Information Technology (IT) Professionals Code of Conduct

I. POLICY STATEMENT

All Auburn IT professionals will sign an annual acknowledgment that they have read, understand, and will comply with the IT Professionals Code of Conduct.

II. POLICY PRINCIPLES

Auburn University IT professionals must be educated in and follow the IT Professionals Code of Conduct. The IT Professionals Code of Conduct will be reviewed on an annual basis and updated if necessary by the Office of the CIO.

III. EFFECTIVE DATE

Adopted: October 3, 2018

IV. APPLICABILITY

Auburn University Information Technology Professionals

V. POLICY MANAGEMENT

***Responsible Office*:** Office of Chief Information Officer
***Responsible Executive*:** Chief Information Officer (CIO)
***Responsible Officer*:** Chief Information Security Officer (CISO)

VI. DEFINITIONS

Information Technology Professionals are individuals who maintain, build, repair or assist users with hardware and software associated with computer systems or other components related to information processing. At times, individuals with non-IT titles may be required to interact with IT resources. Faculty, staff, students, researchers, and temporary workers are equally bound by this Code of Conduct when performing IT related tasks.

VII. POLICY PROCEDURES

- IT staff will receive communications on the IT Professionals Code of Conduct.
- IT staff will be required to annually review and affirm the IT Professionals Code of Conduct.
- IT leadership will provide guidance on the IT Professionals Code of Conduct as challenges are observed or encountered.
- IT leadership will review and revise the IT Professionals Code of Conduct as needed in response to any incidents or as technology changes.

VIII. SANCTIONS

Deliberate violation of this policy will be subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

If a need arises for exceptions to the principles and examples in the IT Professionals Code of Conduct document, approval must be obtained from the University CIO or the CISO.

X. INTERPRETATION

The Chief Information Officer

AUBURN UNIVERSITY
INFORMATION TECHNOLOGY PROFESSIONALS
CODE OF CONDUCT

IT professionals:

- May have access to users' electronic information, some of which may be personal and confidential.
- May require access to users' electronic information in order to develop, test, implement and support the University's applications, systems and networks to ensure they run properly; to protect against threats such as attacks, malware, and viruses; to protect the integrity and security of information; to help support business continuity; and to respond to threats to campus safety and the safety of individuals.
- Should understand that part of their job is to help protect all users' electronic information from inappropriate use and unauthorized access.

All Auburn IT professionals will sign (may be electronic) that they have read, understand and will comply with the IT Professionals Code of Conduct.

As an IT professional, I:

- Will not knowingly violate University or departmental policy, state or federal law governing information privacy
- Will not access information or data as defined in the Auburn Data Classification Policy or proprietary information or data on Auburn University computer systems, or in any other manner, except when it is in keeping with assigned duties as an employee.
- Will not use social media sites to make comments about, or post work details or photographs of, other employees, students or other associates in a manner that breaches an individual's privacy rights. This includes where individuals are not named, but can be readily identified by themselves or others from the information posted.
- Will only obtain the information needed to perform my job or that I have been directed to obtain by proper University authorities.
- Will appropriately maintain and protect the confidentiality of any information or data to which I have access, regardless of the method used to retrieve or display it.
- Will only use the information gathered for the purpose for which it was obtained, properly protect the information while in my possession, and dispose of it properly once it is no longer needed for business purposes.
- Will not make any unauthorized alterations (add/change/delete) to any information or data to which I may have access.
- Will work to prevent the download, distribution, and installation of pirated software.
- Will not install or encourage the installation of software without a valid license or the installation of a single user license on multiple machines.
- Will not remotely or physically login to another user's machine or attempt to access another user's files without the individual's permission, except when necessary in the course of performing assigned duties as an employee.
- Will not try to compromise the security of the Auburn University network or devices attached to the network, except when it is necessary in the course of assigned duties as an employee.

- Will comply with the Electronic Privacy Policy.

Below are some examples of the IT Professionals Code of Conduct in practice. These are meant to be representative and helpful, but not comprehensive.

- IT professionals must never request or ask a user for their password and must not observe a user entering their password.
- IT professionals must not open emails or files while troubleshooting an issue without proper authorization and must examine only the content of emails or files as required to troubleshoot a particular problem.
- Remote access to computer equipment for support purposes can only occur with the approval of the end-user.
- When developing, testing, analyzing, maintaining or troubleshooting issues in University applications, records should only be interrogated if they are related to the problem being investigated.
- When showing examples of pages, files, business flow or report output in documentation, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data.
- For purpose of presentation, development, testing, analyzing, maintaining, or troubleshooting, appropriate measures should be taken to disguise the information to protect the identity of the individual(s) associated with the data.
- While there is no guaranteed right to privacy on any Auburn-owned electronic resource, data traversing the network will not be monitored for content or for purposes other than maintenance, specific diagnostics, traffic management and system protection purposes.
- Access to log information must only be used for business purposes and as required to support the integrity of systems.
- Data contained in log files and databases should not be disclosed beyond the need of the IT group to develop, maintain, troubleshoot or perform diagnostics unless under direction from proper University or legal authorities.
- Information about a specific user's access to networks, systems, databases, or any other computer based resources must not be disclosed to anyone beyond the owner unless under direction from the proper University or legal authorities or for the purposes of development, testing, maintenance, protection and support of an IT system.
- The casual viewing of any data contained in logs or databases that fall outside of an employee's job responsibilities is strictly prohibited.
- All physical access to University IT Data Centers must follow established access management protocols; all requests for access must be approved by the Data Center Manager or Director.
- All requests for access to systems must follow established access management protocols; all requests for systems access that fall outside of the specific ones covered by the access management protocol must be referred to the data owner.
- All requests for privileged access to production systems must follow the established procedures for granting such access, including the timely and accurate logging of the request and the timely reverting of privileges upon completion of the work that prompted the request for privileged access.