

**The University of Tennessee at Martin Office of Information Technology Services
Student Acceptable Use Compliance Form**

Effective Date: 1/30/2004

Revision Date: 1/30/2004, Approved by Chancellor's Staff 12/31/2003

Version: 2004.01

The Student Acceptable Use Compliance Form will be displayed for acceptance upon authorization to connect to the UT Martin network.

- All computers attached to the UT Martin network are required to run current anti-virus software with up to date virus definitions. The software is available from UT Martin. Beginning Fall 2004, student computers will be required to run the UT Martin approved anti-virus software set to load virus definition updates automatically.
- The operating system must be upgraded and patched to the most current version.
- No one shall knowingly or willingly interfere with the security mechanisms or integrity of UT Martin's Technology Resources. Users shall not attempt to circumvent data protection schemes or exploit security loopholes.
- No one shall knowingly create, install, execute, or distribute any malicious code (e.g., virus, Trojan Horse, worm) or another surreptitiously destructive program on any of UT Martin's Technology Resources, except for as explicitly authorized by the campus Information Security Officer or Team and only for the express purpose of improving campus security practices and after special precautions are taken.
- No one shall interfere with the intended use of UT Martin's Technology Resources. All users shall share computing resources (e.g., bandwidth) in an ethical and fair manner and not unduly interfere with use by other authorized users.
- No one shall use UT Martin's Technology Resources to attempt unauthorized use, or interfere with the legitimate use by authorized users, of other computers or networks elsewhere- users are responsible for adhering to the policies and principles of such networks. UT Martin cannot and will not extend any protection to users who violate external network policies. Abuse of networks or computers at other sites through the use of UT Martin Technology Resources will be treated as an abuse of UT Martin Technology Resource privileges.
- No one shall use UT Martin Technology Resources for individual financial or commercial gain; use of these resources, except for authorized University business, is prohibited.
- No one shall perform, participate, encourage, or conceal any unauthorized use or attempts of unauthorized use of UT Martin Technology Resources.
- No one shall use a system either directly attached to UT Martin Technology Resources or through wireless means to capture data packets (e.g., "sniffer") except for authorized or other official University business.
- No one shall use UT Martin Technology Resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by state or federal laws.
- No one shall launch, intentionally or otherwise, denial of service attacks against other users, systems, or networks.

**The University of Tennessee at Martin Office of Information Technology Services
Student Acceptable Use Compliance Form**

Effective Date: 1/30/2004

Revision Date: 1/30/2004, Approved by Chancellor's Staff 12/31/2003

Version: 2004.01

- No one shall abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a University account.
- No one shall connect any computer or network system to any of UT Martin's networks (e.g., direct connection, direct dial-in access, or wireless access) without, at a minimum, requiring user identification and authentication.
- No one shall misrepresent his or her identity or relationship to the University for the purpose of accessing or attempting unauthorized access to UT Martin Technology Resources nor misrepresent his or her identity to other networks (e.g., IP address or email address "spoofing") from UT Martin Technology Resources.
- No user shall access (e.g., read, write, modify, delete, copy, move) another user's files or electronic mail without the owner's permission except by system and LAN administrators duly authorized by the official policies and procedures applicable. In addition, it is the individual user's responsibility to protect his/her files.
- No one shall use UT Martin Technology Resources in violation of applicable patent protection and authorizations, copyrights, license agreements, other contracts, State or federal laws, or by University rules or regulations.
- No one shall place confidential information on computers without appropriately protecting it. The University cannot guarantee the privacy of files, electronic mail, or other information stored or transmitted on UT Martin Technology Resources.
- No one shall compromise the privacy of others or the confidentiality of the information contained on UT Martin Technology Resources.

Violations

Abuse of UT Martin policies or standards, abuse of UT Martin Technology Resources, or abuse of other sites through the use of UT Martin Technology Resources may result in termination of access, disciplinary review, expulsion, termination of employment, legal action, and/or other appropriate disciplinary action.

Notification will be made to the appropriate UT Martin office, e.g., Public Safety, Personnel Services, Student Affairs, or local, State and federal law enforcement agencies.

System administrators and designated security officers or teams will, when necessary, work with other University offices in the resolution of security incidents.

The Security Officer or Team shall establish procedures for isolating and/or disconnecting systems from the network while assessing any suspected or reported security incident in order to minimize risk to the rest of the UT Martin network. In the event of a legal investigation, the University reserves the right to isolate the system and "lock it down" to preserve evidence during investigation by law enforcement agencies.

**The University of Tennessee at Martin Office of Information Technology Services
Student Acceptable Use Compliance Form**

Effective Date: 1/30/2004

Revision Date: 1/30/2004, Approved by Chancellor's Staff 12/31/2003

Version: 2004.01

Reporting Security Incidents & Infractions

Users are expected to report any information concerning instances in which they suspect or have evidence that the above principles have been or are being violated.

Reports about suspected violations of these principles should be directed to helpdesk@utm.edu for customer relations regarding inappropriate public behavior or for network operations or infrastructure. Receipt of incident reports will be acknowledged and investigated in a timely manner.

When a complaint of possible system or account misuse is reported to the University, the validity of the incident will be investigated per standard operating procedures. Any incidents that appear to be valid are forwarded to the appropriate UT Martin office with all supporting documentation or evidence gathered for investigation and resolution. All parties will be informed of the resolution of such incidents.