

# ADMINISTRATIVE PROCEDURES

## COMPUTERS

---

### Information Security

The linked [Information Security Policy](#) should be considered current Office policy and compliance is expected.

**Data Ownership:** All data kept on the Office of University Audits' network should pertain to the University and related professional duties of the audit staff. As such, these files are considered the property of the Office of University Audits, rather than the property of the individual who has created them.

**Data Security and Privacy:** To further accessibility, yet provide for adequate data security and integrity, the following standards have been developed:

1. All directories, subdirectories, and files of the audit staff should have a security level no greater than "read only."
2. Personnel related directories, and other directories of a sensitive nature should be given higher security levels.
3. Other noncritical files, e.g., Continuing Professional Education records, training notes, or individual personnel documents, may be stored on CD diskettes.
4. Security levels will be maintained by the Network Administrator.

These standards are designed to allow efficient access to information by those who have a reason to use it, yet protect the integrity of the original.

### Microsoft EFS (Encryption File System)

Encryption is needed to encrypt data on hard drives of notebook computers so that sensitive data is not exposed in case the computer is lost or stolen. Microsoft EFS is a product that is available in our current environment. The following document provides general information on Microsoft EFS and instructions on how to encrypt data on hard drives.

- [Using Microsoft Encryption File System](#)

### Acceptable Use of Computing and Network Resources

The University Administration (UA) Acceptable Use of Computing and Network Resources Policy guidelines should be considered current auditing division policy and compliance is expected.

Effective February 1, 2008, all UA employees must comply with the guidelines outlined in this policy. It is the employee's responsibility to thoroughly review this policy and it is available at [https://nessie.uhr.uillinois.edu/cf/policies/index.cfm?Item\\_id=3894](https://nessie.uhr.uillinois.edu/cf/policies/index.cfm?Item_id=3894).

The purpose and applicability sections of the policy are quoted below.

## PURPOSE

This policy describes the acceptable use of computing and network resources at the University of Illinois, UA. It is based on University policies which were developed to comply with all applicable laws and regulations and is intended to protect UA employees and the University from damaging actions including lawsuits, virus attacks, and the compromise of network systems and services. This policy is not intended to impose undue restrictions that are contrary to University of Illinois' established culture of openness, trust, and integrity.

## APPLICABILITY

This policy applies to all employees, contractors, consultants, temporaries, and other individuals assigned to UA ("User"). This policy covers computer equipment and related software owned or leased by the University of Illinois, including but not limited to computers, application software, operating systems, data files, storage media, network accounts providing electronic mail, Internet browsing, FTP, login accounts and passwords.

Maintaining a secure and responsive network environment is a team effort involving the participation and support of every User of University technology resources. It is the responsibility of every technology User to know this policy and to conduct their activities accordingly. *Users must also comply with, and are subject to, the campus security and computer use policies of their primary campus location as well as other University policies.* Failure to comply with these policies could be cause for disciplinary action up to and including dismissal.

## Auto Audit Backup Procedures

A centralized backup procedure exists to automatically backup Auto Audit files on the production server. When you are using your Local AutoAudit database, changes that you make to your database need to be replicated back to the production server so that changes are included in the automatic backup mentioned above. This replication should take place at least daily.

If you are working away from the office, replicate whenever you connect to the network. This provides several benefits: your work is saved and protected against computer failure or theft; you receive any review comments that may have been made; and your work is available for others to review on a timely basis.

Files outside of AutoAudit that you have created and saved must be backed up to the network on a weekly basis.

## Microsoft Briefcase

The Briefcase feature in Windows XP helps you keep your files updated by automatically synchronizing multiple copies of individual files. In other words, Briefcase keeps track of the relationship between files on two or more computers. For example, if you use a desktop computer at the office, and you use a portable computer when you are on the road, Briefcase synchronizes and updates the files on your desktop computer to the modified versions when you reconnect your portable computer to the desktop computer. The following document provides general information on Microsoft Briefcase and instructions on how to use it.

- [Using Microsoft Briefcase](#)

## Software Piracy Policy Compliance Procedures

Administrative support personnel will maintain a file that will hold:

1. Proof-of-purchase documents
2. Software licenses
3. Office computer list

These records will be maintained until the software program is uninstalled.

## Handling Computer/Network Problems

Computer, application, or network problems from all three campuses will be handled as follows:

1. AutoAudit issues: contact the Director of IT Audits
2. Lotus Notes issues: contact the Director of IT Audits
3. All other computer, application, or network issues and problems need to be reported directly to the Microcomputer Support Specialist (MSS).
  - a. The MSS will notify the user how the issue will be handled, e.g., the MSS will attempt to resolve the issue or will identify who the issue/problem was passed to or will notify if the user needs to resolve the issue.
  - b. The MSS will address the situation first, attempting to handle workstation and local server issues. If the MSS cannot solve the issue quickly, the computer will be replaced with the office backup computer. The MSS will then work on the problem computer on an ASAP basis in conjunction with other responsibilities.
  - c. If the MSS cannot solve the problem, or if the problem is not a workstation issue, the Director of IT Audits will be notified.
4. The Director of IT Audits will be our primary contact with AITS (helpdesk and network support). In the event the Director of IT Audits is not available, the MSS will be our secondary contact with AITS. No one else should contact AITS directly.

## Laptop Computers

Laptops assigned to staff are the responsibility of the staff person until returned. Staff members who have a laptop assigned to them should not loan that laptop to other staff members, family members, or friends.

The following procedures should be followed when using and storing laptop computers.

### Laptop Care

1. Laptops should be transported in their protective carrying cases at all times.
2. Laptops should be protected from temperature extremes and precipitation (rain, snow, sleet, and ice).
3. Staff members should refrain from placing drinks or food near laptops and in places where spills could cause damage to the laptop.
4. The laptops are provided with all the necessary software. **Do not download any software to the laptop, or install any software to the laptop without the approval of the Network Administrator.**

### **Laptop Security - In the Office**

1. Laptops should be secured when not in use and overnight.
2. Doors to offices with laptops should be locked over the lunch hours.
3. A designated staff person will be responsible for the safeguarding of, and accountability for, any laptops not assigned to a particular staff member.

### **Laptop Security While out of the Staff Member's Home Office**

1. Laptops should be either secured during lunch or any other time the auditor is away from his working area (e.g., while interviewing auditees or touring facilities).
2. Preferably, laptops should not be left unattended in automobiles. However, if it is necessary to leave the laptop in an unattended car for a short period of time, the laptop should be placed in the trunk.

---

This Section Last Revised: 03/31/08

Return to the  
[Audit Manual Table of Contents](#)