Augusta University
Policy Library

Acceptable Use of Information Technology

Policy Owner: Information Technology Support and Services

POLICY STATEMENT
It is expected that all users of information technology resources use them responsibly and to the benefit of the enterprise's mission. Each business unit may prescribe procedures that are more restrictive than this policy, but not less restrictive.

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: Include any other stakeholders not listed above.

DEFINITIONS
For the purpose of this policy a user is any employee, contractor or individual who has been granted authority or access to use Augusta University's 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.

Confidential/Regulated Data is 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.

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

Office of Compliance and Enterprise Risk Management Use Only
Policy No.: 580
Policy Sponsor: Chief Information Security Officer
Originally Issued: Not Set
Last Revision: 07/10/2017
Last Review: 06/16/2017

Augusta University information systems are the property of the enterprise. The information on the enterprise's systems is also the property of Augusta University, 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. Augusta University 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 Augusta University's' technology resources remains the property of the enterprise.

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.

Acceptable Use

Augusta University expects all users of computing resources to use them responsibly and productively.

While incidental personal use of electronic resources is not necessarily unacceptable, personal use must not adversely affect the performance of an employee's official duties, must not be disruptive of co-workers, must be of limited duration and frequency and should be restricted to matters that cannot be addressed during non-duty hours. An illustration is something analogous to using your office phone to call your sitter to let him/her know you're running late.

To the extent an employee is forced by business circumstances to make personal use of the enterprise owned devices, such use should be incidental and immaterial and never add costs to the enterprise.

Unacceptable Use – The following activities are strictly prohibited.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Augusta University.

2. Knowingly introducing malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, etc.)

3. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4. Interfering with the operation of any information system with the intent to disrupt the normal operation of the system.

5. Attempting to circumvent the security controls of any information system or host.

6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

7. Port scanning or security scanning unless these duties are within the scope of an employee's normal job responsibilities and with proper authorization.

8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty and with proper authorization.

10. Providing sensitive or confidential data to parties who do not have a legitimate or official need to know, including both internal and external to Augusta University, without obtaining authorization.

11. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Examples would include, creating or forwarding chain email letters.

12. Using computing resources to harass another individual.

13. Impersonating another individual or device including "spoofing" one's identity or forging of email header information.

14. Assisting, encouraging, or concealing from authorities any unauthorized use, or attempt at unauthorized use, of the enterprise's information systems, hosts, or network facilities. Computers and networks are just like any other Augusta University facilities - they are to be used only by people who have permission.

15. Using the enterprise's resources for personal or commercial gain or benefit except in connection with scholarly pursuits.

16. Using enterprise's computing resources for political campaigns.

17. Absent a legitimate academic or research purpose, use of Augusta University's electronic resources by faculty, staff, students, student employees, vendors, contractors, temporary employees, and visitors to intentionally view, print, display, distribute, retransmit, or otherwise disseminate sexually explicit or obscene content. For the strict prohibition of child pornography, see 18 below.

18. Use of Augusta University's electronic resources by faculty, staff, students, student employees, vendors, contractors, temporary employees, visitors or **any other person** to view, print, display, distribute, retransmit, or otherwise disseminate child pornography. Such viewing, printing, displaying, distributing, retransmitting or other disseminating is strictly prohibited by federal and state criminal laws. Any incident involving child pornography must be immediately reported to Public Safety as required by law and Augusta University policy.

REFERENCES & SUPPORTING DOCUMENTS

Intentionally left blank.

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

President, Augusta University and CEO, AU Health System Date: 06/16/2017