
1.7. Information Technology Security Policy

1.7.1. Purpose

The purpose of this document is to define and clarify the policies, principles, guidelines, and responsibilities related to the security of the AUA's information technology resources.

1.7.2. Principles

The AUA acknowledges the standards and expectations established by the University System Information Technology Security Policy. The Policy provides the following directions:

* Assignment of Responsibilities: Policy contains description of roles and responsibilities related to securing information resources.

* Consistency of Security Provisions: The AUA is maintaining access controls to servers, network, Internet) used to retain, access, or transport the information.

* Separation of Duties: The AUA administers security responsibilities separate from other duties that might result in compromises to the protection of the AUA's information resources.

* Expectation of Appropriate Security: Users of the AUA's information processing facilities can be confident that the facilities are secure and provide reasonable protection to the information the AUA retains or transports.

1.7.3. Scope

This policy applies to all AUA employees, AUA's students and others authorized to use the AUA's information technology resources.

Implementation of this policy helps to insure that the following characteristics apply to information technology resources:

* *Confidentiality* - sensitive information is protected against unauthorized access.

* *Integrity* - information is protected from tampering, unauthorized modification, or falsification.

* *Availability* - legitimate users of the AUA's information technology resources can access those resources in a timely manner.

1.7.4. Enterprise Roles

ICTS Department

On behalf of the enterprise, the Department will:

* Maintain security administration tools adequate for departments to control access to the information held, processed, or transported by the department on their behalf.

* Administer security for Computer Services staff and services.

* Assist departments with the implementation of access control decisions.

* Assure that security policy and technology are addressed in enterprise information technology planning and implementation projects.

* Establish AUA-wide standards for computing and network (AUA Computer and Network Appropriate Use Policy)

* Establish and implement strategies to periodically monitor compliance with security policy standards.

* Identify the names of custodians of AUA departmental databases. The custodian will be held responsible for proper distribution of individual access to AUA departmental databases.

* Ensure new AUA-wide software tools used to retain, access, or transport data are properly secured.

1.74.1. Roles and Responsibilities

The AUA has identified roles, responsibilities and relationships related to the security of information technology resources of the AUA.

The roles and responsibilities for security in the AUA include the following:

1.7.4.2. Chief Information Officer (CIO)

The AUA's Chief Information Officer (CIO) is the Director of ICTS. The CIO is responsible for the configuration of the AUA's information technology resources and for the development, promulgation, and enforcement of the university's security policies.

The CIO is responsible for issuing the security policies, procedures, and relationships among various information technology security functions within the AUA. The CIO appoints the Security Officer; all security functions report to the Security Officer who reports to the CIO.

1.7.4.3. Security Officer

The Security Officer is the AUA System Administrator.

The Security Officer will:

* Provide network perimeter, key servers', Internet key services security.

* Identify Associate Security Officer (or Security Associate) and assign responsibility for specific security functions.

* Monitor unusual activities, e.g., violation reports.

* Identify training requirements, determine the frequency of training, provide or assist in arranging for training for the Associate Security Officer.

* Develop AUA disaster recovery procedures.

* Develop and implement strategies to make users aware of security polices, procedures, and benefits; determine the frequency of awareness training and information.

* Communicate the direction for AUA security standards, procedures and guidelines.

* Enforce AUA security policies.

* Work with the AUA Physical Security Officer as needed.

The Security Officer is responsible for establishing processes to assure security, and communication with end users, including for example:

* Standardizing the format and process for all employees to acknowledge an understanding of the security requirements;

* Strategies and processes for regular reminders of the security responsibility of all users.

In case of urgent necessity the Security Officer can stop network services and investigate problems on the network even if it will require some privacy infringement.

The Computer Services may require pre- employment screening for the position of Security Officer and/or for individuals who are delegated the security functions.

The Chief Information Officer and Security Officer develop and disseminate guidelines and examples for users to assist them in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, etc. and should include but not be limited to information on passwords and password protection, logon id, virus protection strategies, etc.

Due in part to licensing requirements and software compatibility issues, AUA has a policy stating that installation of all workstation hardware and software must be authorized by the Computer Services.

Confidential information should not be on the workstation hard drive for security and business reasons. Most workstations pose a risk of unauthorized access because the "C" drives are not private or restricted to the user who is normally assigned to a workstation.

Software that includes a terminal locking feature, e.g. screen saver with password protection, must be available to all users. The use of password protection and terminal locking is mandatory for the security officer and security associates.

1.7.4.4. Associate Security Officer

The AUA Associate Security Officer is the AUA Network Administrator. It works under the guidance of the AUA Security Officer and report to him.

The AUA Associate Security Officer will:

* Provide AUA internal servers' and services security.
* Organize a timely update of security patches and virus definition updates.
* Establish access controls.
* Inform AUA users about new security patches and virus definitions updates.
* Assign access privileges based on matching the privilege to an appropriate job function.
* Perform the role of e- mail administrator adding new users and deleting those terminated their contracts.
* Performs housekeeping of the AUA users databases.
* Perform timely backups of the AUA network servers.
* Develop disaster recovery procedures for the AUA network servers.

The Associate Security Officer is responsible for establishing processes to assure security, and communication with end users, including for example:

- Publishing guidelines to create passwords.

1.7.4.5. AUA Computer Labs Security Officers

AUA Computer Labs Security Officers are lab supervisor and proctors. They are responsible for installation of security patches and virus definition updates on all lab computers. They are custodians of the lab workstations administrative passwords and are responsible for keeping them confidential. They are also responsible for physical security of lab equipment. Lab Security Officer can't leave his working place without a short -term transfer of the lab supervision to a devoted person.

1.7.4.6. AUA Departmental Database Custodians

AUA Departmental Database Custodians are department employees appointed by Heads of Departments. They work in cooperation with Security Officer and Security Associate and are responsible for:

* Security of departmental databases,

* Granting access rights to the departmental server information,

* Installation of patches and virus definition updates on departmental servers,

* Timely backup of departmental server information.

1.7.4.7. Workstation Security Officers

Workstation Security Officers are Computer Services software engineers. They are responsible for checking workstations software for viruses, antivirus program and other application program installation.

1.7.5. AUA Users

AUA Users include faculty, staff, students, and other customers who are authorized to use the information technology assets and have an access to the AUA network and Internet. AUA users are responsible for timely updates of virus definitions and installation of security patches according to Computer Services announcements.

1.7.5. Physical Access to Network Equipment

1.7.5.1. General Introduction and Requirements

The AUA has established controls over physical access to critical or sensitive hardware and the physical environment of that hardware for AUA. In addition to following the AUA guidelines, Computer Services has established more stringent controls over access to servers and enterprise network environment. Physical access to network servers may result in access to data on those systems.

AUA system and network administrators must work in cooperation with the AUA's staff in the Security Department to implement physical access and environmental control measures to protect the AUA's computing infrastructure. These security measures, which cover routers, gateways, bridges, all types of servers, desktop and laptop computers, and other mobile technology, should be commensurate with the value placed on the assets by the Department. Security measures should not adversely affect productivity and should be appropriate for the facility where the equipment is located.

All reasonable efforts should be made to ensure the safety and security of the hardware that comprises the AUA Network.

The following measures should be taken to physically safeguard the Department's information technology equipment and environment.

1. Risk Assessment & Security Review

The Department Head, or other department -assigned person, for each Department must periodically assess the physical security of information technology at each network site. The Departments' plans for security must be submitted to the AUA's Vice President and Chief Information Officer for approval. The Chief Information Officer, the Security Officer, the Security Associate, the Inventory Control Supervisor, and the Vice President will periodically review security procedures in all Departments.

2. Access Control

All Department production file, database, and communications servers and all other critical network related equipment should be in secure environments; test files and equipment should be secured when possible, but less emphasis is put on these. In all situations, the list of individuals who have access to secured areas must be on file with the Chief Information Officer, Security Officer, and Associate Security Officer.

1.7.5.2. Workstation Security

Reasonable efforts should be made to safeguard individual workstations. Workstations can be secured by securing the rooms where they are located and by physically attaching them to tables or work areas so that special tools are required to remove them from the premises. AUA also requires the following:

- Passwords should not be built into the logon script for auto- sign on.

AUA Faculty/Staff Workstations

Faculty and staff are on site during normal business hours from 9:00 a.m. to 5:45 p.m. Due to flexible schedules and project requirements faculty/ staff may be on site both earlier and later. AUA Faculty and Staff are responsible for keeping the doors of their offices locked in their absence. Unauthorized access to offices is partly controlled by Security Services.

Student Workstations

Student workstations are available in the main computer lab during the posted hours. Lab supervisor and proctors should be on duty for all hours of service. Students should be monitored when using computers in labs or classrooms. Computer classrooms are lo cked when classes are not in session.

1.7.6. Backups

All servers' information is backed up routinely. The AUA should have a Disaster Recovery procedures established by ICTS. Backup procedures for central servers and databases are developed by the Securit y Officer. The Security Officer in cooperation with departmental information custodians will develop disaster recovery and backup procedures for departmental servers and databases.

The Security Officer and Associate Security Officer will developed the schedule of backups.

1.7.7. Laptop and other portable technolog y

Portable technology refers to any model designed to be carried from place to place, such as notebook, laptop, cell phones, LCD panels, etc. This equipment may be connected to a server for terminal emulation where modems and authority are provided.

The following applies to all uses of portable technology:

- AUA employees or consultants who are granted this permission may check out portable equipment. Availability is on a first come, first served basis.
- The work unit responsible for the unit will maintain a checkout log. This log, which may be electronic, should include the user's name, date of pick - up and return, and where the equipment will be used. Checkout and check - in procedures will also include an inspection of the equipment, e.g. requisite cables and spare parts.
- Portable equipment and related software may only be used for AUA business.
- All copyright laws must be observed. Use of property for personal gain, or by non-AUA employees, except for authorized consultants, is prohibited.
- Where appropriate to the equipment and the location, it must be plugged into a surge protection device and kept in a locked, protective carrying case when not in use. Where possible, the equipment should be placed in a locked file or supply cabi net.
- Portable equipment should not be checked as luggage on airlines and should be under observation at all times.
- Equipment should not be left unattended unless appropriately secured.
- Equipment should not be left in a vehicle where it could be exposed to temperature damage or theft.
- Be observant of surroundings when using equipment on the road to access AUA systems.

1.7.8. Home Placement of AUA -Owned Computer Equipment

In some cases, job duties require network access from home and it may be undesirable to check out a Department laptop or use an individual's personal

computer. Requests for an AUA -owned computer to be placed in one's home will require justification, signoff by the employee's supervisor, and written approval from the Vice President and finally, a computer must be available for loan. A copy of the written approval should be sent to the Chief Information

Officer and the Inventory Supervisor. The Computer Services Chief Engineer will maintain a list of individuals with home computers, and this list will be available to those assigned to monitor any access activity.

1.7.9. Risk Assessment

Security is a critical application design feature. AUA will continue to use technology to secure data, e.g., security components of the Windows platform for the network. Risk must be assessed in relation to the following factors:

* Quality of the control mechanism
* Size of the threat
* Potential loss

Strategies for Security are cumulative and include:

* Low security required. Routine data backup, mechanisms to detect data corruption, and refresh corrupted data. Group ids are appropriate at this level only for general purpose/general access. The response to a security threat at this level is follow - up to determine the source of the threat depending upon the consequences of that threat to the university.

* Medium security required. Equipment is kept in locked facilities, user authentication is required at the time of access, individual user ids are required, passwords are encrypted, list of user ids to verify passwords, tools to assure that the individual accessing the system continues to be the person who logged on, possible time-out during long sessions to verify that the legitimate user continues to be the person accessing the system. The response to a security threat results in an examination of the source(s) of the threat.

* High security required. Equipment is kept in access -controlled facilities. Security measures include logging of users and access times, intruder detection alarms, regular security audits, encryption, and individual user ids. Network access of this device(s) should be excluded from access through the firewall. The response to a security threat results in energetic efforts to investigate the source of the threat and to implement strategies to prevent the threat from reoccurring.

1.7.10. Computer Crime

All users of information technology resources who are issued a user id must be aware that the following policy violations are considered as Computer Crimes:

* Accessing or attempting to access another individual's data or information without proper authorization (e.g., using another person's password to look at their personal information) Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained
* Tapping phone or network lines (network sniffers)
* Sending an overwhelming number of files across the network (e.g., spamming or e- mail bombing)
* Intentionally releasing a virus or other program that damages, harms, or disrupts a system or network
* Intentionally preventing others from accessing services
* Sending forged messages under someone else's id
* Unauthorized access to data or files even if they are not securely protected.

1.7.11. Escalation

If an exposure to a breach of security is identified, report the exposure to the Chief Information Officer as soon as possible. The CIO will determine:

* The best course of action.
* The number of individuals who need to know about the exposure.
* If the exposure is beyond the Department's boundaries and will affect the AUA.

If so, the CIO will report the exposure to the Vice President.

1.7.12. Training

The AUA's CIO will arrange for training for the Security Officer and those to whom the CIO has delegated authority. This training will address responsibility, authority, requirements for access and exemptions to access.

The AUA's CIO will regularly participate in training regarding responsibilities to design, implement, maintain, and upgrade a sound configuration of the AUA's information technology assets. The CIO will also participate in training regarding strategies to train security staff in security responsibilities.

The Security Officer will regularly participate in training regarding emerging technology and strategies to protect university information technology resources. Associate Security Officer will participate in training identified by the Security Officer.

The Database Custodians in the Departments will participate in training regarding their respective roles as custodians of university data.

All department users of electronic assets of the AUA will receive training regarding AUA security policies and procedures and their respective responsibilities in relation to protection of the AUA's information technology assets.