ELECTRONIC PRIVACY POLICY

Responsible Office: Division of Institutional Compliance & Privacy

I. POLICY STATEMENT
Auburn University reviews of the contents of accounts and/or files will be limited to those actions necessary to preserve the financial integrity of the University, the security of people and property, or the functionality of IT resources and systems or to protect the University from liability or comply with applicable law.

II. POLICY PRINCIPLES
The purpose of this policy is to describe the level of privacy and confidentiality that users of Auburn University Information Technology (IT) resources, such as computers, mobile devices, e-mail systems and network resources, can expect, and to indicate the types of situations in which Auburn University may review the contents of such resources. This policy covers all Auburn University-issued accounts (students, employees, guests, retirees) as well as IT resources.

Auburn University is committed to the concept of privacy and, to the greatest extent possible in a public institution, strives to protect the privacy of electronic material, communications of AU employees and academic freedom of AU faculty.

However, individuals who are using Auburn University IT resources should be aware that there are circumstances under which the content of such resources may be reviewed by University employees in the scope of their job responsibilities or by third parties as directed by the University or as required by law.

University IT resources are intended to be utilized to conduct University business. Individuals having concerns about the confidentiality of their personal non-work-related communications or data are encouraged to use non-AU IT resources for those purposes.

III. EFFECTIVE DATE
January 1, 2008
Revised: October 29, 2018

IV. APPLICABILITY
This policy applies to all University accounts, information technology resources, and data.

V. POLICY MANAGEMENT

Responsible Offices: Division of Institutional Compliance & Privacy
Responsible Executive: Associate V.P., Audit, Compliance & Privacy
Responsible Officer: Executive Director Institutional Compliance & Privacy
VI. DEFINITIONS

VII. POLICY PROCEDURES

1. Actions to review IT resources and subsequent release of records of an individual may be required in order to respond to a lawfully issued court order or subpoena, or as prescribed by statutes, and may be authorized by the Office of the General Counsel.

2. In the event an employee is unavailable for a time frame affecting normal business functions (e.g., deceased, critically ill, extended absence, or terminated) the University may review email and data files assigned to the employee to preserve continuity of University business. Such reviews will generally be conducted by the employee’s immediate supervisor. The immediate supervisor must receive approval from the Division of Institutional Compliance & Privacy. The reviewer will be held to the confidentiality standard described in this policy. Other requests for access (such as by the estate of a deceased user) shall be referred to the Division of Institutional Compliance & Privacy.

3. Other requests to review electronic content on resources assigned to an individual must be routed through the appropriate chain of command for approval by the Office of the General Counsel, except for internal reviews conducted in accordance with the Office of Audit, Compliance & Privacy Charter. The Office of the General Counsel will maintain a log of approved electronic review requests. The log shall include, but is not limited to, the name(s) of the individual(s) requesting the review, the date of the request, and a general statement of the reason for the review. This log will be treated as a sensitive and confidential personnel matter.

Prior to conducting a review, Auburn University shall notify the subject of the action, unless it is determined by the Office of Audit, Compliance & Privacy or Office of the General Counsel that doing so is inconsistent with institutional interests or relevant law.

4. Personnel charged with the management of e-mail and network resources may be required to perform in-depth analysis of computers, networks, and/or accounts as they seek to solve technology, security, and/or performance related problems. Such activities do not require the approvals set forth above.

   i. Personnel charged with the management of e-mail and network resources will avoid viewing information not intended for them, but it should be understood that such information may be visible in their normal course of work.

   ii. Personnel charged with the management of e-mail and network resources may in the normal course of their work be required to advise the individual, or the individual’s supervisor, of computer or network activity that is having a negative impact on University IT resources.
iii. Personnel charged with the management of e-mail and network resources may in the event of a suspected breach or exposure, utilize automated tools to locate and delete emails that compromise data security (e.g., “phishing” emails or malware) and to search the contents of user files for potential Personally Identifiable Information (PII) subject to data breach notification laws. If potential PII is located within the system files, the Division of Institutional Compliance & Privacy will be notified for any further action, which may include review of individual emails containing potential PII.

iv. It is a violation of this policy for University officials to pressure personnel charged with the management of E-Mail and network resources to turn over any such information, except as prescribed above.

5. In all cases of electronic content review approved under this policy, access to results will be limited to those individuals with a legitimate need to know and presentation of review results will be limited to information directly related to the review action justification.

6. In all cases, individuals who have access to electronic media and communications of others, shall keep all information accessed strictly confidential in accordance with the Auburn University Information Disclosure & Confidentiality Policy (as well as any other confidentiality agreements mandated by the employee’s unit) with the exception that information which appears to be in clear violation of state or federal laws should be referred through the appropriate administrative channels to the Office of the General Counsel for a determination of how to proceed.

VIII. SANCTIONS
    Deliberate disregard of this policy or principles may result in discipline up to and including dismissal.

IX. EXCLUSIONS

X. INTERPRETATION
    The Director of the Institutional Compliance & Privacy and the Auburn University General Counsel have the responsibility to interpret this policy.