

# IOWA STATE UNIVERSITY

## Code of Computer Ethics and Acceptable Use Policy Summary

July 2004

This summary of the ISU Code of Computer Ethics and Acceptable Use Policy outlines the ethical, acceptable, and unacceptable use of information systems. It is intended to identify key security issues for which individuals, colleges, departments, and units are responsible. The complete document is located in the Iowa State University Policy Library <http://policy.iastate.edu/>.

- 1) Privacy and confidentiality must be balanced with the need for the university to manage and maintain networks and systems against improper use and misconduct.
- 2) Exceptions to privacy of information allow ISU to access, monitor or disclose confidential or personal information residing on its information networks and systems.
- 3) Policies for protection of information and security practices are defined as:
  - a. Protection of information depends on who has created the information, who is maintaining the information, the nature of the information itself, and whether there are specific federal and/or state laws or university requirements or guidelines associated with the use and distribution of the information.
    - i. University information: Students, faculty and staff are responsible for accessing only confidential and business university information for which they are authorized and are required to comply with security policies established by the university or specific departments.
    - ii. Individuals are responsible for securing and protecting their information based on the level of risk associated with its loss or misuse.
  - b. Password security – users are responsible for passwords and activities linked to their accounts and must follow university standards for maintaining and managing passwords.
  - c. User security practices – users are required to employ security practices to prevent unauthorized activity. Such practices include using password protected screen savers, not storing passwords in obvious places, securely transferring information, etc.
  - d. Security for IT systems – to protect systems individuals must use and promptly upgrade virus-scanning software, security patches, operating and other software, and any other security measures for specific security threats.
  - e. Reporting security breaches  
Individuals are expected to prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring and take immediate action to prevent the spread of any acquired infections from any computers under their control. Individuals should power down the computer or disconnect it from the campus network then report IT security incidents to an information technology support professional. First attempt to contact local department, college, or designated information support professional. If unavailable, complete the IT security incident reporting form found at <http://www.it.iastate.edu> or call the Information Technology Security Response Team (ITSRT) at 294-3221.  
  
IT Support Professionals should take immediate action to stop the incident from continuing or recurring then determine whether the incident should be handled locally or reported to the security response team.
- 4) Framework for unacceptable use activities in addition to illegal violations includes:
  - a. Excessive non-priority use of computing resources, such as recreational activities or non-academic or business services
  - b. Unacceptable system and network activities
    - i. Engaging in or effecting security breaches or malicious use of network communication
    - ii. Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access
    - iii. Interfering with or denying service to another user on the campus network or using university facilities or networks to interfere with or deny service to persons outside the university.
- 5) Enforcement guidelines for interim, suspension of services, and disciplinary action are defined.
  - c. Unauthorized use of intellectual property
    - i. Engaging in unauthorized copying, distribution, display or publishing of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.
    - ii. Using, displaying or publishing licensed trademarks, including Iowa State University's trademarks, without license or authorization or using them in a manner inconsistent with terms of authorization.
    - iii. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.
    - iv. Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.
    - v. Using computing facilities and networks to engage in academic dishonesty prohibited by university policy (such as unauthorized sharing of academic work, plagiarism).
  - d. Inappropriate or malicious use of IT systems
    - i. Setting up file sharing in which protected intellectual property is illegally shared.
    - ii. Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
    - iii. Inappropriate use or sharing of university-authorized IT privileges or resources.
    - iv. Changing another user's password, access, or authorizations.
    - v. Using an Iowa State University computing asset to actively engage in displaying, procuring or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.
    - vi. Using an Iowa State computing asset for any private purpose or for personal gain. Refer to the University Policy Manual section 2.5(10). Abusing or misusing computer hardware or software.
  - e. Misuses of e-mail and communications activities.
    - i. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, except as approved under the Mass E-Mail Policy and Effective e-Communication policy.
    - ii. Engaging in harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
    - iii. Masquerading as someone else by using their e-mail or internet address or electronic signature.
    - iv. Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
    - v. Creating or forwarding "chain letters" or solicitations for business schemes.
    - vi. Using email originating from within Iowa State's networks for commercial purposes or personal gain.
    - vii. Sending the same or similar non-business-related messages to large numbers of email recipients or newsgroups.