Augusta University
Policy Library

Acceptable Use of Information Technology

Policy Manager: Chief Information Security Officer

POLICY STATEMENT
It is expected that all users of information technology resources use them responsibly and to the benefit of the mission of Augusta University (AU). This policy applies to members of the Augusta University community and affiliates who use AU's computer and data resources and/ or who have access to sensitive data sent, transmitted, viewed, received, or stored on these resources. Each business unit may prescribe procedures that are more restrictive than this policy, but not less restrictive.

This policy is in accordance with guidance of the University System of Georgia, USG IT Handbook.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☒ Visitors
☒ Other: All individuals using enterprise technology resources.

DEFINITIONS
Affiliates: Refers to individuals who have contractual or other relationships with the University and who are not employees, faculty, or students.

Authorization: In this context means to grant permission to an identified individual to use a computer or data resource. Acceptance of authorization to use AU computer and data resources establishes an obligation on the part of the individual to use those resources responsibly.

User: A user is any employee, contractor or individual who has been granted authority or access to use AU information technology resources to carry out their job responsibilities and/or to support enterprise business, clinical and/or academic endeavors. This definition includes students who may be using the information technology resources as part of their academic pursuits or in their capacity as part-time, temporary employees. Sensitive Data is institutional data that is not legally protected but should not be made public and should only be disclosed under limited circumstances. Users must be granted specific authorization to access since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

Computer Data: Computer and data resources include computers and computing devices, both wired and wireless; computing, application, and database access (including passwords); software, hardware, computer, and email services; and associated computing accounts. Computers and computing devices include, but are not limited to, desktops or laptop computers, smartphones and cellphones, USB flash memory drives, or similar devices, and all other mobile devices on which High Risk Data may be sent, transmitted, viewed, received or stored.

Office of Legal Affairs Use Only
Executive Sponsor: VP for Information Technology
Next Review: 6/2024

Confidential/Regulated Data: Institutional data for which there is a legal obligation not to disclose. These data elements require the highest levels of restriction due to the risk for harm that will result from disclosure or inappropriate use.

Members of the University (AU) community: Refers to full- and part-time employees, faculty, and students.

Port scanning: Is using a software application designed to probe a network host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

PROCESS & PROCEDURES

Privacy and Ownership

Augusta University information systems are the property of the enterprise. The information on the enterprise's systems is also the property of AU, unless applicable laws, contracts or policies indicate otherwise. All users should have no expectation of privacy in any data, format, or other kind of information or communications transmitted, received, printed, stored, or recorded on any of these systems. AU reserves the right to monitor all employee usage of these systems and to intercept and review any data or communication, in any format, including but not limited to social media postings and activities. You consent to such monitoring by your acknowledgement of this policy and/or your use of such assets and systems. The enterprise may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice. Do not use the enterprise's electronic communications assets for any personal matter that you desire to be kept private or confidential. Information created using AU's technology resources remains the property of AU.

Every employee has a responsibility to promptly report the theft, loss, or unauthorized disclosure of proprietary information, protected health information, and computing devices.

You may access, use, or share Augusta University's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Accessing the enterprise's network from a remote site (i.e. home, hotel, etc.) can be done using a virtual private network client. The same policies, standards, and guidelines for computer and network use apply when this connection is active.

Policy Requirements

1. Acceptance of *authorization* to use AU *computer and data resources* establishes an obligation to:
    - behave in accordance with AU's educational, research, and service purposes and in a manner compliant with this and other applicable AU policies and procedures and all applicable laws and regulations;
    - not use your account for any commercial purposes;

- behave with civil regard for other members of the AU community and of the wider community on the Internet;
- take reasonable steps to ensure that any computer used to access AU resources, whether it is located on an AU campus or elsewhere, is secure, virus-free, and otherwise not compromised;
- protect the confidentiality, security, integrity, and recoverability of all *computer and data resources* and take reasonable and appropriate steps to guard these resources from improper or unauthorized use, including such use by third parties;
- use applications that conform to AU's privacy and security policies and guidelines;
- refrain from activities that interfere with the ability of others to use *computer and data resources*; and
- be aware of and comply with other relevant University policies, procedures, and business rules and applicable local laws and regulations; in all cases the more stringent standard should be followed.

This obligation applies regardless of:

- where the computer used to access *computer and data resources* is located in an AU office, classroom, public space, or lab, or at home or elsewhere outside the University;
- who owns the device used to access or store the *sensitive data*; or
- the form or manner in which *sensitive data* are stored or transmitted, including, but not limited to, local file, shared file, file on removable media such as CD-ROM disk and jump drive, central database, fax, printer, copier, network, phone, email, or voice mail.

2. Access and use, or causing or allowing access and use, of *computer and data resources*, including email services, by anyone other than as permitted by AU is strictly prohibited by AU and by state and federal laws and may subject the violator to criminal and civil penalties as well as AU-initiated disciplinary proceedings.

3. Use of some AU *computer and data resources* may be governed by additional University, college, school, or departmental policies and procedures. Anyone authorized to use these resources is responsible to become familiar with and abide by such policies and procedures.

4. In order to safeguard the security and efficiency of *computer and data resources*, AU computer systems are routinely monitored and recorded for integrity and operation of the system by authorized University staff. *Computer and data resources* provided by AU are the property of AU and not the personal property of the individual.

5. Designated individuals at the University entrusted with overall responsibility and management of *computer and data resources* and *sensitive data* and related systems have decision-making authority for authorizing access to and use of those resources and systems.
    - These individuals at the University include, but are not limited to, University-wide administrators, such as the Registrar, Deans, and other School administrators, and individuals responsible for Research on data-intensive research projects.

- These individuals at the University have responsibility for the development, implementation, and maintenance of policies and procedures related to authorizing access to the shared stores of the various categories of *sensitive data* in use in electronic form at AU and for handling that data appropriately wherever it resides. Such individuals may delegate responsibilities, as they deem appropriate, in specific functional areas.
- These individuals at the University may have more stringent standards for the use, storage, and transmittal of the data they manage than those set forth in this policy; the more stringent standard should be followed. Individuals authorized to use the data are expected to be aware of relevant current policies and to abide by them.
- Access to *sensitive data* will be granted only on an "as needed/minimum necessary" basis.

6. Augusta University's Chief Information Officer is responsible for periodic reviews of the University's security policies and procedures relating to *computer and data resources* and *sensitive data*, which will be revised as necessary and any updates publicized. Current versions of the University's policies relating to *computer and data resources* and *sensitive data* are maintained on the AU IT website (https://www.augusta.edu/compliance/policyinfo/policies.php).

7. Cybersecurity Caveat
Be aware that although computing and IT providers throughout Augusta University are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as:
   - Safeguarding their account and password
   - Taking full advantage of file security mechanisms
   - Backing up critical data on a regular basis
   - Promptly reporting any misuse or violations of the policy
   - Using virus scanning software with current updates
   - Using personal firewall protection
   - Installing security patches in a timely manner

   Every user of AU IT resource has an obligation to report suspected violations of the above guidelines. Reports should be directed to the institution, unit, center, office, division, department, school, or administrative area responsible for the particular system involved.

8. Violators of this policy may be subject to disciplinary action, up to and including the termination of employment or contract with the University, or, in the case of students, suspension or expulsion from the University. Anyone who knows or has reason to believe that another person has violated this policy shall report the matter promptly to his or her supervisor, in the case of students to the Division of Student Affairs, or as appropriate. Any attempt to retaliate against a person for reporting a violation will itself be considered a violation of the policy and may result

in disciplinary action up to and including the termination of employment or contract with the University. The appropriate office or entity, including the Office of the Vice President, Chief Information Officer, the University council, and other University officials as required, will lead the investigation into all alleged violations or reports of violations of this policy and, where appropriate, will take steps to remedy the situation.

SPECIFICATIONS

1. **AU Computer Security**

Computer security controls are based on the construct that the data on an individual machine/device influences the classification of that machine/device and, in turn, the multi-layer security strategy for defense against unauthorized access.

Safeguarding Computers for Individual Use

This section describes measures to safeguard computers typically used by individuals in AU-related activities and for accessing other University resources. As used in these operational specifications, "computers" include but are not limited to desktops or laptop computers, smartphones and cellphones, USB flash memory drives, or similar devices.

Physical Security

- not give physical access to computers to unauthorized persons.
- Take appropriate precautions to prevent theft and damage.
- Where possible, position monitors to prevent casual viewing by visitors or passersby.

System Security

- Install anti-virus software and keep virus definitions up to date.
- Install operating system and software patches and take other recommended steps to mitigate known vulnerabilities of the computer in a timely manner.
- Use only AU-approved software; do not download unauthorized software.
- Use a locking screensaver or other mechanism to prevent unauthorized use of the computer.
- Do not leave your computer unattended without locking it or logging off.
- Do not install or use Peer-to-Peer file sharing software that is not AU-approved; these programs typically enable unauthorized remote access without any password to the contents of the computer.
- Do not install or run software that requires a license without that license. Respect license agreements and do not infringe on the copyright of others. (See section A.4)
- Respond promptly to notices from authorized University staff that vulnerabilities have been detected in your computer's system.
- Take particular care to secure your AU-access information (e.g., log-ins, passwords) on home computers from unauthorized use by others.

- Do not install unsecured third-party applications that may deliver malware to a personal device on which you may have High Risk Data, thereby putting AU at breach risk.

Passwords

- Where possible, secure all computer accounts with passwords, and use passwords to protect all file sharing.
- Use strong passwords. Strong passwords consist of at least eight (8) characters. They should not be dictionary words or readily guessable. They should include at least three (3) of the following four (4) characteristics in any order: upper case letters, lower case letters, numbers, and symbols.
- Change passwords periodically. Avoid reusing a password for at least several change iterations. If you have multiple accounts, avoid using the same password for those accounts. Additional information about passwords may be found in the Password Protection Policy.
- Do not keep passwords in plain text in a computer file or in plain sight on paper. Passwords should neither be sent in an email nor provided verbally by telephone. If you must communicate account access information in order to ensure business continuity, you should communicate it in a secure manner. Supervisors and managers should make certain that offices have plans for access to files and data for business continuity.
- Keep a well-secured copy of your passwords available for emergency access. Encrypt any computer file containing passwords. Keep any written file of passwords in a physically secure location, preferably separate from the computer or application they secure.
- Passwords for sensitive websites or email accounts should not be saved on the computer.
- Where possible, do not configure programs to automatically store passwords.
- Shut down web browsers, email programs, or other applications that might store passwords temporarily when they are not in use.

Remote Access

- See Remote Access Policy

<u>Business Continuity</u>

Take reasonable steps to ensure that, in case of emergency, another authorized person is able to access the AU computer you use in order to provide continuity of AU functions performed on and through it. The University's business interests should be balanced with data safeguards and privacy. There are numerous methods available of ensuring shared responsibility for data and systems rather than sharing passwords. For assistance, contact the AU Cybersecurity Team (72CYBER@augusta.edu).

Purchasing
Discuss adherence to applicable AU policies and procedures as part of the purchasing process. Computers and software acquired for use with AU *computer and data resources* should conform to these specifications. See Procurement of Information Technology.

Software Licensing
Software users shall use and install only properly licensed software on AU computers and the AU network.

- *Unauthorized* duplicating, distributing, downloading, sharing, selling, or installing software and related documentation or using unlicensed software and related documentation constitutes a violation of the software license agreement and of University policy.
- Each department or other unit is responsible for ensuring that software used on their computers is properly licensed, for adhering to the terms and conditions of those software licenses, and for maintaining appropriate documentation of those software licenses.
- Upon separation from AU, all University-owned software, including all AU-licensed software, must be removed from non-AU owned computers. This includes mobile devices, laptops, and home computers. If you have software on your office computer that permits you to install a second copy on your home computer, remove that second copy.

Equipment Disposal or Redeployment

- See Securely Disposing of Electronic Media Policy

2. **AU Data Security**
How you handle non-public data depends on its data classification. The more restrictive the data is, the better it should be secured. Consult the Data Management and Classification Policy for requirements; the following are more general requirements.

Protecting *Sensitive Data* on Computers

- Follow *AU Computer Security Specifications* set forth above.
- Know what data are stored on your computer, the sensitivity of that data, and what policies apply.
- Keep local data retention to a minimum. Rely on unit, department, or University storage where you can.
- Where possible, password protect or encrypt sensitive data.
- Back up local data on a regular basis and keep the backup secure. Protect backups with the same level of security as the original data. Test backup recovery periodically to verify that it works.
- If you use a computer shared with others, take appropriate precautions to safeguard sensitive data that others may not be authorized to access. Where possible, create separate accounts for each person who uses the computer, setting appropriate permissions.

Storing or Transmitting Sensitive Data

- Do not redistribute *sensitive data* to others within or outside the University, unless you are an authoritative source for and an authorized distributor of that data and the recipient is authorized to receive that data.
- Do not allow *sensitive data* to be stored on computers or servers outside AU, unless such storage is authorized.
- Whenever possible, *sensitive data* should be transferred in encrypted form, e.g., using SSL (Secure Socket Layer) or SSH (Secure Shell).
- Remember that email typically is not a secure form of communication. Care should be taken to be certain that the recipient is authorized to receive that data and the address is accurate.
- *Sensitive data*, including electronic protected health information (EPHI), Social Security numbers, or credit card information, should not be sent unencrypted via email. If use of email is necessary, use encryption technology to protect the transmission of *sensitive data* in email. This may include the use of VPN (Virtual Private Network), SSL, or encryption of the message itself using approved software.
- Do not transmit *sensitive data* using instant messaging technology such as Slack, WhatsApp, and Facebook Messenger, which use servers outside of AU. These services may allow *sensitive data* to be accessed by or stored by unauthorized parties. It is recommended that you consult with AU IT Global Office of Information Security (72CYBER@augusta.edu) for guidance.
- Take special care when sending *sensitive data* by fax to make sure that it is clearly marked as confidential. Every effort should be made to ensure that only the intended recipient has access to the faxed information.
- Keep fax machines, printers, and copiers used for sensitive data in secure areas. Faxes, printouts, and copies of *sensitive data* should be picked up promptly and handled appropriately.

Disposing of Sensitive Data

- *Sensitive data* should be destroyed in a manner that prevents re-creation.
- Reformat or physically destroy any removable storage media (such as floppy disks, zip disks, tapes, or compact disks (CD)) that contained *sensitive data* before disposing of them.
- Shred printouts of *sensitive data*.
- Ensure that *sensitive data* are removed from devices you use, including remote printers, before you dispose of or re-deploy those devices.

See Securely Disposing of Electronic Media Policy

Responding to Requests for Information

- Do not share *sensitive data* with representatives of the press (radio, television, print, or electronic media), other individuals, or in public forums, such as mailing lists or web bulletin boards, without appropriate *authorization*.
- Refer subpoenas and similar requests or demands for the release of *sensitive data* to the Department of Legal Affairs.

POLICY COMPLIANCE

Exceptions

Any exception to the policy must be approved by the Cybersecurity team in advance.

REFERENCES & SUPPORTING DOCUMENTS

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
Health Insurance Portability and Accountability Act (HIPAA) of 1996 Privacy and Security regulations
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended
Acceptable Use Policy
Privacy Rule (16 C.F.R. Part 313)
USG IT Handbook

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021