Electronic Privacy Policy: V7 (Working Draft)

October 22, 2004

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 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 not have an expectation of absolute privacy in the use of these resources and 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-Auburn 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 USA 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, security, or functionality of the university, or to protect the university from liability.

    a. All actions to review electronic content on resources assigned to an individual employee must be approved by the Office of the President.
    b. Prior to initiating a review action, Auburn University shall notify the employee of the action, the notification shall be verified, and a copy of the verified notification given to the employee. In addition, a file shall be maintained in the office of the President of all approved and verified review actions.
    c. Form xxxxx**&#65533;** **Request for Electronic Content Review** will be used to obtain verified notification of the employee.

3. 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.

    a. System Administrators or other personnel charged with the management of e-mail and network resources will not seek to view information not intended for them, but it should be understood that such information may be visible in their normal course of work.**&#65533;**
    b. 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**&#65533;**s supervisor of computer or network activity that is having a negative impact on university IT resources.
    c. 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 in #2 above.

3. E-mail accounts and data files of suddenly deceased employees may be reviewed to resolve any unfinished Auburn University business. Any personal e-mail or files shall be left undisclosed by the reviewer and will be available only to the estate of the deceased. **&#65533;**Such reviews will be conducted by IT staff assigned by the IT Director and the reviewing IT professional will be held to the confidentiality standard describe in this policy.

4. E-mail accounts and data files of employees terminated for cause may be reviewed to resolve any unfinished Auburn University business. With the exception of information in clear violation of state or federal law, all personal e-mail or files shall be left undisclosed by the reviewer. Such reviews will be conducted by IT staff assigned by the IT Director and the reviewing IT professional will be held to the confidentiality standard described in this policy.
5. In all cases of electronic content review, 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 receiving information that appears to be in clear violation of state or federal law should refer this information to the university general counsel for a determination of how to proceed. The assigned owner of the electronic media will not be held accountable for extraneous information not placed on electronic media by the assigned owner.

8. Procedure for requesting an electronic content review action:

    a) Requests to review electronic content of computers or accounts, or other digital electronic material will be made on form xxxxxx and submitted to the Office of the President.
    b) Electronic content review requests will be reviewed and approved or denied as appropriate and a copy sent back to the requesting party.
    c) Upon receipt of an approved review action, the requesting party will notify the employee and obtain a verification signature. If an employee refuses to sign, a witness signature will be required to certify that notification was made to the employee.
    d) Copies of the verified notification will be distributed as follows:
        a. Employee
        b. President
        c. Requesting party
        d. Appropriate unit head of the IT resource in question.
    e) Upon receipt of a fully signed Request for Electronic Content Review form, the appropriate technology unit will initiate the requested review.