

University of Maryland Baltimore (UMB) BioPark Customer Acceptable Use Policy

Effective Date: 9/1/2005

I. Purpose

This Policy addresses acceptable use, and unacceptable misuse, of internet services ("Services") provided by UMB to BioPark occupants under contracts with those business.

II. Definitions

"Customer": an organization located at the UMB BioPark which contracts with UMB for Services.

"Authorized Users": persons authorized by a Customer to use UMB Services at the Customer's BioPark facility.

"CIO": the UMB Vice President of Information Technology and Chief Information Officer.

"IT Representative": the representative of a Customer designated by the Customer as responsible for oversight of the Customer's use of Services.

"IT Resources": all information technology resources, including, but not limited to, computerized information, computing facilities, computer networks, hardware, software, systems, programs and devices.

"UMB IT Resources": IT Resources owned, leased, or used by UMB, and used by UMB or by Customer so that Customer can access the Services.

"UMB": University of Maryland Baltimore (including all its schools and administrative units).

III. Requirement of Acceptable Use

Customers and Authorized Users must use Services and UM IT Resources in accordance with UMB policies, procedures, and guidelines, software licenses and contracts UMB enters into regarding Services, and applicable laws. Use of Services must be responsible and professional.

Direct and indirect use of Services and UM IT Resources made available to a Customer and its Authorized Users is a privilege granted by UMB, and is revocable by UMB at the discretion of the CIO.

IV. Misuse

Misuse is use of Services and UM IT Resources in a manner not consistent with standards for acceptable use. Misuse by Customers and their Authorized Users includes, but is not limited to:

- A. Securing unauthorized access to or unauthorized use of Services or UM IT Resources, or facilitating such use or access by another person.
- B. Accessing or attempting to access Services or UM IT Resources without authorization. This is also referred to as hacking.
- C. Any deliberate or reckless act that denies or interferes with the access and use of Services or UM IT Resources by others.
- D. Use of Services or UM IT Resources in violation of the law, the policies of UMB, or the terms of contracts through which UMB secures any part of the Services.
- E. Personal communication, or other personal use, that interferes with the use of Services and UM IT Resources by Authorized Users or by UMB and its personnel.
- F. Software theft or piracy, data theft, copyright violations, and other actions that violate intellectual property rights of others.
- G. Inappropriate access, use or disclosure of data including social security numbers, birth dates, or addresses; unauthorized sale or transfer of such information.
- H. Altering UMB system hardware configurations without authorization; installing or deleting system software without authorization; installing or removing system hardware without authorization.
- I. Intercepting or monitoring communications, user dialog, or password input intended for another recipient.
- J. Collecting or storing information about users of Services or UMB IT Resources without user authorization.
- K. Illegal activity.
- L. Business or commercial activity not related to the Customer's activities in the BioPark.
- M. Transmitting messages that are threatening, obscene, vulgar, derogatory or harassing, messages that attack another individual or group of individuals, or messages that violate the policies of UMB.
- N. Anomalous (unusual or unexpected) internet activity that is illegal or wasteful of UMB IT Resources, that violates the terms of use of the licenses and agreements through which UMB obtains or uses UMB IT Resources, or that violates the terms of the Customer's agreement with UMB for Services.

V. Security and Monitoring

The maintenance, operation, and security of UMB IT Resources require UMB to monitor and access IT Resources. UMB monitors UMB IT Resources and Customer's use of Services as part of normal operations and maintenance. Normal monitoring includes, but is not limited to, logging activity and monitoring usage patterns. In special situations, communications including internet activity of specific individuals or systems are subject to monitoring by UMB for other purposes, e.g., allegations of violation of law or allegations of unauthorized use of Services and UM IT Resources.

To the extent feasible, as determined by UMB, and taking into account the electronic environment and the public agency status of UMB, UMB will protect the confidentiality of Customer communications and data transmitted with use of Services. Access to and disclosure of confidential information to others in any manner not permitted by law is prohibited.

There is no assurance of confidentiality or privacy for much of the information transmitted using Services. State and federal laws, and the needs of UMB to meet its administrative, business, and legal obligations, require UMB to routinely monitor activities involving Services and UM IT Resources, and may require UMB to access and view communications using Services.

UMB seeks to maintain the security of UM IT Resources, but cannot guarantee security. Customers and Authorized Users have no expectation of privacy as to information stored or transmitted using Services and UM IT Resources, and generally should not maintain or transmit sensitive commercial or personal information using Services or UM IT Resources. Customers are responsible for making arrangements, independent of UMB, for encryption and other protective measures regarding their business information transmitted via the internet using Services.

UMB may monitor the use of Services by Customer and its Authorized Users without notice to Customer or the Authorized User in situations when it is necessary or appropriate in the judgment of the CIO, e.g.:

- The activity has been made available to the public, as by posting to an electronic list or web page.
- Monitoring is necessary to preserve the security, integrity, or functionality of Services and IT Resources.
- UMB has a reasonable basis to suspect that Customer or an Authorized User may be violating this Policy, or the terms of Customer's agreement with UMB for Services.
- Use of Services is demonstrating anomalous activity based on usage patterns.
- UMB has a reasonable basis to suspect that a person using Services made available to Customer is doing so without authorization.
- Otherwise necessary, as permitted by law, required by lawful directive to UMB, or required to investigate allegations of misuse of UM IT Resources.

When monitoring of specific activity and accounts is required, the CIO will consult with the IT Administrator prior to monitoring activities of specific Authorized Users.

VI. Administration and Enforcement of Policy

The CIO is responsible for the administration and enforcement of this Policy. Allegations of violations by Customers and Authorized Users will be resolved by the CIO following consultation with the IT Administrator. The CIO may suspend a Customer's Services until an investigation is completed.

The CIO shall refer suspected criminal violations of law to the University Police and concurrently advise University Counsel of the matter.

Immediate action may be taken by the CIO in response to potential or ongoing threats to UM IT Resources security, the health or safety of persons, the privacy rights of students, employees, patients, clients, research subjects or others, compliance with the law, or the security of confidential or proprietary information.