University of Baltimore

III-A Acceptable Use of Information Technology Resources

Approved by University Council 9/29/06
Approved by AG 8/16/07
Approved by President 9/17/07
Last Reviewed: 11/16/2020

I. Introduction

Access to and use of information technology (IT) and telecommunications is vital to the mission of the University of Baltimore, a mission that includes teaching, lifelong learning, research, and service. IT offers increased opportunities for communication and collaboration, and is essential to achieve a level of excellence in its effective use by all faculty, staff and students.

The use of IT and related resources must be consistent with the University's mission and its role as a public agency. Each member of the University community is expected to protect the integrity of these resources and to know and adhere to University rules, regulations, and guidelines for their appropriate use. Regulations that govern personal conduct and use of University facilities also apply to the use of IT resources.

This Acceptable Use policy establishes standards for responsible and appropriate use of all University IT and network resources. Additional policies may also apply to specific computers, computer systems, or networks at the University of Baltimore, or to uses within specific departments.

This policy applies to all users of University of Baltimore's IT and network resources. By accessing a University of Baltimore IT resource, a user agrees to abide by this policy in its entirety, as the same may be amended from time to time.

II. Guiding Principles

As a public, urban institution of higher education, the University of Baltimore is committed to fostering a climate in which students, faculty and staff can appropriately share information and ideas. The fundamental principles of academic freedom and freedom of expression extend to University IT and network resources. The University does not censor lawful expression of personal opinion, and is not the arbiter of what may be regarded as "offensive" by some members of the community. However, such opinions may not be represented as the views of the University of Baltimore.

III. Definitions

Information technology resources include, but are not limited to, all university-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; UB voice or data network traffic, including traffic entering and leaving the University network; classroom technologies; communication services and devices, including e-mail, voice mail, modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems. Some University computing resources are reserved or dedicated to specific functions that may limit their use by the general UB community. Personal devices used to access University of Baltimore Information Technology resources are subject to this policy.

Authorized users include current University of Baltimore students, faculty, staff, and employees under temporary contract or assignment, and campus visitors.

IV. Acceptable Use Policy Statement

University computing resources are provided to members of the University of Baltimore community in support of instructional, research, service, and administrative missions, for purposes associated with academic programs and professional responsibilities. The use of University of Baltimore Information Technology resources is a privilege, subject to compliance with all applicable policies and laws.

In the interest of making the use of IT resources a natural part of the day-to-day learning and work for all members of the University community, incidental personal (non-commercial) use is tolerated. However, one should use non-University sources of email, Internet access, and other IT services for activities of an extensive nature that are not related to University purposes.

Appendix A of this document contains specific examples of prohibited behavior and activities.

Users of University of Baltimore Information Technology resources shall:

1. Understand and comply with University policies and applicable public laws. Users are responsible for understanding and complying with all laws, rules, policies, contracts, and licenses applicable to their particular uses. Related policy references are located in Appendix A.
2. Make reasonable efforts to protect all assigned accounts and passwords. Account owners are responsible for all actions, network use, and transactions originating from an assigned computer account.
3. Use University IT, network resources, and user accounts for appropriate University activities.
4. Respect all pertinent licenses, copyrights, and contracts.
5. Respect all restricted and/or proprietary data and information.
6. Respect the freedom, rights, and privacy of others.
7. Use IT and network resources responsibly, ethically, and with integrity.
8. Make reasonable efforts to maintain a secure home and/or personal computing environment if devices will be used to access University of Baltimore IT resources.
9. Acknowledge that University of Baltimore may monitor computer or network use to protect the computing environment.
10. Acknowledge that the University of Baltimore may examine files, mail and printer history logs for the purpose of diagnosing and correcting technical problems.
11. Report known violators of University policy and/or laws to the University of Baltimore Information Security Team.

V. Violations

Violations of this policy will constitute unacceptable use of computing resources, and will be investigated and acted upon by appropriate University authorities and law enforcement agencies. The University may confiscate log files, email, documents and university-owned equipment as evidence. The University may temporarily suspend or block access to an account prior to the initiation or completion of such processes, when the action is reasonable to protect the integrity, security, or functionality of IT resources, and/or to protect the University from liability.

Appendix A - Representative Examples of Irresponsible or Prohibited (not intended as an exhaustive list)

1. Due to the potential of a security or data breach, use of another person’s UB credentials and/or sharing your UB credentials with another person is prohibited. (Refer to Section IV, #2)
2. Misrepresentation of yourself or your data on the network.
3. Transmission of threatening, harassing, intimidating, or obscene messages.
4. Use of IT resources to harass, intimidate, defame or discriminate against others or to interfere with ability of others to conduct University business.
5. Use of IT resources to gain unauthorized access to, or attack any remote computer or network.

6. Any intentional act that would deny or interfere with the access and use of IT resources by others, including acts that are wasteful of computing resources, or that unfairly monopolize resources to the exclusion of other users.
7. Violations of copyright law. Copying, or making available on the network copyrighted material, including without limitation, software programs, music files, video files, still and digital images, radio and television broadcasts, and written text works, unless permitted by a license, by the consent of the copyright owner, by a fair use limitation under copyright law, or by permitted copying under the Digital Millennium Copyright Act (DMCA) when made by a library or archive for preservation purposes. Reference the following resources for additional information:
    - USM Bylaws, Policies and Procedures of the Board of Regents, Section IV
    - VII-5.3 Policy on Use of Copyrighted Materials - UB
    - VIII-5.1 Intellectual Property Policy - UB
8. Intentional misuse or theft of software and/or IT resources.
9. Unauthorized or inappropriate access to information resources, data, equipment, or facilities, including, but not limited to: tampering with components of a local-area network (LAN), or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
10. Inappropriate use of data. The unauthorized sale or transfer of data contained on University IT resources on networks (including social security number, date of birth, addresses, and other information that may be used for identity theft).
11. Unauthorized interception or monitoring of communications, user dialog, or password input, circumventing data protection schemes or exploit security loopholes or interfere with standard technical measures that identify and protect the rights of copyright owners.
12. Altering or disrupting system software or hardware configurations without authorization.
13. Introduction of unauthorized, independent computer or network hardware to the University IT environment. Personal devices may not be connected to the University secure network without written authorization from the Office of the CIO. (Refer to UB Network Security Policy)
14. Unauthorized use, or permitting unauthorized use of and access to electronic distribution lists and/or mailing lists created by the University of Baltimore.
15. Use of University IT resources for personal profit or to solicit sales for any goods, services, or contributions not authorized by UB.
16. Use of University IT resources by University employees to support the nomination of any person for political office, or to influence a vote in any election or referendum.

Appendix B - Related Policy and Information References

1. University of Baltimore Information Technology Security Policy
2. University of Baltimore Network Security Policy
3. University of Baltimore Email Policy
4. University of Baltimore Email Guidelines
5. University of Baltimore Student Affairs Policies
6. University of Baltimore Bogomolny Library Code of Conduct
7. University of Baltimore Law Library Policies
8. Bogomolny Library Copyright Information
9. University System of Maryland Board of Regents Bylaws, Policies, and Procedures