The UMB School of Nursing follows and adheres to the UMB Campus Information Technology Acceptable Use Policy. The UMSON further defines “Authorized User” to also include any person who receives a password ID from the UMSON, or who uses an e-mail address that ends in “son.umaryland.edu” to be an Authorized User.

University of Maryland Baltimore
Information Technology Acceptable Use Policy

Purpose

The purpose of this policy is to state what constitutes the acceptable use and what constitutes the misuse of UMB IT Resources (as defined below). This policy also states responsibilities and procedures for administering and enforcing this policy, reporting violations, and initiating disciplinary actions against those who violate this policy.

Definitions

“Affiliate": an organization located at the UMB campus which has IT Resources connected to UMB IT Resources, or which has IT Resources used by Authorized Users; also, an organization located off campus which provides IT Resources used by Authorized Users in the course of their activities in relation to their affiliation with UMB or an Affiliate; also, does not include a business entity which contracts with UMB for IT services.

"Authorized Users": students, faculty, staff, visitors, and guests of UMB who use UMB IT Resources, on-campus or off-campus, in the course of UMB employment, educational activities, or other purposes related to their UMB affiliation; also, employees of Affiliates who use UMB IT Resources to fulfill their employment responsibilities, and any other persons authorized to use UMB IT Resources. Any person who receives a password ID from UMB or who uses an e-mail address that ends in "umaryland.edu" is an Authorized User. All Authorized Users are subject to this policy.

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

"IT Administrator": the administrator or academic officer of a UMB unit or school who, as determined by the applicable vice president or dean, is responsible for management and oversight of the IT Resources located in, or used by Authorized Users affiliated with that unit or school.

"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 or its Affiliates, or by USM, and used by Authorized Users.

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

"USM": University System of Maryland.

Scope

This policy applies to all Authorized Users.

Acceptable Use

In general, acceptable use of UMB IT Resources is use in support of the research, education, service, and administrative activities of UMB or of an Affiliate. Authorized Users should always use IT Resources in accordance with UMB, USM, and Affiliate policies, procedures, and guidelines, software licenses, and applicable laws. UMB depends upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users of UMB IT Resources. Use of UMB IT Resources must be responsible and professional. Acceptable use balances limits necessitated by law, economy, security and privacy with the principles of academic freedom and constitutional rights of free speech.

Authorized Users are responsible for safeguarding their own identification (ID) codes and passwords, and for using them for their intended purposes only. Authorized Users are solely responsible for all transactions made under the authorization of their ID, and for activity involving IT Resources which originate from computing devices owned by or assigned to them. Authorized Users may not represent or imply that personal electronic publications (e.g. web pages) or personal communications reflect the views or policies of UMB.

Authorized Users may not state or imply that links provided from web pages hosted on UMB IT Resources constitute or imply a UMB endorsement of those sites, their content, or products and services associated with those sites.

Direct and indirect use of UMB IT Resources made available to an Authorized User is a privilege granted by UMB. The privilege is subject to compliance with this policy, other applicable UMB and USM policies, Affiliate policies and State and federal laws.

Misuse

Misuse is use of UMB IT Resources in a manner not consistent with standards for acceptable use. Misuse includes, but is not limited to:

A. Securing unauthorized access to or unauthorized use of UMB IT Resources, or facilitating such use or access by another person.
B. Accessing or attempting to access UMB IT Resources on or off the UMB campus without authority. This is also referred to as hacking.
C. Any deliberate or reckless act that denies or interferes with the access and use of UMB IT Resources by others
D. Use of UMB IT Resources in violation of the law, the policies of UMB, USM, or an Affiliate, or the policies or guidelines of any UMB school or unit. Examples of such prohibited use include violations of anti-discrimination or harassment policies, and a school’s honor code.
E. Personal communication, or other personal use, that interferes with the use of UMB IT Resources by Authorized Users for official UMB purposes and for academic responsibilities, or that interferes with or indicates neglect of employment

responsibilities (e.g. use of internet auction sites such as eBay, internet gaming, chat rooms, instant messaging, and web surfing during work hours).

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 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, except when this is done as part of authorized IT resource management, when authorized by the CIO, or if required by law.
J. Collecting or storing information about users of UMB IT Resources without user authorization, except as necessary for official UMB activities and functions.
K. Illegal activity.
L. Business or commercial activity not carried out on behalf of UMB or an Affiliate.
M. Access to or use of electronic distribution lists and email accounts created by UMB, a school or unit of UMB, or an Affiliate, for purposes not authorized by UMB, the school, or the unit; permitting others access to such distribution lists for unauthorized purposes.
N. 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 or USM, any school or unit of UMB, or any Affiliate of UMB.
O. Anomalous (unusual or unexpected) computing activity that is illegal or wasteful of UMB IT Resources or that violates the terms of use of the licenses and agreements through which UMB obtains or uses UMB IT Resources.

Security and Monitoring

The maintenance, operation, and security of UMB IT Resources require UMB and Affiliates to monitor and access IT Resources. UMB and its Affiliates monitor UMB IT Resources 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 and Affiliates for other purposes, e.g., investigation of complaints of violation of work rules, allegations of violation of law, or allegations of unauthorized use of UMB 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 academic information, student information, medical information, attorney-client and patient-provider communications, attorney work product and information developed from or exchanged with clients and patients which is stored and transmitted through UMB IT Resources. Authorized Users may only access confidential information with UMB permission and only to the extent authorized.   Access to and disclosure of confidential information to others in any manner not permitted by law, UMB policy and procedure, and the applicable policies of the school, unit or Affiliate that maintains the information, is prohibited. UMB will not disclose privileged or confidential communications from legal clients, attorney work product, student information, employee information, or medical or health care record information unless permitted by law, authorized by the client or patient, or approved by the school, unit or Affiliate that maintains the information

There is no assurance of confidentiality or privacy for much of the information transmitted or stored by UMB IT Resources. The Maryland Access to Public Records law applies to electronic data, including archived electronic messages. Other state and federal laws, and the needs of UMB to meet its administrative, business, and legal obligations, require UMB to routinely monitor activities involving UMB IT Resources and may require UMB to access and view stored data.

UMB seeks to maintain the security of UMB IT Resources, but cannot guarantee security. Authorized Users have no expectation of privacy as to information stored or transmitted using UMB IT Resources, and generally should not maintain or transmit sensitive personal information about themselves or others using UMB IT Resources. However, UMB IT Resources which have appropriate security measures in place can be used for personal information of clients, research subjects, and patients.

Related security policies of UMB, its schools, units and Affiliates apply to certain categories of personal information (e.g., medical records, UMB Law Clinic records, records of Affiliate health care organizations) stored or transmitted using UMB IT Resources. Authorized Users must comply with these policies.

UMB may monitor the specific activity and accounts of any Authorized User without notice to the Authorized User in situations when it is necessary or appropriate in the judgment of the CIO or a school, unit or Affiliate IT Administrator, for example:

- The user has voluntarily made the activity or account information 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 IT Resources.
- UMB or an Affiliate has a reasonable basis to suspect an Authorized User may be violating this policy.
- A user of UMB IT Resources, or an account, is demonstrating anomalous activity based on usage patterns.
- UMB or an Affiliate has a reasonable basis to suspect that a person using UMB IT Resources is doing so without authorization.
- Otherwise necessary, as permitted by law, required by lawful directive to UMB or an Affiliate, or required to investigate allegations of misuse of UMB IT Resources.

When monitoring of specific activity and accounts is required, the CIO or designee, or the IT Administrator, will consult with an academic or administrative unit's Dean or Vice President, or designee, prior to monitoring activities of specific Authorized Users, and prior to disclosing patient or client information as permitted by law or authorized by the patient or client. If a matter directly involves a Dean or Vice President, the President may waive this consultation requirement.

Electronic Mail (E-Mail)

Copyright laws, license agreements, USM and UMB policies, and state and federal law apply to e-mail. E-mail sent with the intent of disrupting communication or other system services is not allowed. The proliferation of unsolicited commercial e-mail (also known as UCE or "spam"), virus warnings, urban legends and electronic chain letters are not acceptable uses of UMB IT Resources.

Broadcast e-mail, i.e., e-mail messages sent to a list of users in all schools and units of UMB, is forbidden unless approved by the President or his designee. Broadcast e-mail to users in a particular school or unit is prohibited unless permitted by the Dean of the school or Vice President of the unit, or that administrator's designee.

The primary purpose, and primary use, of e-mail using UMB IT Resources is for UMB-related activities. Occasional use of e-mail for personal communications during the business day is acceptable. Users are advised; however, that they have no right of privacy in personal communications sent or received using campus email. Such messages, like all other messages, are subject to monitoring and disclosure as stated above.

Web Pages

Any Authorized User who creates, maintains or hosts a web page using UMB IT Resources is responsible for the integrity of the information contained on the page and for compliance with USM and UMB policies, and federal and state laws, including laws governing copyright, obscenity, defamation, and software piracy.

Personal web pages and commercial web pages may not be posted using UMB IT Resources unless expressly authorized by a UMB school, unit or Affiliate and then only if the web page is related to the academic activities of the school or the operational activities of the unit or Affiliate. Web pages that are not in good taste are not allowed. Anyone who wants a web page primarily or exclusively for personal or commercial purposes, rather than academic activities or the operational activities of UMB or an Affiliate, should not use UMB IT Resources to create or host the web page.

Administration and Enforcement of Policy

The CIO is responsible for the administration of this policy. Each school, unit, and Affiliate of UMB, and the IT Administrator of each UMB School, unit, or Affiliate may provide additional guidelines for appropriate use of UMB IT Resources in that school, unit, or Affiliate.

Enforcement of this policy is delegated to the heads of the UMB schools and administrative units, i.e., deans and vice presidents. In cases where there is a question about authority to enforce this policy a determination shall be made by the UMB President or a designee, normally the CIO.

Violations

Suspected violations of this policy shall be reported to the CIO, the IT Administrator of any school or unit involved, and the IT Administrator of any Affiliate involved. Within a school or unit, the IT Administrator will report the suspected violation to those responsible for supervision of the Authorized Users involved, unless complete confidentiality is required during an investigation of the violation, and to those responsible for administration of disciplinary policies applicable to the Authorized Users involved. Authorized Users who are accused of violating this policy and who have a student or employment relationship, or an academic appointment with UMB, will be subject to disciplinary actions or other proceedings consistent with an accusation of misconduct.

The CIO and/or IT Administrator shall investigate thoroughly the issues concerning use of UMB IT Resources, provide a complete report to the School or employing unit, and cooperate in disciplinary proceedings.

Allegations of violations by Authorized Users other than students, employees or appointees will be resolved by the CIO in consultation with the applicable school, unit or Affiliate. The CIO may suspend an accused user's access to some or all UMB IT Resources until an investigation is completed and, if required, a hearing has been held to determine the validity of the allegations involved.

Authorized Users who commit serious or repeated violations of this policy are subject to additional sanctions. Such additional sanctions may include permanent termination of access to UMB IT Resources, use restrictions, or special monitoring of activities involving UMB IT Resources.

The CIO or any IT Administrator 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 or an IT Administrator in response to potential or ongoing threats to UMB IT Resource 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.

Violations of this policy may result in actions under Human Resource policies, faculty policies, or student policies, in addition to actions under this policy. Termination of enrollment, employment or appointment may follow from violations of this policy.

School and Unit Responsibilities

Schools and units may require their Authorized Users to follow additional guidelines for appropriate use of school and unit UMB IT Resources. Such guidelines shall be no less restrictive than this policy and do not supplant this policy.

When Authorized Users change status, e.g., upon resignation, termination, graduation, retirement, imposition of a disciplinary sanction, or a change in position, role or responsibilities within UMB, the school or unit responsible for initiating a change in status must coordinate with central support units (e.g., Center for Information Technology Services, Human Resource Services, Payroll) to discontinue or change access and authorization to UMB IT Resources accessible to the Authorized User before the change of status.

Change history

Date	**Version**	**Created by**	**Description of change**
5/1/2013	1.0	Fred Smith	Basic document update