X-1.00(A) UNIVERSITY OF MARYLAND POLICY ON THE ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

(Approved by the President, April 5, 2006)

PRIMARY PRINCIPLES: FREEDOM OF EXPRESSION AND PERSONAL RESPONSIBILITY

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at the University of Maryland. These values lie at the core of our academic community. Censorship is not compatible with the tradition and goals of the University. While some computing resources are dedicated to specific research, teaching, or administrative tasks that would limit their use, freedom of expression must, in general, be protected. The University does not limit access to information because of its content when it meets the standard of legality. The University's policy of freedom of expression applies to computing resources.

Concomitant with free expression are personal obligations of each member of our community to use computing resources responsibly, ethically, and in a manner which accords both with the law and the rights of others. The University depends first upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

GENERAL

This policy sets forth standards for responsible and acceptable use of University information technology (IT) resources. These resources include computer systems, computer labs, applications, networks, software, and files.

IT resources are provided to support the academic, research, instructional, and administrative objectives of the University. These resources are extended for the sole use of University faculty, staff, students, and all other authorized guests to accomplish tasks related to the status of that individual at the University, and consistent with the University’s mission.

Those using University IT resources, whether at the University or elsewhere, are responsible for complying with security standards set forth by the Vice President and Chief Information Officer (VP/CIO), safeguarding identification codes and passwords, and for using them solely for their intended purposes. Individuals are solely responsible for their personal use of IT resources and are prohibited from representing or implying that statements related to such use constitute the views or policies of the University.

The maintenance, operation, and security of IT resources require responsible University personnel to monitor and access systems and networks. To the extent possible in the electronic environment and in a public setting, a user’s privacy will be preserved. Nevertheless, that privacy is subject to applicable federal and state law, including the Maryland Public Information Act, and the needs of the University to meet its administrative, business, and legal obligations.

PROHIBITED CONDUCT

The following provisions describe conduct prohibited under this policy:

1. Altering system software or hardware configurations without authorization; disrupting or interfering with the delivery or administration of IT resources.

2. Attempting to access or accessing another's accounts, private files, e-mail messages, or intercepting network communication without the owner's permission except as appropriate to your job duties and in accordance with legitimate University purposes.

3. Misrepresenting oneself as another individual in electronic communication.

4. Installing, copying, distributing, or using digital content (including software, music, text, images, and video) in violation of copyright and/or software agreements or applicable federal and state law.

5. Engaging in conduct that interferes with others' use of shared IT resources.

6. Using University IT resources for commercial or profit-making purposes or to represent the interests of groups unaffiliated with the University or unassociated with the normal professional activities of faculty, staff or students without written authorization from the University.

7. Ignoring individual departmental or unit lab and system policies, procedures, and protocols.

8. Facilitating access to University IT resources by unauthorized users.

9. Exposing sensitive or confidential information or disclosing any electronic information that one does not have the authority to disclose.

10. Knowingly using IT resources for illegal activities. Criminal or illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, University trademark infringement, defamation, theft, identity theft, and unauthorized access.

ENFORCEMENT

Violation of the provisions of this policy constitutes unacceptable use of IT resources, and may violate other University policies and/or state and federal law. Known or suspected violations should be reported to the appropriate University computing unit. Reports may also be sent to the security unit within the Office of Information Technology (abuse@umd.edu). If possible, reports should include a copy of any non-sensitive information relevant to the putative violation.

Violations will be acted upon by the appropriate University authorities and/or law enforcement agencies. Violations may result in the restriction or revocation of access to IT resources; faculty, staff, or student disciplinary action; academic dishonesty proceedings through the Student Honor Council; or legal action.

The VP/CIO or designee may suspend, block, relocate to a secure location, or restrict access to information and network resources when necessary to protect the integrity, security, or functionality of University IT resources or to protect the University from liability. Notice of such action will be provided to the designated security contact for the affected unit.

ADMINISTRATION

Individual areas within the University (including divisions, colleges, schools, and departments) may elaborate upon this policy with unit-specific policies as long as they do not violate the spirit and intent expressed elsewhere in this policy.

Consistent with University System of Maryland requirements, this policy will be reviewed and updated annually or as needed based on the recommendations of the VP/CIO.