Statement of Acceptance Use of Computing Resources

Effective April 15, 1996

The University values openness and promotes access to a wide range of information. Campus information systems have been designed to be as open as possible, and as such the University insists on responsible use of these systems.
The use of computers, electronic information and computer networks is essential for research, instruction and administration within the academic community. Because the electronic environment is easily disrupted and electronic information is readily reproduced, respect for the work and rights of others is especially important.

Users of the University's facilities are expected to adhere to this policy and, by accessing the system, the user agrees to comply with and be subject to this policy. These policy statements are intended to augment, not supersede, any additional contractual agreements of conduct or confidentiality to which a user may be subject. The University reserves the right to amend this policy at any time with or without notice. Questions or comments regarding this document should be addressed to the Director of Information Systems and Technologies.

User Responsibilities

Access to University computing and networking resources is a privilege which is available to all members of the academic community. Certain responsibilities accompany that privilege. Understanding them is important for all computer users. The framework of responsible, considerate, and ethical behavior expected by the University extends to coverage of the use of all campus computers, campus network resources, and networks throughout the world to which the University provides computer access.

The user is responsible for the correct use of the tools each computer system provides for maintaining the security of stored information. A summary of the security procedures relevant to this end is given below:

a. Computer accounts, passwords, lab access cards, and other types of authorization are assigned to individual users and should not be shared with others unless specifically authorized by proper University officials. The person to whom an authorization is assigned will be held accountable for any activity originating from that account.

b. The user should select an obscure password and change it frequently.

c. The user should seek to understand the level of protection each computer system automatically applies to files and supplement that protection, if necessary, for sensitive information.

d. It is incumbent upon every user to adhere to security policies and procedures and to call to the attention of Information Systems and Technologies those whom they feel are violating these procedures. Every effort will be made to ensure total anonymity.

e. If a user should encounter or observe a flaw in system or network security, this discrepancy must be reported to Information Systems and Technologies. Individuals must refrain from exploiting any such lapse in security.

f. The computer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being either their victim or propagator

Confidentiality

In general, information stored on computers is considered confidential, whether protected by the computer system or not, unless the owner intentionally makes that information available to other groups or individuals. The University of Wisconsin Oshkosh takes the position that computer users wish the information they store on central and campus shared computing resources to remain confidential.

Users should be aware that data (including e-mail) may, due to software or hardware failure, become accessible to those who are not explicitly authorized for that access. Systems management personnel may also on occasion have access to such data while performing routine operations or pursuing apparent systems or user problems. Systems personnel are required to report apparent improper or illegal activities so discovered. No guarantee of complete privacy is made or implied by this policy.

Requests for the disclosure of confidential information will be governed by the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Wisconsin Open Records Statutes (Chapter 19, Ss 19.31 - 19.39, Laws of 1992). All such requests will be honored only when approved by University officials who are the legal custodians of the information requested, or when required by state or federal law, or court order. Users found to be copying, modifying, or otherwise accessing information for which they have not been granted permission will be liable to disciplinary action.

Inappropriate Usage

Users must be sensitive to the public nature of shared facilities. Behavior reflects both upon the individual and the University. Computing and networking resources should be used only in accordance with this policy. Any intentional behavior with respect to the electronic environment that interferes with the missions or activities of the University or members of the University community will be regarded as unethical and may lead to disciplinary action under standard University rules for misconduct and existing judicial, disciplinary or personnel processes. Examples of inappropriate and unacceptable use of computing and networking resources include, but are not limited to, the following:

a. Destruction of, unauthorized removal of, or damage to equipment, software, or data belonging to the University of Wisconsin Oshkosh or other users.

b. Disruption or unauthorized monitoring of electronic communications. Tampering, modification, or additions to network software, hardware, or wiring.

c. Generation of excessive network traffic exceeding levels which create errors or performance problems for all users. Applications or computer hardware found to cause such problems may be moved to a different location or removed from the network, at the discretion of the network management staff.

d. Willful violations of computer system security.

e. Use of e-mail or messaging services to harass, intimidate, or otherwise annoy another person, for example, by broadcasting unsolicited messages or sending unwanted mail. Some mass mailings may be authorized by appropriate University authority. This would also apply to material originating from this campus but sent to other sites or persons on the Internet.

f. Use of computer accounts, access codes, or network identification numbers other than those assigned to you.

g. Use of computer and/or network facilities in ways that impede the computing activities of others (for example, randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, playing games on shared resources, or the overuse of network-accessible discussion lists or file-transfer sites).

h. Setting up network servers or network services (such as naming and/or address servers, Web servers, dial-in access, file servers, etc.) without the prior authorization of the network management staff. Unauthorized activity of this type may be detrimental to the overall operation of the network and is not allowed.

i. Intentionally creating, displaying, printing or transmitting information which violates the university's sexual harassment policy.

j. Use of computing facilities for financial gain or commercial purposes unrelated to the mission of the University.

k. Violation of software copyrights and usage licensing agreements.

l. Violation of the usage policies and regulations of the networks of which the University of Wisconsin Oshkosh is a member or has authority to use.

m. Academic dishonesty (for example, plagiarism or cheating).

Sanction and Appeal Process

Violation of the policies described herein for use of computing resources will be dealt with seriously. Violators are subject to disciplinary procedures of the University, may lose computing privileges or account and network access, and may also be subject to prosecution by state and federal authorities under laws including, but not limited to: The Privacy and Protection Act of 1974; Wisconsin Statutes 1992-93, (41st Edition) (Chapter 19, Public Records and Property, Ss 19.31 - 19.39; Chapter 939, Crimes - General Provisions, Ss 939.32(2), 939.50(3), 939.51(3), 939.66(4), 939.72(3); Chapter 943, Crimes Against Property, Ss 943.70); The Wisconsin Computer Crimes Act; The 1986 Electronic Communications Privacy Act; The Computer Fraud and Abuse Act of 1989. The sanction and appeal process will vary, depending upon the classification of the offender within the University community. Suggested courses of action are described by, but are not limited to:

a. Student - Wisconsin Administrative Code, Section UWS 14 and UWS 17. These regulations are also maintained in a separate document entitled Student Discipline Code, which is available in the Dean of Student's Office.

b. Classified Staff - Administered by the Personnel Office, pursuant to the current University of Wisconsin System Classified Employees Work Rules; Chapter 230.34(1) of Wisconsin Statutes; Section Pers 24 of Wisconsin Administrative Code; and existing collective bargaining agreements.

c. Academic Staff / Faculty - The University of Wisconsin Oshkosh Faculty and Academic Staff Handbook and specific departmental procedures, as warranted.

d. Other - Subject to the procedures of the organization or group with which they are affiliated, revocation of computing privileges, and possible state and federal prosecution.