Proposal to Modify the Acceptable Use Policy

Discussion Paper - December 18, 2008

University information technology (IT) resources and the data that resides within those resources are regularly assigned to individual employees. These resources include email accounts, central storage, and desktop or laptop computers (to name a few), and are secured through the use of the employee's IT account and password. There are many circumstances in which IT staff are asked to provide access to electronic resources managed by individual employees. The most common reasons include situations where an employee has left their position, is unexpectedly unavailable because of an illness, accident, termination, or death. Statistics about the requests received by the Columbia campus and examples of the types of requests are provided in Attachment B.

The University's Acceptable Use Policy (AUP), found in the Collected Rules and Regulations as CRR 110.005, lists a set of reasons for which inspection is permitted. The AUP specifically says:

> ***University Inspection of Personal Electronic Information* --** *Electronic information on University networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by the University where:*
>
> 1. *It is necessary to maintain or improve the functioning of University computing resources;*
> 2. *There is a suspicion of misconduct under University policies, or suspicion of violation of Federal or State laws; or*
> 3. *It is necessary to comply with or verify compliance with Federal or State law.*

The AUP does not address circumstances when an individual is unexpectedly unavailable. Therefore, the AUP should be modified to allow for examination of electronic information when:

4. **It will serve the legitimate business need of the University**

Because "legitimate business need" is difficult to define, a standard procedure should be implemented to manage requests of this type. Requests for access are often time sensitive. Therefore, adoption of a standard procedure must ensure requests can be processed in a timely manner.

See Attachment A for proposed procedural requirements. Once approved, these procedures should be incorporated into the UM Information Security Program.

Attachment A
Proposed Electronic Access Procedures

Standard procedures to provide access to electronically held information should include the following provisions. Because of organizational differences, the titles of approving authority may vary from campus to campus.

General Guidelines

1) Requests should be managed by the Information Security department for each business entity unless the request affects an individual working for that department or an individual in the chain-of-command of that department.
2) Requests should be fully documented and retained in accordance with University records retention policies.
3) In all cases, access will be granted to a specified individual using that individual's own credentials. Access will <u>not</u> be granted by providing the owner's credentials to the requestor.

Processing Guidelines

Request processing guidelines should include:

1) The specific reason for the request
2) The specific IT resources for which access is being requested - blanket authorizations to peruse unrelated data locations will not be provided.
3) An approval by someone in the individual's chain-of-command but at least 2 levels above (i.e., an employee's direct supervisor cannot approve the request).
4) A check for pending grievances or litigation between the individual and their co-workers, their supervisors or the University.

Approvals

In addition to the approval obtained in item #3 in the previous section, the following additional approvals should be obtained:

1) If the request affects a faculty member, an approval by a faculty representative.
2) An approval by one of the following University administrators at the Chancellor, Vice Chancellor, Provost or Vice Provost level as follows:
   i. Students including student employees – Student Affairs
   ii. Staff – Administrative Services or Human Resources
   iii. Faculty – approval from the Chancellor or Provost or designee
3) Approval by the business unit Chief Information Officer (CIO) or designee

Preservation Activities

When there is a concern about the loss of data through automatic deletion cycles or due to scheduled overwriting of data storage sectors, the business unit CIOs can approve the preservation of the requested data prior to receiving the appropriate inspection approvals.

Attachment B

Number and Types of Requests Received by the MU Campus

The Division of IT has processed the following number and type of requests since December, 2005:

2005	1
2006	6
2007	15
2008 YTD	9

- 50% have been due to the employee leaving the University, 22% have been due to termination, 14% due to a death, and 14% due to being placed on leave or from incapacitation.
- There were no requests for individuals holding a title of professor or assistant professor.
- The following types of access were requested:

94%	Access to email
10%	Access to university owned computer
23%	Access to central file storage location

Examples

An administrative assistant within an academic unit left the University. Her email address had been published on Web pages and in print form to collect internship applications. Without access to her email account, the college could not respond to pending and new applications. Additionally, some of the applications had been saved within a centrally managed file storage location that only the employee could access.

A business manager with an academic unit left the University. She had important and sensitive financial data on her computer and in her email account that wasn't available from any other source. The department requested access in order to move relevant financial files to another location.

An office support person in an administrative unit was terminated. This employee was responsible for setting up audio conference calls for customers. The calls were scheduled using her email account. The department needed access to ensure they could continue to manage and schedule conference calls until the work assignment could be transitioned to a new employee.

An employee, responsible for shipping containers between the University and its customers, passed away. The department needed access to the employees email account to determine the status of pending orders and access to his computer to find shipping documents that had been saved there.

A Research Fellow passed away suddenly. She was partially funded through an NIH training grant and had data in her email account and on her computer related to her investigations. Access was requested by her faculty advisor.

A Human Resource Specialist left the University. Her email account contained unresolved HR issues, recruitment activities and other HR related activities. The department requested access in order to continue to manage ongoing hiring activities and to ensure pending HR issues were addressed.