

Information Technology Management

The Information Technology Management Policy applies to all members of the University of Cincinnati community. This companion policy to the General Policy on the Use of Information Technology sets forth unit-level responsibilities for the operation and maintenance of computers and networks. For the purpose of this policy, all university departments and offices will determine their respective unit affiliation.

All operating units that use information technology (IT) shall be responsible for:

- Developing and implementing, when appropriate, additional IT policies, guidelines or procedures specific to their academic or administrative units.
- Maintaining the functionality of the IT systems within their area.
- Facilitating training and the dissemination of information.
- Maintaining the security of the IT systems and the network to which they are connected.
- Preventing unauthorized access to university information, personal files and e-mail.
- Promoting IT policy adherence.
- Creating and maintaining a plan for recovery of mission critical data and systems if loss is sustained.

The academic or administrative head of each operating unit shall designate an Information Technology (IT) Coordinator to ensure that these responsibilities are carried out and to serve as a contact person for that unit with the UC Office of Information Technologies (UCit). This policy recognizes that different units have different needs, IT resources, and levels of internal expertise. Hence, the needs and resources of a given unit may not require the IT Coordinator to have an extensive technical background. Many units also have "Technical Managers" who are responsible for the operation of the IT systems and with whom the IT Coordinator may share the responsibilities in this policy. Technical Managers are expected to have the technical expertise required to ensure the safe and reliable operation of their respective unit's IT systems.

The purpose of this policy is to establish some general rules to be followed by all units carrying out the responsibilities set forth below.

Responsibility for Local Information Technology Policies

Each operating unit shall adopt policies governing the use of its IT resources using whatever procedures it normally follows for adopting policies in the unit. Such policies shall be consistent with the General Policy on the Use of Information Technology and all other University rules and policies, and shall include at minimum the following components:

- A statement identifying the kinds of IT resources in the unit and establishing general policies for each kind of resources. These policies should require the operating unit to identify the persons responsible for each kind of resource, the persons authorized to use the resources, and the uses permitted for the resources. Where appropriate, the policy should cover issues of shared access, resource limitations, and personal use.

- A policy statement on security and data preservation that addresses unique information technology issues presented by the unit or resource in question and identifies the individual in the unit who is responsible for matters of security;
- Cross references to the University's General Policy on the Use of Information Technology as well as other rules and policies applicable to the unit or resource.
- A policy statement regarding mission continuity planning to address system, application, and data backups and procedures for the recovery and restoration of unit's mission critical IT resources in the event of loss.

If a unit's IT usage does not warrant the development of unit-specific policies, the unit may exercise the option of adopting the University's general IT policies as its unit-level policies.

Units that do not adopt unit policies, and units that do not have more restrictive policies on personal use of IT resources, shall be deemed to have adopted a policy prohibiting personal use by employees of telephones, pagers, cell phones, computers and other IT resources when such use interferes with the efficient performance of an employee's duties or with the functionality of the unit's IT system or when it results in increased operating costs for the unit or the University. Subject to supervisor discretion, incidental personal use of IT resources that does not produce the above effects is authorized. Employees must promptly reimburse the unit for any personal use of telephones, cell phones, or other IT resources that result in long distance toll charges or other identifiable increased costs for the unit.

Responsibility to Maintain Functionality

Each information technology system at the University of Cincinnati is intended to serve some function or set of functions. The unit's IT Coordinator shall ensure that the IT systems in the unit continue to serve their functions with an appropriate degree of reliability.

Responsibility for Facilitating Training and Disseminating Information

The unit's IT Coordinator shall facilitate appropriate training and IT knowledge transfer within the unit. User-paced training affords systems user opportunities to remain current or expand their technical skills and knowledge of applications. IT Coordinators should direct system users within their respective unit to avail themselves of IT training opportunities available both within and outside the university community. The unit's IT Coordinator is also responsible for communicating important technical information to the users of the unit's systems.

Responsibilities for Security

The Office of the Vice President for Information Technologies shall provide leadership and direction for the University's network and systems security. The Office of the Vice President for Information Technologies has developed and implemented a network architecture that places an emphasis on security. The University's Network and Systems Security Team will collaborate with IT Coordinators and Technical Managers to develop system security awareness practices, appropriate system safeguards and effective responses to breaches in security within the units. Security in a networked environment must be a responsibility shared by everyone. A single compromised workstation can be used to attack other systems both within and outside the University.

IT Coordinators are responsible for establishing, communicating and enforcing unit level practices and procedures that promote security. The following areas should be covered:

- Physical security.
- Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, and data files.
- Prevention of unauthorized access.
- Detection of security breaches.
- Procedures for reporting security breaches to management or appropriate authority.
- Account auditing which includes the removal of accounts no longer authorized access to the University's information technology resources.

IT Coordinators and technical managers will work with UCit security personnel, other system administrators, and law enforcement officials, both inside and outside the University of Cincinnati, to find and correct problems caused on any UC network or on another system by the use of the system under their control. Where violations of this or any other IT policy come to the IT Coordinator or Technical Manager's attention, they are authorized to take reasonable actions to maintain the security of the system. A user's access privileges may be temporarily suspended if the IT Coordinator or Technical Manager believes it is necessary or appropriate to maintain the integrity of the computer system or network.

Responsibility to Prevent Unauthorized or Inappropriate Access and Disclosure

IT Coordinators are responsible for unit level safeguards and procedures that minimize the possibilities of unauthorized access to University or personal files. As matter of University policy, no one, including IT Coordinators, Technical Managers and their staff members, may access user files except in the circumstances described below. Even where access is permitted, those who have accessed information must not reveal it to others who are not authorized to receive it. Technical Managers must configure their systems to minimize the possibilities for any unintended disclosure of personal information. In instances where a unit does not have a Technical Manager, the IT Coordinator has the responsibility to arrange for the proper configuration of the unit's systems.

Permissible Access by IT Coordinators, Technical Managers, and Staff

- Investigation of System Problems

IT Coordinators, technical managers and their staff members are permitted to access user accounts, files or communications when there is reason to believe that the user is interfering with the performance of the system or network, but only to the extent reasonably necessary to ascertain whether there is a problem and to take corrective measures. In situations in which the IT Coordinator and the Technical Manager have no reason to suspect misconduct on the part of the user, the technical manager or staff member shall advise the user prior to access to the extent reasonably practicable. In situations in which misconduct is suspected, the technical manager or IT Coordinator shall first notify the appropriate authority for investigating disciplinary matters involving the particular user prior to attempting to gain access. However, in no case shall a technical manager be restricted from immediately accessing any account, file or communication on a system for which the manager has responsibility, or from taking

corrective action, where there is a reasonable belief that a failure to do so will result in loss of system or network stability, substantial damage to the system or network, or liability to the University.

- Investigation of Misconduct

As part of an investigation into possible violations of University rules or policies, or of local state or Federal laws, individual user accounts, files and communications may be accessed as part of the investigation upon a showing that there is reason to believe that the accounts, files or communications contain information relevant to the infractions under investigation. With the exception of authorized UCit security personnel, access to a suspect system will not be granted by the IT Coordinator or technical manager without the approval from the dean or administrative head of the unit or the dean's or administrative head's designee. In all cases, an authorized UCit investigator shall notify the user prior to accessing the user's accounts, files or communications, except where reasonable efforts to contact the user are unsuccessful or upon a showing that prior notification would compromise the investigation. Pending approval of the appropriate dean or administrative head of a unit, the authorized investigator may take reasonable steps to ensure that the accounts, files or communications are not altered or destroyed.

- Where Required by Law

The university will permit access to individual accounts, files and communications where required to comply with a lawfully issued subpoena, court order, Public Records Act request and other request having the force of law.

- Access for Coworkers

Each operating unit shall develop policies regarding shared access to University files by coworkers and administrators. In situations in which a co-worker or administrator cannot access files for which they have authorization (because of the absence of an employee on whose workstation they are stored), an IT Coordinator or technical manager, with the approval of the unit head, may make such files and only those specific files available to the authorized individual.

Responsibility for Policy Adherence

The Office of the Vice President For Information Technology shall provide university-wide leadership over unit level adherence to the Information Technology Management policy. It is expected that departments and offices will become aligned to a unit within six months of the university's adoption of this policy. Actual unit-level policies should be developed and shared with the Office of the Vice President For Information Technology within one year of the university's adoption of the Information Technology Policy. Future newly formed units will have one year to develop a unit-level policy for submission to the Office of Information Technology.

In collaboration with the Office of the Provost and Vice President Offices, the Office of the Vice President for Information Technologies will monitor unit-level progress and will offer assistance to facilitate unit formation, unit-level policy development and overall compliance to the Information Technology Management Policy. The Office of the Vice President for Information Technologies will maintain a database of unit-level IT Coordinators and Technology Managers. The Office of the Provost

will remind academic units of compliance deadlines through their respective IT Coordinator. Correspondingly, the appropriate Vice President Office will remind administrative units of compliance deadlines through their respective IT Coordinator or Technology Manager.

IT Coordinators and technical managers share the responsibility for seeing that University and local policies governing the use of the system and network are followed. IT Coordinators and technical managers also have the obligation of ensuring that protections for the university's user community are upheld. Technical Managers may resolve minor or inadvertent violations. Where more serious violations of such policies have occurred or are suspected, it is the responsibility of the IT Coordinator to assist an investigation by an appropriate authority. The appropriate authority is typically the dean or administrative unit head in cases involving faculty and staff, and the Office of the Vice President for Student Affairs or the Student Conduct Officer in cases involving students.

Should an academic or administrative unit fall into a state of non-compliance to the Information Technology Policy, The Office of the Vice President for Information Technology will collaborate with the applicable Provost or Vice President Office to bring the unit into compliance. If a given unit disregards or consistently fails to adhere to the unit-level responsibilities set forth in this policy, the unit may be subjected to University disciplinary actions that could range from a temporary interruption of central IT support services to a restructuring of the unit to enhance information technology management.

System Users' Responsibilities

Consistent with the University of Cincinnati General Policy on the Use of Information Technology, this policy does not relieve ordinary users of personal computers or systems of the responsibility to maintain and protect the integrity and security of information technology resources. If a computer is connected to the UC network, the user is responsible for ensuring that the computer is not used to compromise the security of the network. If the computer contains UC information resources, the user is responsible for data integrity, data backup, physical security of the machine, and for protecting the system from computer viruses and other attacks. In most units, there are support personnel who will assist the user with these responsibilities.