AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Computer Use and Copyright Policy

Policy Category: Information Technology Policies

Subject: This policy prohibits individuals from accessing or attempting to access any account, file, and/or software for which they do not have specific authorization.

Office Responsible for Review of this Policy: Office of the President

Procedures: AU Web Copyright and Privacy Policy Statement

Related University Policies: Data Classification Policy, IT Security Policy

---

I. SCOPE

All AU faculty, staff, and registered students are given computing and network access privileges. Each person is assigned a computer account code (user ID or user name) that provides access to university computing resources and systems for instructional, research, and administrative purposes. Access to these resources is a privilege, not a right. Resources include networks, laboratory systems, residence hall systems, library systems, faculty and staff office systems, and software licensed by the university or its agents for use on university systems.

II. POLICY STATEMENT

Because the entire AU community relies upon computing resources and systems to use and store important and confidential data, including software and computer programs, it is morally wrong and strictly prohibited for individuals to access or attempt to access or view any account, file, and/or software for which they do not have specific authorization. Also, it is prohibited to disrupt, delay, endanger, or expose someone's work or university operations.

III. POLICY

Prohibited actions under this policy, include, but are not limited to, the following:

1. providing computer access to unauthorized persons (e.g., by loaning your account to someone else or disclosing someone's password to a third party);

2. disrupting access to a computer system, network, or files (e.g., by crashing a public system; releasing viruses; attempting to learn or alter someone's password; tying up computer resources, printers or operating systems; or using computer systems for illegal activities);
3. accessing or changing someone's files without permission;
4. downloading or uploading unauthorized copyrighted materials or any material that infringes on any third party intellectual property rights;
5. using email, messaging services, or any electronic communication service to harass, stalk or intimidate another person (e.g., by broadcasting unsolicited messages, repeatedly sending unwanted mail, or using another individuals' name or user name);
6. intentionally wasting resources;
7. using the network to violate any university policy or commit a criminal offense or to encourage conduct that would constitute a criminal offense, or otherwise violate any local, state, Federal, or international law or regulation, including, but not limited to, export control laws and regulations governing the transmission or retransmission of technical data from the United States;
8. using an AU computer system or network to make publicly available any sensitive personal information of another person without that person's consent (sensitive personal information includes but is not limited to AU ID, social security numbers, and credit card numbers);
9. using the network to upload, post, e-mail, or otherwise transmit any unsolicited commercial advertising, non-university related promotional materials, or other forms of inappropriate solicitation to other users including, without limitation, "junk mail," "spam," "chain letters," or "pyramid schemes";
10. interfering with or disrupting the AU websites or servers or networks connected to AU, or violating any requirements, procedures, policies, or regulations of networks connected to AU; and
11. uploading or transmitting information or material that contains virus, or other harmful content.
12. refrain from using University resources for commercial purposes or for personal financial or other gain.

AU computing accounts are provided to assist in university and university-related work only. No commercial activity is permitted unless approved in advance and in writing by Information Technology.

Violations and Sanctions

Violations of this policy will be adjudicated by appropriate university processes and may result in the following sanctions:

1. temporary or permanent loss of access privileges;
2. university judicial sanctions as prescribed by student, faculty, or staff behavioral codes, including dismissal or termination from the university;

3. remedial education;
4. monetary reimbursement to the university or other appropriate sources;
5. prosecution under applicable civil or criminal laws (violations of local, state and federal law may be referred to the appropriate authorities).

The university will take any action that in its sole discretion is necessary to investigate and address violations of this policy, including temporarily or permanently terminating computer use privileges pending the outcome of an investigation or a finding that this policy has been violated.

Network Security

In order to provide secure electronic communications, the university must protect the physical and logical integrity of its networks, systems, data, and software. Some potential security threats include unauthorized intrusions, malicious misuse, and inadvertent compromise.

Each account is assigned to a single individual, who is responsible for all computer usage under that account. Any attempt to circumvent or subvert system or network security measures is prohibited. In the event of alleged or detected prohibited activities, the university will pursue the owner of the account. Individual passwords

should be kept secret, not shared, and changed periodically to prevent unauthorized access.

Privacy

As a matter of course, university IT staff do not look into private, individual accounts and data. However, the university reserves the right to view or scan any file or software stored on university systems or transmitted over university networks. This will be done periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of university resources. Policy violations discovered in this process will be acted upon.

Electronic mail and messages sent through computer networks, including the Internet, may not be confidential while in transit or on the destination computer system. Any data on university computing systems may be copied to backup devices periodically. IT will make reasonable efforts to maintain confidentiality, but individuals may wish to encrypt their data. If unsupported encryption software is used, the individual is responsible for remembering the encryption keys. Once data is encrypted, IT staff will be unable to help recover it should the key be forgotten or lost. Note: the university has enterprise encryption software available that is managed by IT.

Copyright

AU respects the rights of copyright owners, their agents, and representatives and is committed to implementing procedures and policies to support their rights without infringing on legal use of those materials by individuals. Legal use can include, but is not limited to, ownership, license or permission, and fair use under the U.S. copyright law.

Users of university computer resources and systems are also prohibited from making or using illegal copies of copyrighted materials or software, storing such copies on university systems, or transmitting them over university networks. Any misappropriation of intellectual property may be grounds for disciplinary actions. Such misappropriations include plagiarism, invasion of privacy, unauthorized access, trade secret and copyright violations, violations of federal, state or local laws, and university regulations and policies that are specific to computers and networks.

Notice and Take-Down Procedures

A. Designated Agent

In accordance with the Digital Millennium Copyright Act (DMCA), American University has designated an agent to receive notification of alleged copyright infringement occurring on university web pages or computer servers. For suspicions of copyrighted infringement on a university page or server, you may notify the university's Designated Agent for complaints under the DMCA:

Cathy Hubbs
Chief Information Security Officer
Office of Information Technology
American University
Email: hubbs@american.edu

Phone: 202.885.3998
American University
4400 Massachusetts Ave., NW
Washington, DC 20016

B. Complaint Notice Procedures for Copyright Owners

DMCA requires that all notices of alleged copyright infringement be in writing and inform the Designated Agent of the following:

1. identify the work that was allegedly infringed;
2. describe the allegedly infringed work and provide sufficient information to identify the location of the infringement;
3. state that you have a good faith belief that the use of the work in the manner complained of is not authorized by the copyright owner, the owner's agent, or the law;
4. certify that the information you provided is accurate and that you attest under penalty of perjury that you are authorized to enforce the copyrights that you allege were infringed;

5. provide your contact information, which includes an address, telephone number, and e-mail address; and
6. include your physical or electronic signature.

C. Take-down Procedures of Alleged Infringing Work

When properly notified of the alleged copyright infringement, the Designated Agent will send the information to university IT. IT will determine whether the alleged infringing work exists as described. IT will notify the user to take down the existing alleged infringing material and disable access to avoid continuing the alleged infringement. Once the user has notified IT that the infringing material has been removed from his/her computer and stated they have reviewed this policy, the user's access will be reinstated.

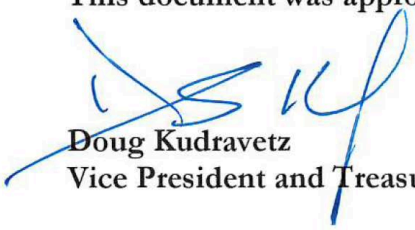
D. Sanctions

Individuals who have been found to infringe copyrighted materials on the university network are subject to disciplinary proceedings under the Computer Use and Copyright Policy, Faculty Manual, Student Code of Conduct, and Staff Manual of Personnel Policies.

IV. SIGNATURE, TITLE AND DATE OF APPROVAL

This policy need to be signed by the appropriate officer (listed below) before it is considered approved.

This document was approved and signed by



Doug Kudravetz
Vice President and Treasurer

David Swartz
Vice President and CIO

Date Approved:
April 26, 2004
Revision October 2010;
Revision February 2015
Revisions March 2018