

# **Application of the University's Policy on Acceptable Uses of Information Technology Supervisor's Guide**

The University's Policy on the Acceptable Use of Information Technology Resources <http://www.uiowa.edu/~our/opmanual/ii/19.htm> was established to recognize and balance a number of interests that may at times be in conflict with one another. The policy seeks to protect the fulfillment of the University's threefold mission of teaching, research and service, while also balancing the rights of intellectual freedom, freedom of thought and expression and the individual privacy rights of faculty and staff members.

The implementation of this policy often integrates the application of other policies, such as the Ethics and Responsibility Statements for Faculty and Staff, the Human Rights Policy, the Policy on Sexual Harassment, and regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA) and other regulations and policies governing the conduct of the University community. Implementation of the Acceptable Use Policy raises some unique issues that will be addressed here.

## **◆ Privacy Rights Issues**

While the Acceptable Use Policy recognizes an implied right to privacy in a general sense, its application requires us to recognize differential levels of privacy expectations. For example, computer files stored in a shared network drive, normally accessible by multiple users, do not carry an expectation of personal privacy with other users of the shared drive. In contrast, files that are password-protected on a personal drive on a server, on a personal device or on the hard drive of a single user machine carry an implied expectation of personal privacy and therefore, supervisor access is more difficult to justify. Such differences in user expectations are reflected in the application of the probable cause standard for searches, established in the Acceptable Use Policy.

## **◆ Password Privacy**

Supervisors are responsible for establishing and maintaining appropriate procedures to protect the privacy and security of computer files and systems. Protecting the security and integrity of key University applications such as Workflow and Human Resources, as well as applications with regulatory constraints such as INFORMM and IDX, requires sensitivity to individual authorizations while managing the appropriate use of resources. A supervisor may not override or force a disclosure of personal passwords. Employees are charged to keep their passwords secure and to never share them. In a critical emergency, passwords may be reset or shared with a supervisor to address limited kinds of circumstances. Even so, once the

# **Application of the University's Policy on Acceptable Uses of Information Technology Supervisor's Guide**

emergent need has subsided, the password should be changed immediately to restore the previous level of security.

## **◆ Issues of Discovery**

Questions of acceptable use of technology resources may sometimes arise from inadvertent discoveries, such as viewing an open computer screen or accessing information during the temporary absence of an employee. In such cases, while acceptable use may be part of the issue, it may not be the primary focus of the concern. For example, violations of the sexual harassment policy, as may be evidenced by sexually explicit material in an electronic format, should be addressed directly as a violation of the sexual harassment policy, rather than focusing on a violation of the Acceptable Use policy. In such cases, the use of technology may be a method, but may not be the core problem to be addressed. Focusing on inappropriate use of technology raises issues of privacy, whereas, a violation of the sexual harassment policy does not raise the privacy issue, and thereby allows us to address the behavior more directly.

## **◆ Personal Use**

Unless further restricted by department or unit based policies, the Acceptable Use Policy does not prohibit all personal use. Rather, similar to the telephone use policy, limited personal use is permitted unless it interferes with productivity, violates other University policies, results in additional expense to the University, or otherwise interferes or compromises the intended University use or achievement of the University mission. As the policy is structured, personal use alone cannot generally be used as evidence of a technology policy violation, unless it exceeds the "de minimus" threshold established in the policy, or is tied to evidence of a policy violation or evidence of unsatisfactory productivity. Personal use, as a reflection of time and effort, must be put into a context with other measures. Supervisors typically can assess other productivity measures without confronting issues of employee privacy. In such cases, it is preferable to rely on these measures, rather than focus on the technology.

## **◆ Scanning and Monitoring versus Searching**

Technical staff members who provide computer service and support are responsible for detecting anomalies such as noticeable disparities or changes in personal storage space requirements, equipment malfunctions, problematic file names or file types, or other discoveries that may indicate inappropriate use. Such discoveries are not construed as breaching an expectation of privacy unless file contents are reviewed without permission. Technical staff

# **Application of the University's Policy on Acceptable Uses of Information Technology Supervisor's Guide**

members are expected to troubleshoot anomalies, and report suspected policy violations to supervisory staff.

The Information Technology Security Office is charged to perform network security vulnerability scans, manage security incident response activities including the forensic analysis of compromised machines, and engage in other activities to assist with the secure use of information technology. These activities are not breaching an expectation of privacy, but are required for the secure rendition of service.

Similarly, the ITS Telecommunications and Networking Services and UI HealthCare Information Systems Telecommunications departments log network activity, monitor general usage patterns, and perform other such activities that are necessary for the provision of network service.

## **◆ Restrictions on Computer Searches**

The Acceptable Use Policy establishes a procedure for searches of computer files or drives that override individual expectations for privacy, based upon the establishment of probable cause that a violation of University Policy or law has occurred.

The establishment of probable cause must be evaluated by the IT Security Officer, working in consultation with the General Counsel, on a case-by-case basis, weighing the rights and interests of the individual and the University in the context of the alleged violation. Individual supervisors are prohibited from conducting searches of the contents of computer files and drives which are password-protected or otherwise give rise to an expectation of privacy, without approval from the IT Security Officer.

## **◆ Probable Cause**

To establish probable cause for a search, a credible suspicion of violation of University policy must exist, preferably based upon more than one source; the information sought must be essential to the investigation; and not be reasonably or reliably obtained through any other source. Substantial University interests must exist to override the individual privacy concerns. As noted above, as the level of privacy expectation rises, the threshold for the establishment of proper cause to conduct a search rises as well.

## **◆ Procedure**

# **Application of the University's Policy on Acceptable Uses of Information Technology Supervisor's Guide**

As with other types of discipline issues, supervisors are advised to consult with their local Human Resources Representative and/or Senior Human Resource Leadership Representative in their college or division. If a search is contemplated, Central Human Resources/Employee and Labor Relations or Hospital Human Resources department should be consulted early in the investigation. If probable cause appears to exist or is in question, Human Resources will consult with the IT Security Officer, and if appropriate, request a search. In relation to the timeliness of any search, consideration may be given to interim measures necessary to preserve evidence or to protect individuals and property, in relation to the timeliness of any search. Specific search parameters will be established in each case and will be maintained by the IT Security Officer in consultation with the University's General Counsel. Once approved, the staff member will be informed of the search procedures implemented.

## **Resources**

In addition to the written University policies, specifically the Policy on the Acceptable Use of Technology Resources, supervisors should consult with their Unit Human Resource Representative, College/Division Senior Human Resource Leadership Representatives, or the Office of Employee and Labor Relations in University Human Resources. The IT Security Officer and Office of the General Counsel are also available to serve as resources for the campus.