Information Security Policies and Guidelines
For the Offices of
UM Institutional Research and Planning
MU Institutional Research

Purpose

The purpose of this document is to outline detailed policies and guidelines that govern information security practices in the offices of UM Institutional Research and Planning and MU Institutional Research referred jointly throughout the remainder of this document as University IR. These policies and guidelines will serve as the basis for ensuring that information security practices in University IR are in compliance with the University Information Security Program as outlined on the following website: http://infosec.missouri.edu/.

Throughout this entire document, any reference to staff shall apply to any persons employed in University IR. Any reference to offices shall apply to the offices and other areas that are designated for use by staff of University IR. While the staff of University Archives also maintains offices on the same floor as University IR, their information security policies and guidelines may differ due to the nature of their business operations.

Section 1- Access to Work Area

Objective: To control unauthorized access to work areas where confidential or sensitive information is held or utilized.

A. Staff should challenge unfamiliar persons wandering the main hallway of University IR. Although University IR shares the main hallway with University Archives, it is the duty of everyone to recognize and respond to unfamiliar persons whether they do or don't appear to be in the vicinity for university-related business. Suggestions for responding to strangers include the following: May I help you find someone? Do you have an appointment with someone today? , etc.

B. Staff should become familiar with evening janitors and attempt to determine identity of any new/unfamiliar janitor whose ID badge should be displayed at all times. Campus police should be called immediately if it is suspected that someone is posing as a janitor and has gained unauthorized access to any of the offices.

C. From time to time, staff from other offices such as Information & Computing Services (ICS) and Campus Facilities must have access to a particular office to service a computer, provide maintenance, etc. Preferably, the staff member that occupies the office will be present during such visits. However, if it is not feasible for the staff member to be present, she/he should notify remaining staff members via email of the expected visit and if necessary designate another member of the staff to provide access to the office for which the service is scheduled.

D. The main doors to access University IR offices (on opposite ends of hallway) and the doors to the break /library and conference rooms shall remain unlocked during normal business hours. Any staff working beyond normal business hours (including weekends) shall make sure that these doors are locked.

E. Documentation regarding who has keys to access University IR offices; doors on opposite ends of hallway; and doors to main building in which University IR is housed shall be maintained by the administrative assistant of University IR.

F. Any staff member separating from University IR either voluntarily or involuntarily must return all keys to the administrative assistant of University IR. The administrative assistant will document the date that keys were received and also obtain appropriate signatures regarding the transfer of keys.

G. Report any suspicious persons that do not appear to be on the main floor of University IR for university-related business to all of the following:

During regular business hours:

Floor monitor for University IR: Christy Ludeman; 721 Lewis Hall; 882-2778 or 882-4077; and

Building coordinator for Lewis Hall: Leanna Garrison; 405 Lewis Hall; 884-2113; and

Assistant Building coordinator for Lewis Hall: Adria Koehn; 605 Lewis Hall; 882-8034.

Evening/weekends/non-business hours (or other times deemed appropriate):

University of Missouri Police, 882-7201 (main line), 882-5923 (office), 999-1979 (cell) or umcpolice@missouri.edu

Section 2- Access to Work

Objective: To control unauthorized access to confidential or sensitive materials and work equipment.

A. Care should be taken when sending faxes that contain sensitive information as part of university-related business.
   - Only send sensitive information by fax if it is not feasible to send via another more secure method such as delivery by hand, secure email, etc.
   - Always send a completed cover letter that includes the total number of pages faxed.
   - If sending to recipient for the first time, verify the fax number with a test send and receipt of dummy fax.
   - Before sending fax, alert intended receiver on other end that fax is being sent.
   - Do an immediate follow-up call to make sure that the fax was received by the intended recipient.

B. Do not place sensitive or confidential information into files in the break room.

C. Resources and the availability of space will factor into the long-term goal of moving office files from the break room (a semi-public location) to a room with lock and key.

D. Staff shall store sensitive or confidential documents in the file cabinets of their respective offices during breaks and at the end of the work day.

E. Each staff member shall configure his/her office computer's Windows OS to time-out to screen saver mode after a nominal period of time of keyboard and mouse inactivity (e.g., after five minutes of such inactivity). The configuration must require the staff member re-enter his/her UM log-on password in order to resume working at his/her PC.

F. Staff shall place sensitive or confidential documents out of plain view during times when staff from other offices such as ICS or Campus Facilities must have access to an office.

Section 3- Information Systems Security and Access

Objective: To appropriately manage confidential and sensitive electronic files and IT resources.

A. Each member of University IR shall protect confidential information over which they have control when stored electronically. Individuals with access to sensitive data shall safeguard resources and maintain appropriate levels of confidentiality in order to protect the integrity of all electronic data.

B. SecureDoc shall be used as added protection and a tool for data security of highly protected and valuable electronic information to prevent both deliberate and accidental unauthorized access to University IR's restricted data. SecureDoc must be installed in all UM IR computers, including external hard drives and laptops.

C. An *encryption key* shall be used to lock and unlock protected information. Keys should be protected. Users should have a single personal key to unlock protected information on their hard drive or removable media. They may also share a key with others in their group to unlock protected information that needs to be accessible to other people.

D. SecureDoc does not encrypt data sent out through e-mail therefore care should be taken when sending files that contain sensitive materials as part of university-related business.

E. Each staff member shall ensure that his/her office computer has current DoIT-recommended anti-virus/anti-malware software installed and kept updated. These include Symantec's "Endpoint Protection", Lavasoft's "Ad-Aware", and Safer Network Ltd's "Spybot-Search & Destroy. [Doing this will reduce the likelihood that information on PC and/or server hard drives will become corrupted or otherwise compromised (e.g., by spyware).]

F. Staff shall not just log off their respective computers during breaks and at the end of the work day. Staff shall shut their computers down as they leave their respective offices.

G. Staff shall lock doors on each occasion they leave their office.

H. The fire exit door access to UM IR should remain locked at all times. The main access door to UM IR should be locked at 5pm or upon exit if no staff are present.

Section 4- Access to Waste Materials

Part 1

Objective: To ensure paper files are properly destroyed when appropriate.

A. A shredder shall be provided in the University IR break room to facilitate proper disposal of sensitive or confidential paper documents that are no longer needed.

B. All paper documents containing sensitive or confidential information that are no longer needed shall be shredded prior to disposal.

Part 2

Objective: To ensure electronic files and other media are properly destroyed when appropriate.

A. Prior to disposal, electronic media such as floppy disks, rewritable CD-ROMS, and zip drives that contain confidential/sensitive information shall be reformatted if the media type allows it or erased if formatting is not possible.

Section 5- Departmental Procedures and Employee Expectations

Objective: To set expectations and raise awareness among employees who handle confidential or sensitive information.

A. In addition to the orientation that is required of all employees new to the University, any new hire to University IR shall receive a comprehensive orientation to University IR that shall include a review of all applicable information security policies and guidelines.

B. All University IR staff shall receive written policies and guidelines that set forth clear expectations regarding responsibilities for securing sensitive information that is handled and managed as part of normal business operations.

C. The University IR staff may be required to read and sign the University of Missouri Access and Confidentiality Agreement which further outlines the applicable laws and policies regarding sensitive/confidential information and the consequences for failure to abide by the agreement which include discipline, possible termination of employment or legal liability. The current document serves as a specific guide to University IR. It is a living document that should be revised annually at a joint meeting scheduled by a University IR Administrative Assistant.