AMERICAN UNIVERSITY WASHINGTON, D.C.

IT Security Guidelines

1. General Use

AU encourages everyone associated with the university to act in a manner that is fair, mature, respectful of the rights of others, and consistent with the educational mission of the university.

Users should be alert to and report any abnormal behavior exhibited by computers or software applications since this may indicate the existence of a malicious program undetected by anti-virus software. Help to prevent problems by responding to suspicious network activities and unauthorized system use by reporting such activities to OIT by e-mail helpdesk@american.edu or by calling the Help Desk x2550.

2. Network User Names and Passwords

Passwords are the first line of defense for the protection of AU information system resources. Using good passwords will help reduce the possibility of unauthorized access and abuse of information. Below are some simple suggestions to assist with proper password management:

- Immediately change your password if it has been disclosed
- Protect all software and files containing formulas and algorithms used for the generation of passwords
- Never use your login name in any form as a password – either as-is, reversed, capitalized, doubled, etc.
- Avoid personal names as passwords – yours, your spouse, children, etc.
- Avoid using personal information as passwords that could readily be obtained or guessed – this could include license plate numbers, pet names, telephone numbers, social security numbers, the brand of your automobile, zip code, the name of the street you live on, etc.
- Avoid a password using several repeating digits or letters
- Avoid using words unless combined with numbers or punctuation marks
- Configure devices with separate accounts for privileged and unprivileged access, where possible, then, authenticate with an unprivileged account rather than a privileged account, switching to the privileged account only when and or as long as necessary while logging all activity. Note that password changes on all centrally-managed systems are synchronized so that one change updates all systems with the same password.

See OIT's web pages for tips on creating strong passwords.

3. Physical Security

Physical controls are often viewed as involving only physical access to a facility. However, physical controls also include access to controlled areas within a facility, access to computers or other network devices, handling of laptops, and location and handling of printers. Unauthorized access to

an unattended device can result in harmful or fraudulent use of the device or exposure of confidential or office-use only information stored within it or accessible through it.

Access to AU facilities should be controlled in a manner that provides security to the AU community and assets while providing for the detection of perimeter breaches. Since no physical security measure will withstand all intrusions, AU facilities should always be provided with a degree of physical protection commensurate with the value of the assets in, around, or accessible from that facility.

Users should protect their workstations in a manner that precludes unauthorized access to AU information resources. This would include logging out of computers when left unattended or invoking a password protected screen saver to deter unauthorized use. Encryption of files that contain protected information should be considered for the storage of protected information.

Laptop computers require special consideration in addition to those regarding general purpose desktop computers. When not in use the laptop should be stored in a locked cabinet or desk drawer, or otherwise secured with some type of physical locking device. When traveling, maintain physical control of the system at all times, and consider the use of removable media for storage of protected information while on travel.

Note that all AU facilities must also adhere to all local, state and national electrical, fire, and other appropriate codes and insurance requirements.

4. Elimination of Unnecessary Programs

Many devices automatically enable a variety of programs which are not necessary for the user's normal operating purpose (for example, allowing remote access). All unnecessary programs should be disabled.

5. Third-Party Services

Where appropriate, review documentation about the service provider's security controls (for example, in their "Statement on Auditing Standards (SAS) No. 70 Service Organizations" report).

6. Electronic Mail Usage Guidelines

E-mail service is primarily provided to support the academic and administrative functions of the university, and is intended to be a convenient way for students, faculty, and staff to communicate with one another and colleagues at other locations. It is not the practice of AU to monitor the contents of electronic mail messages. However, the information in electronic mail files may be subject to disclosure under certain circumstances; for example, during audit or legal investigations.

IT Security Guidelines

Users should not send e-mail so that it appears to have come from someone else or from an anonymous source. Users should not send unsolicited advertising via e-mail, or distribute communications that are intimidating or harassing.

Users should be aware that legal restrictions on sending or receiving copyrighted, obscene, and / or objectionable material may apply and use discretion when forwarding messages to others.

7. Internet Usage Guidelines

AU provides Internet access primarily to enable the conduct of academic and administrative activities in support of the university's mission. The following guidelines for Internet usage should be noted:

- Access to Internet resources from on-campus AU facilities must be made using Internet access arranged or approved by OIT
- When using the Internet from the AU network, you are presenting yourself as a representative of the university and should conduct yourself in accordance with all aspects of University Policies
- Users must not download material from the Internet that is subject to copyright or other intellectual property right protections unless the material is governed by fair use principles or express permission to do so is granted by the material owner Users are encouraged to verify the authenticity and accuracy of materials sent via the Internet, and to use good judgment when deciding whether to download or open materials from people they do not know and organizations they did not contact.