UtahStateUniversity

POLICY MANUAL

OPERATING POLICIES AND PROCEDURES

Number 3016
Subject: Data Privacy
Effective Date: September 24, 2008

3016.1 PURPOSE

The objective of this policy is to provide assurance of Institutional respect for privacy of information placed by users on University computers and to define the circumstances and limits on exceptions to that privacy. Users are also cautioned about potential exposure of information and limited privacy on the Internet.

3016.2 POLICY

Information received and stored on University computers by faculty, staff and student users is considered confidential. Distribution and access to the information is under the control of the user, as defined by their role, position or job description. Users are expected to understand the available access control options and maintain appropriate access restrictions for stored information in their control. The University does not routinely inspect or monitor this stored information. However, confidential information on University computers is subject to institutional scrutiny under specific conditions, as follows:

1. To meet system administration/troubleshooting needs:
   - to debug delivery or storage problems
   - to investigate unauthorized accesses

2. To meet institutional needs:
   - to retrieve information about University business
   - to insure proper retention and deletion of official records
   - to investigate reports of violation of University policy
   - to investigate allegations of employee misconduct
   - to meet emergency needs including threats to health and safety

- to insure compliance with this policy, including necessary use of encryption

3. To meet external legal requirements:
    - to investigate reports of violation of local ordinance or state or federal law
    - to comply with subpoenas and other legal requests for information discovery (e.g. GRAMA)

When authorized by the President or Provost in conjunction with University Counsel, examination of stored information to meet (#2) institutional needs or (#3) legal requirements will be performed by a system administrator in conjunction with a representative who is independent of the need or requirement, from Internal Audits, Risk Management or University Counsel. Those units are charged to develop appropriate procedures to handle such requests.

Only information relevant to the need will be forwarded to the requestor. Any costs associated with the examination will be borne by the requestor. In all cases where misconduct is suspected, the stored information will be immediately secured against alteration and copied for examination. When the issue has been resolved all additional copies of the data will be destroyed. At the conclusion of the investigation, the independent representative will provide a summary report of the information examination to the President.

Violations of policy and appropriate use which are inadvertently discovered in the course of system administration/troubleshooting will be reported by the system administrator to management and to Internal Audits.

While various precautions are taken to protect the privacy of information stored or transmitted on Institutional IT Resources, privacy protection from unauthorized user cannot be guaranteed. Users should take additional precautions to protect their own private information and to limit the exposure of that information to unauthorized access.