# University of Hartford
# Responsible Technology Use Policy

University of Hartford maintains information technology systems for the research, education, administrative, and other roles of faculty, staff and students. Because computing and network resources are shared, individuals should use the systems responsibly in pursuit of academic and administrative functions, and in doing so, are not to infringe on the rights, integrity or privacy of others or their data. In using the computing systems and network, individuals and groups must abide by standards of lawful and ethical behavior.

Users of the University of Hartford's information technology resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the University itself. This University of Hartford Responsible Technology Use Policy provides guidelines for the appropriate use of the University's resources as well as for the University's access to information about, and oversight of, these resources.

The Responsible Technology Use Policy applies to all users of information technology systems, including but not limited to University students, faculty, and staff. It applies to the use of all information technology systems. Use of information technology systems, even when carried out on a privately owned computer that is not managed or maintained by the University, is governed by this policy.

For statements of other related University policies, consult The Source, the Faculty Policy Manual, the Supervisor's Manual and/or the Staff Handbook.

## *Definitions*

**University of Hartford Information Technology Systems:**
Computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, phone system, software, and data files that are owned, managed, or maintained by the University. University systems include institutional, departmental information systems, faculty research systems, library systems, desktop computers, the University's campus network, and University general access computer labs.

**Information Technology User**:
Any person who makes any use of any University system from any location.

**University of Hartford Information Technology User:**
A user with authorization to access a non-public University system. University users include University of Hartford students, faculty members, and staff members.

## *Purpose*

This policy is to secure an information technology system that promotes the basic missions of the University of Hartford in teaching, learning, research and administration. In particular, this Policy aims to promote the following goals:

- Secure the integrity, reliability, availability and performance of the systems;
- Secure that use of the systems is consistent with the policies and values of the University, and with federal and state laws;
- Secure that systems are used for their intended purposes; and
- Maintain processes for addressing policy violations and sanctions for violators.

## *Responsible Use*

This policy is intended to act as a guide to responsible use of the information technology systems for University faculty, students, and staff. Information technology systems may be used only for their authorized purposes -- that is, to support the research, education, administrative, and other functions of the University of Hartford.

**Authorization:**
Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

**Use that interferes with the activities of others:**
Users must not interfere with service to other users in any way. Intentional or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that is not authorized and causes excessive network traffic or computing load is also prohibited.

**Use that is inconsistent with University of Hartford's non-profit status:**
The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of information technology systems for non-University purposes is generally prohibited, except if specifically authorized by the University's Chief Information Officer. Using information technology systems in a way that suggests University endorsement of any political candidate or ballot initiative is prohibited.

**Harassing or threatening:**
Any use of University technology in a harassing or threatening manner is a violation of University policy.

**Display of offensive material/Violation of University harassment policies:**
Display of offensive material out of context in the workplace/classroom/common areas, and repeated unwelcome contacts with another via electronic messaging or e-mail is a violation of University policy.

**Attempts to defeat system security:**
Users must not defeat or attempt to defeat any system's security -- for example, by "cracking" or guessing and applying the identification or password of another user. (This provision does not prohibit the University from using security scan programs to protect the integrity of the systems.)

**Unauthorized access or use:**
The University recognizes the importance of preserving the privacy and confidentiality of users and data stored in Information Technology systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data or accounts on systems that they are not authorized to access. Furthermore, users must not make or attempt to make any deliberate, unauthorized changes to data on a system. Users must not intercept or attempt to intercept or access data communications not intended for that user.

**Concealed Identity:**
Users must not conceal their identity when using Information Technology Systems, except

when the option of anonymous access is explicitly authorized. Users are also prohibited from impersonating others or otherwise using a false identity.

**Distributing computer viruses:**
Users must not knowingly distribute or launch computer viruses or other damaging programs.

**Virus/Trojan Horse detection and prevention:**
Users are responsible for maintaining antivirus software and other appropriate measures to secure their machines and the network from attack, or inclusion in an attack.

**Modification or removal of data or equipment:**
Without specific authorization, users of University Systems must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, or reconfiguration of control switches or parameters. This rule protects data, computing, and communications equipment owned or leased by the University, or any person or entity on University property. 'Specific authorization' refers to permission by the owner or Systems Administrator of the equipment or data to be destroyed or modified.

**Unauthorized devices:**
Without specific authorization, users must not attach any additional network device (such as a hub, switch, or router) to the University Network.

**Violation of law:**
Illegal use of information technology systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. This may include but is not limited to: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights and trademarks; and making threats.

**Copyright infringement:**
Copyright law governs. The law permits use ("fair use") of copyrighted material without authorization from the copyright holder for *some* educational purposes, but an educational purpose does not automatically mean that the use is permitted without authorization.

**Violating University contracts:**
All use of information technology systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.

**Personal Account Responsibility:**
Users are responsible for reading University-related messages mailed to their University of Hartford account and responding as necessary and/or appropriate. Users are responsible for maintaining the security of their own Information Technology Systems accounts and passwords. Accounts and passwords are assigned to single users and are not to be shared with any other person. Users are responsible for any activity carried out under their Information Technology Systems accounts or posted on their personal web pages.

> **Note:** Those who use a non-University e-mail account should arrange to have their University e-mail forwarded to their active account. Mail must be checked regularly as time-sensitive University material may be disseminated through e-mail.

## *Conditions of University Access*

The University places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the University may determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant University access to relevant Information Technology Systems without the consent of the user. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

**Conditions:**
In accordance with federal, state, and/or local law, the University may access all aspects of information technology systems, without the consent of the user, in the following circumstances:

- When necessary to identify or diagnose systems or security problems, or otherwise secure the integrity of the Information Technology Systems; or
- When required by federal, state, or local law or administrative rules; or
- In response to a lawfully issued subpoena; or
- When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
- When such access to Information Technology Systems is required to carry out essential business functions of the University; or
- When required to preserve public health and safety.

**Personal Identification:**
Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

**Process:**
Consistent with the privacy interests of users, University access without the consent of the user will occur only with the approval of the CIO, or respective designee, except when an emergency entry is necessary to secure the integrity of facilities or to secure public health and safety. A user may be notified of University access to relevant Information Technology Systems without consent depending on the circumstances, at the University's discretion.

**User access deactivations:**
In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

**Use of security scanning systems:**
By attaching privately owned personal computers or other Information Technology resources to the University's network, users consent to University use of scanning programs for security purposes on those resources while attached to the network.

**Complaints or Reports of Alleged Violations:**
An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint with Information Technology Services or Internal Audit.

**Disciplinary Procedures:**
Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students.

**Legal Liability for Unlawful Use:**
In addition to University discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any Information Technology System.

## *Revision*

This policy shall take effect on July 1, 2004, and may be amended from time to time as conditions warrant.