is the responsibility of the ACOM Information Systems Staff.

Enforcement

Enforcement of these policies and associated standards is the responsibility of the Director of Information Systems - ACOM or designee. Any system that does not comply with security policies and standards, is susceptible to a known vulnerability, or is compromised may have its network access blocked immediately and without prior notification to protect the integrity of other systems and data.

Any device directly connected to the campus network (i.e., with a direct wired or wireless connection, dial-in modem, remote access software like Windows Remote Desktop, use of a Virtual Private Network (VPN), and the like) may be scanned and assessed by designated ACOM information technology or Information Systems staff at any time to determine compliance with security policies and standards, or detect anomalous activities, vulnerabilities, and security compromises. Firewalls must be configured to permit this remote scanning function. Scanning may only be performed to the extent necessary to detect and assess the risk.

ACOM's Information Systems Staff has defined procedures for restoring network access after the vulnerable or compromised system has been repaired. The Director of Information Systems – ACOM

will determine whether the repair will require the computer to be reformatted and the operating system and all software and data re-installed, depending on the nature of the compromise.

Security Personnel Responsibilities:

College IT Security Officer (Director of Information Systems-ACOM): The College employee who leads the IT security program to protect ACOM's information, computing, and network resources. Responsibilities include assisting with college-wide IT security policies, controls and procedures; developing and maintaining security architecture, standards, and guidelines; monitoring compliance with IT security policies and standards; risk assessment; coordinating responses to security incidents; communication with organizations outside the College; chairing the Security Incident Response Team; and promoting training and awareness of the secure use of information, computing and network resources.

IT Security Analyst (Network\Security Systems Analyst): Technical personnel in information systems units assigned with responsibility for the secure operation of information, computing and network security at the enterprise level. Responsibilities include monitoring the state of information, computing and network security; detection and remediation of security incidents, implementation of preventative measures, configuration and management of security technology (for example, firewalls and intrusion detection systems), and communication of alerts and remedies to departmental/unit security representatives.

Security Incident Response Team (SIRT) (Information Systems Department): All members of the information systems division that provides advisory, proactive, and reactive support for ACOM's IT security program. Responsibilities include coordinating the campus-wide response to major security incidents; coordinating implementation of preventative measures in their colleges/units; communicating threats and best practices to their colleges/units; approving requests for restoring network access to vulnerable or compromised computers; participating in the development of IT security policies, standards, guidelines, and procedures; and assisting with IT security training and awareness efforts. SIRT duties should constitute no more than 30% of an individual's job responsibilities.

Departmental Security Representatives: The primary point of contact for departments for IT security matters. The departmental security representative serves as a liaison between SIRT and the department by assisting with communication, facilitating implementation of preventative measures in the department, and coordinating the response to security incidents involving technology or data within the department.

Deans and Department Heads: Responsibilities include authorizing access to computer systems in their units, ensuring that System Users understand and agree to comply with College and unit security policies, and ensuring that the technical and procedural means and resources are in place to assist in maintaining the security policies and procedures outlined above.

System Users: Responsibilities include agreeing to and complying with all applicable College and unit security policies and procedures; taking appropriate precautions to prevent unauthorized use of their accounts, software programs, and computers; protecting college data from unauthorized access,

alteration, or destruction; representing themselves truthfully in all forms of electronic communication; and respecting the privacy of electronic communication.

Questions

Questions regarding this policy should be sent to the Director of Information Systems - ACOM at support@acom.edu.