AMERICAN UNIVERSITY
WASHINGTON, DC

University Policy: Responsible Use of University Technology Resources

Policy Category: Information Technology

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.

Responsible Executive: Vice President & Chief Information Officer

Office(s) Responsible for Review of this Policy: Office of Information Technology

Supplemental Documents: Technology Resource Usage Standard

Related University Policies: Data Classification Policy, Intellectual Property Policy, IT Security Policies

---

I. SCOPE

AU faculty, staff, students, and contingent workers (e.g., contractors, university affiliates) are given access privileges to university network and technology resources. To grant this access, a person is assigned a technology user account (user ID or username) that provides access to university technology resources for educational, instructional, research, operational, and administrative purposes. Access to these resources is a privilege, not a right.

II. POLICY STATEMENT

Because the entire AU community relies upon computing resources and systems for teaching, learning, administrative, and operational purposes, it is unethical 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. Members of the university community are expected to be good stewards of the university's technology resources and data, and use them in a safe, responsible, ethical, and legal manner.

For specific standards associated with the use of university technology resources and the life cycle of a user account, please see the Technology Resource Usage Standard.

III. DEFINITIONS

University Technology Resources: The full set of information technology services used to perform university operations, including all computer, telecom (voice, video, and data), and communication devices, and other technologies involved in the processing, storing, accessing, and transmission of information and data. Devices include but are not limited to, personal computers, printers, servers, phones, and network devices.

IV. POLICY

A. Prohibited Actions

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. Interfering with or disrupting access to use of a University Technology Resource (e.g., by disrupting a device, system or service; releasing viruses; attempting to learn or alter someone's password; wasting computer, printer, or telecom resources, systems, or services);
3. Accessing, editing, uploading, downloading, or otherwise changing someone else's electronic documents, files, or software without permission;
4. Downloading, uploading, or any other form of unauthorized sharing of copyrighted materials or any other materials that infringes on the intellectual property rights of another person or third party;
5. Using University Technology Resources to harass, stalk, intimidate, or impersonate another person or entity (e.g., by broadcasting unsolicited messages, repeatedly sending unwanted mail, posing as someone else, using another individual's name or username without authorization, etc.);
6. Using University Technology Resources to 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;
7. Using University Technology Resources to make publicly available any confidential and sensitive information of another person (including confidential information as defined by the Data Classification Policy) without that person's consent.
8. Using University Technology Resources to upload, post, email, 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;
9. Using University Technology Resources to violate any policies of or agreements with the university;
10. Using University Technology Resources to upload, download, or otherwise transmit information or material that contains malware or other harmful content;
11. Using University Technology Resources for commercial purposes or for personal financial or other gain; and using University Technology Resources to engage in commercial activity unless approved in advance and in writing by the CFO, Vice President and Treasurer.

B. 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 sanctions as prescribed by the Faculty Manual, the Student Conduct Code, and Staff Personnel Policies, 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 or otherwise limiting access to University Technology Resources pending the outcome of an investigation or a final determination regarding a potential policy violation.

C. Information Security

In order to secure university systems and data, including University Technology Resources, the university must protect its technology architecture, including but not limited to the physical and logical integrity of its networks, systems, data, software, and services. Security threats include, but are not limited to, unauthorized intrusions, malicious misuse, denial of service, and inadvertent compromise.

Each user account is assigned to a single individual, who is responsible for all technology resource usage under that account. Any attempt to circumvent or subvert information security measures is strictly prohibited. In the event of alleged or detected prohibited activities, the university typically initiates follow-up with the account owner.

D. Privacy

American University is committed to respecting the privacy of individuals and safeguarding their personal information. Authorized staff do not review private, individual accounts and data unless required to comply with university obligations imposed by judicial orders or legitimate requests from law enforcement or other regulatory bodies, to ensure the security or functionality of University Technology Resources or make determinations regarding potential policy violations.

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. The Office of Information Technology (OIT) 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, OIT staff will be unable to help recover it should the key be forgotten or lost. Note: OIT supports

whole disk encryption on university owned workstations.

E. 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 Technology Resources are 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. See the University's Intellectual Property policy for further information on copyright, patent, and intellectual property ownership.

1. 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:

Director of Cyber Policy
Office of Information Technology
American University
4400 Massachusetts Ave., NW
Washington, D.C. 20016
Email: dmca@american.edu

    b) Complaint Notice Procedures for Copyright Holders

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

a. Identify the work that was allegedly infringed;
b. Describe the allegedly infringed work and provide sufficient information to identify the location of the infringement;
c. 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;
d. 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;
e. Provide your contact information, which includes an address, telephone

number, and e-mail address; and
f. Include your physical or electronic signature.

2. Take-down Procedures of Alleged Infringed Work

When properly notified of the alleged copyright infringement, the Designated Agent will send the information to OIT. OIT will determine whether the alleged infringing work exists as described. OIT 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 OIT 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.

3. Sanctions

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

V. EFFECTIVE DATE AND REVISIONS:

This Policy is revised effective October 30, 2023

This Policy was approved April 26, 2004 and amended October 2010, February 2015, and March 2018.