



[Home](#) — [Information Technology](#) — [Software & Systems](#) — [Email](#) — [Student Acceptable Use Policy](#)

☰ Menu ▼

Student Acceptable Use Policy

1.0 Preface

This document describes the guidelines that Information Technology uses in providing services to its clients. Information Technology has great leeway within these guidelines to ensure that services it administers are operated as smoothly as possible.

Many people and organizations, local and distant, use university resources. Within this document we refer to this collective group as clients. This document is intended to tell clients what they can expect from Information Technology and what Information Technology expects from them.

2.0 Information Technology responsibilities

Information Technology operates a variety of services for its clients, and assures its clients that these services will be reliable. By reliable we mean that the services will operate according to schedule, efficiently, correctly, and securely. Information Technology will take any action necessary, including unannounced inspection of a client's files, network traffic, denial of access, and instigation of formal University disciplinary procedures, in order to protect the reliability of the services and the security of information. In addition to the policies and responsibilities discussed in this document, Information Technology will also rely on other relevant University documents, such as University of Massachusetts Policies and Guidelines when appropriate.

2.1 UMass Boston Network services

Information Technology maintains connections to various networks, and considers these connections to be among the most vital of our services. Information Technology has a responsibility to help maintain the reliability of computers and networks at other sites. Information Technology will treat any attempt to compromise the reliability of another computing system through the University's computer network as if the attempt were directed at Information Technology's computers.

2.2 Moderate security

Information Technology makes every effort to ensure that the information in its systems is secure. By secure we mean that the information stored in the computer will be safe from unauthorized access, and that Information Technology won't lose the information. It is important to realize that Information Technology cannot make these guarantees absolute. Clients have a variety of levels of security available, and must choose the level appropriate for their own information.

2.3 Privacy

Information Technology will only inspect the contents of non-public files to protect the reliability of its services. Information Technology makes no attempt to censor any information held on its systems. Information Technology may be called upon to provide information and/or files to law enforcement agencies for the express purpose of assisting in active criminal investigations.

2.4 Backup

Information Technology runs regular file backups on its computers. Theoretically, in the event of a computer failure, it is possible to recover all information stored in a computer at the time of the last backup. There are, however, occasional problems with these restorations which can result in other lost information. Information Technology does not restore email messages or mailboxes except in the sole case of a total system restore when recovering from some type of computer disaster.

3.0 Client responsibilities

Information Technology clients must bear certain responsibilities in order to continue using Information Technology resources. Responsible clients are necessary if Information Technology is to provide reliable services. Information Technology computer systems are not immune to tampering. Information Technology relies on its clients to refrain from deliberate attempts to abuse the systems. Information Technology clients are responsible for contacting Information Technology prior to undertaking any activity which Information Technology could interpret as compromising the reliability and security of computer systems and networks. Several other specific responsibilities are described below.

3.1 Proper Use

Information Technology computers and networks are funded by a variety of State and University sources. University employees and students may use Information Technology resources only for work done for the University, and only when it is appropriate that the work be supported by public funds. Personal, for-profit activities are explicitly forbidden.

3.2 Sharable Resource

Information Technology resources are limited, and shared by many clients. To avoid performance problems and/or unnecessary expenses, clients must refrain from initiating activities that consume an unreasonable amount of resources.

3.3 Unauthorized Access

Clients must only access information that belongs to them, is permitted to them, or is public. Clients must not attempt to decode, crack, or discover passwords that belong to others. Information Technology may remove clients who are found to possess programs that could be used to access private information that belongs to others.

Clients can ensure the privacy of their own information by being careful to NEVER share a password with anyone. Do not send passwords through email, because others can easily scan email messages looking for them.

3.4 Harassment

Information Technology clients must not use University resources to harass others. This is considered a serious offense which Information Technology will pursue according to University regulations. Information Technology considers displaying or sending of un-requested, objectionable (as defined by the recipient) material to others to be harassment.

Clients may not use University resources to support inappropriate activities on any network, even if the activities don't interfere directly with University resources. Information Technology will pursue allegations of inappropriate network activities with the utmost diligence.

3.5 Back-up files

Clients are responsible for maintaining their own multiple, current back-up copies of valuable or critical information to insure against inadvertent loss by Information Technology.

3.6 Pay attention to Information Technology Information

Information Technology may at times use its systems to provide clients with important information. We ask that clients pay attention to announcements and/or requests in order to protect themselves from unnecessary difficulties.

This document describes the guidelines that Information Technology uses in providing services to its clients. Information Technology has great leeway within these guidelines to ensure that services it administers are operated as smoothly as possible.

Many people and organizations, local and distant, use University resources. Within this document we refer to this collective group as clients. This document is intended to tell clients what they can expect from Information Technology and what Information Technology expects from them.

2.0 Information Technology responsibilities

Information Technology operates a variety of services for its clients, and assures its clients that these services will be reliable. By reliable we mean that the services will operate according to schedule, efficiently, correctly, and securely. Information Technology will take

any action necessary, including unannounced inspection of a client's files, network traffic, denial of access, and instigation of formal University disciplinary procedures, in order to protect the reliability of the services and the security of information. In addition to the policies and responsibilities discussed in this document, Information Technology will also rely on other relevant University documents, such as University of Massachusetts Policies and Guidelines when appropriate.

2.1 UMass Boston Network services

Information Technology maintains connections to various networks, and considers these connections to be among the most vital of our services. Information Technology has a responsibility to help maintain the reliability of computers and networks at other sites. Information Technology will treat any attempt to compromise the reliability of another computing system through the University's computer network as if the attempt were directed at Information Technology's computers.

2.2 Moderate security

Information Technology makes every effort to ensure that the information in its systems is secure. By secure we mean that the information stored in the computer will be safe from unauthorized access, and that Information Technology won't lose the information. It is important to realize that Information Technology cannot make these guarantees absolute. Clients have a variety of levels of security available, and must choose the level appropriate for their own information.

2.3 Privacy

Information Technology will only inspect the contents of non-public files to protect the reliability of its services. Information Technology makes no attempt to censor any information held on its systems. Information Technology may be called upon to provide information and/or files to law enforcement agencies for the express purpose of assisting in active criminal investigations.

2.4 Backup

Information Technology runs regular file backups on its computers. Theoretically, in the event of a computer failure, it is possible to recover all information stored in a computer at the time of the last backup. There are, however, occasional problems with these restorations which can result in other lost information. Information Technology does not restore email messages or mailboxes except in the sole case of a total system restore when recovering from some type of computer disaster.

3.0 Client responsibilities

Information Technology clients must bear certain responsibilities in order to continue using Information Technology resources. Responsible clients are necessary if Information Technology is to provide reliable services. Information Technology computer systems are not immune to tampering. Information Technology relies on its clients to refrain from deliberate

attempts to abuse the systems. Information Technology clients are responsible for contacting Information Technology prior to undertaking any activity which Information Technology could interpret as compromising the reliability and security of computer systems and networks. Several other specific responsibilities are described below.

3.1 Proper Use

Information Technology computers and networks are funded by a variety of State and University sources. University employees and students may use Information Technology resources only for work done for the University, and only when it is appropriate that the work be supported by public funds. Personal, for-profit activities are explicitly forbidden.

3.2 Sharable Resource

Information Technology resources are limited, and shared by many clients. To avoid performance problems and/or unnecessary expenses, clients must refrain from initiating activities that consume an unreasonable amount of resources.

3.3 Unauthorized Access

Clients must only access information that belongs to them, is permitted to them, or is public. Clients must not attempt to decode, crack, or discover passwords that belong to others. Information Technology may remove clients who are found to possess programs that could be used to access private information that belongs to others.

Clients can ensure the privacy of their own information by being careful to NEVER share a password with anyone. Do not send passwords through email, because others can easily scan email messages looking for them.

3.4 Harassment

Information Technology clients must not use University resources to harass others. This is considered a serious offense which Information Technology will pursue according to University regulations. Information Technology considers displaying or sending of un-requested, objectionable (as defined by the recipient) material to others to be harassment.

Clients may not use University resources to support inappropriate activities on any network, even if the activities don't interfere directly with University resources. Information Technology will pursue allegations of inappropriate network activities with the utmost diligence.

3.5 Back-up files

Clients are responsible for maintaining their own multiple, current back-up copies of valuable or critical information to insure against inadvertent loss by Information Technology.

3.6 Pay attention to Information Technology Information

Information Technology may at times use its systems to provide clients with important

information. We ask that clients pay attention to announcements and/or requests in order to protect themselves from unnecessary difficulties.

Information Technology Services

Healey Library, 3rd Floor

617.287.5220

ITServiceDesk@umb.edu

Back To Top 

100 Morrissey Blvd.

Boston, MA 02125

617.287.5000

Contact UMass Boston

Directory

Employment

Civil Rights & Title IX

Map

Safety & Security

Transportation

Events



UMass System **Accessibility Statement** **Privacy & Terms**