Electronic Privacy Policy

Purpose

The purpose of this policy is to describe the level of privacy and confidentiality that users of Auburn University computers, 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 non-student Auburn University-issued accounts (employees, guests, retirees) and Information Technology (IT) resources assigned to AU employees.

Policy

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 (1) that there are circumstances under which the content of such resources may be reviewed and (2) that there are employees who may in the proper course of their work see information not intended for them.

Actions to view the contents of accounts and/or files initiated by Auburn University will be limited to those actions necessary to preserve the financial integrity of the University, the security of people and property, the functionality of IT resources and systems, or to protect the University from liability. Such reviews may not be used to curtail open debate on substantive issues in the University environment, nor used in a punitive way against individuals with differing points of view.

Individual employees having concerns about the confidentiality of their personal private communications should consider using non-AU ISP facilities and/or storing personal sensitive files on personally purchased off-line media.

Policy Implementation Guidelines

1. Undisclosed actions to review electronic content and/or network access and/or release of records of an individual may be required in response to a lawfully issued court order or subpoena, or as prescribed by statutes, such as the Homeland Security Act, the Patriot Act, or the Electronic Communications Act.

2. Auburn University reserves the right to review digital electronic material and communications when it reasonably appears necessary to do so to preserve the integrity and security of the University, or to protect the University from liability.

i. All actions to review electronic content on resources assigned to an individual employee must be reviewed by the Office of General Counsel and approved by the Office of the President. The Office of General Counsel will create a log entry 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.

ii. Prior to conducting a review, Auburn University shall notify the employee of the action, unless at the institution's sole discretion it is determined by the Office of the President in consultation with the Office of General Counsel, that doing so is inconsistent with institutional interests or relevant law.

3. E-mail accounts and data files of employees who become unavailable in a time frame commensurate with normal business functions (e.g., suddenly deceased, critically ill, or terminated) may be reviewed to resolve any unfinished Auburn University business. Any personal e-mail or files shall be left undisclosed by the reviewer and in the case of deceased employees will be available only to the estate of the deceased. (See exception below for information that appears to be in clear violation of state or federal law.) Such reviews will be conducted by staff assigned by the IT Director and the reviewing professional will be held to the confidentiality standard described in this policy. Such activities are defined as business continuation and do not require the approvals set forth in item 2 above.

4. Systems Administrators or other 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 are not defined as “information gathering” and do not require the approvals set forth in item 2 above.

    i. System Administrators or other 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. System Administrators or other 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. System administrators or other personnel charged with the management of E-mail and network resources will not disclose personal information they may see in the course of their work. Violations of this policy by system administrators are considered a Group I offense under the Auburn University Personnel Manual. Additionally, it is a violation of this policy for University officials to pressure system administrators 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, both employees and students, who have access to electronic media and communications, shall keep all information accessed either intentionally or unintentionally, strictly confidential, with the exception that information which appears to be in clear violation of state or federal laws should be (a) referred directly to the Office of General Counsel if it is an active investigation under this policy, or (b) if it is not an active investigation the information should be referred through the appropriate administrative channels to the Office of General Counsel for a determination of how to proceed. Except for the referral to the Office of General Counsel, all information must be kept strictly confidential. The assigned owner of the electronic media will not be held accountable for extraneous information not placed on electronic media by the assigned owner. Violations of the confidentiality section of this policy by any employee are considered a Group I offense under the Auburn University Personnel Manual.

REVISED: January 1, 2008