Policy 01:011 – Computer Resources Security

The University is committed to providing a campus computing environment consistent with its mission. Equal to this commitment is the University's responsibility to ensure the integrity of University data and to encourage and enforce confidential, legal and ethical standards of management and use of these data in compliance with all applicable federal and state laws governing disclosure of information in these data bases.

A University employee or student who, abuses information technology resources by directly or indirectly damaging or destroying any computer, computer system, computer network, program or data, or who causes such act to occur, may be subject to disciplinary action including termination, expulsion, and/or prosecution.

Information germane to the mission and operation of the University, regardless of its format, is a proprietary asset of the University; therefore, it is essential that University information systems be protected from misuse and unauthorized access, modification, destruction or disclosure, whether accidental or intentional. Data stored in these systems belong to the University and must be maintained in a secure environment. The following are examples of violations of University policy:

- Deliberate and/or unauthorized attempts to access or use the University's computers, computer facilities, networks, systems, programs or data or the unauthorized manipulations, including fraudulent transmissions, of any of the above;
- Deliberate and/or unauthorized use of UM facilities or equipment to access non-UM-owned computers or networks;
- Deliberate and/or unauthorized attempts to modify computer equipment, including terminals or other peripherals, or to deny access to such equipment to other users;
- Circumventing or attempting to circumvent normal resource limits, log-on procedures, and security regulations;
- Use of University computer resources and data for purposes for which they are not intended; i.e., personal or commercial enterprises not consistent with the University's mission; or allowing such use by other individuals;
- Deliberate and/or unauthorized activity which causes University computers, computer facilities, systems, programs or data to be accessed, used or transmitted;

- Deliberate and/or unauthorized activity which causes non-UM-owned computers, computer facilities, systems, programs or data to be accessed, used or transmitted in an unauthorized manner;
- Disregard for, abuse of, or violation of copyrights, license provisions and other restrictions including copying or redistributing copyrighted software, data or reports without proper, recorded authorization that applies to computer software, networks or other outside materials; and
- Any other action which interferes with the proper functioning of the system or impinges on another user's rights.

External Networks

Members of the University community who use networks, facilities, or computers not owned by the University shall adhere to this policy and all policies and procedures established by the administrators of non-University networks, facilities, or computers used (policies and procedures can usually be obtained from the network information center of the network in question). Whether or not an external policy exists, University policy shall remain in effect and shall be adhered to at all times.

Electronic Data Disposal

All computer systems, electronic devices, and electronic media must be properly cleaned of sensitive data and software before being transferred outside of the University, either as trade-ins, surplus property, or as trash. Computer Services is responsible for sanitizing and/or properly disposing of computer hard drives that are transferred for disposal. Departments that directly dispose of equipment are responsible for the removal of all data from the computer hard drives. Disposal of electronic media, including floppy disks, CDs, and printed reports is the responsibility of the department that purchases or produces them.

Violations of this policy may constitute theft and/or unauthorized use of University property, subjecting violators to possible criminal prosecution, if applicable, dismissal or suspension from employment or enrollment, and/or other civil and legal remedies, which may be available.

Approved 5/99

Last Revised 8/05