MITnet Rules of Use

On this page:

Overview

MITnet, MIT's campus-wide computer network, connects the MIT community and our guests to thousands of workstations, servers, printers, mobile devices and electronic resources of every kind located on and off campus. Network connectivity has many advantages which you will discover as you explore MITnet, and the Internet beyond. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

This section summarizes the rules that apply to all users of MITnet. We expect you to follow all these rules, and we hope you will encourage others to follow them as well.

To report someone willfully violating the rules, send email to stopit@mit.edu. If you believe you are in danger, call the Campus Police *immediately* at x3-1212.

Summary

The listing below provides only summaries of the rules. For the full text of each rule, please see the following pages.

MITnet Rules of Use

Comply with Intended Use of the System

1. Don't violate the intended use of MITnet.

Assure Ethical Use of the System

2. Don't let anyone know your password(s).

3. Don't violate the privacy of other users.

4. Don't misuse the intellectual property of others.

5. Don't use MITnet to harass anyone in any way.

Assure Proper Use of System Resources

6. Don't misuse electronic communications and collaboration services.

7. No hubs/switches/routers allowed on MITnet.

MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsible, legal, and respectful of privacy. If you have questions or wish further information about any of the MITnet policies outlined below, send email to security@mit.edu.

All network users are expected to follow these rules. ***Violations of the rules can subject the offender to Institute disciplinary proceedings, loss of network privileges, and, in some cases, civil or criminal prosecution.***

Note: Laws that apply in "the real world" also apply in the "virtual" networked computer world (including MITnet). Laws about libel, harassment, privacy, copyright, stealing, threats, etc. are *not* suspended for computer users, but apply to all members of society whatever medium they happen to be using: face-to-face, phone, *or* computer. Furthermore, law-enforcement officials are more computer-savvy than ever, and violations of the law in "Cyberspace" are vigorously prosecuted.

Similarly, Institute policies (as described in MIT's Policies and Procedures, for example) also apply to MITnet users.

Complying With the Intended Use of the System

It is important that you understand the purpose of MITnet so that your use of the system is in compliance with that purpose.

1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:

- *Don't try to interfere with or alter the integrity of the system at large*, by doing any of the following:
  - permitting another individual to use your account
  - impersonating other individuals in communication (particularly via forged email, texts, instant messages and social media postings)
  - attempting to capture or crack passwords or encryption
  - destroying or altering data or programs belonging to other users
- *Don't try to restrict or deny access to the system by legitimate users.*
- *Don't use MITnet for private financial gain.* For example, users are *not* permitted to run a private business on MITnet. (Commercial activity *is* permitted, but *only* for business done on behalf of MIT or its organizations. Cf. Section 13.2.3 of MIT's Policies and Procedures: "MIT's computing and telecommunications facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization.")
- *Don't transmit threatening or harassing materials.* (Cf. Rule 5.)

Assuring Ethical Use of the System

Along with the many opportunities that MITnet provides for members of the MIT community to share information comes the responsibility to use the system in accordance with MIT standards of honesty and personal conduct. Those standards, outlined in Section 13.2 of MIT's Policies and Procedures, call for all members of the community to act in a responsible, professional way.

Appropriate use of MITnet resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

2. Don't let anyone know your password(s).

While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should *never* let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., IS&T staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password

can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one. And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, see Strong Passwords.

3. Don't violate the privacy of other users.

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections 11.2, 11.3, and 13.2 of MIT's Policies and Procedures). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section 11.1 of MIT's *Policies and Procedures* notes, "Invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- *Don't try to access the files or directories of another user without clear authorization from that user.* Typically, this authorization is signaled by the other user's setting file-access permissions to allow public or group reading of the files. If you are in doubt, ask the user.
- *Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.* These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.
- Unless you understand how to protect private information on a computer system, *don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves* (e.g., grades, address information, etc.)
- *Don't make any personal information about individuals publicly available without their permission.* This includes both text and number data about the person (biographical information, phone

numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.) For instance, it is *not* appropriate to include a picture of someone on a World Wide Web page without that person's permission. (Depending on the source of the information or image, there may also be copyright issues involved; cf. Rule 4).

- *Don't create any shared programs that secretly collect information about their users.* Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)
- *Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.*

4. Don't misuse the intellectual property of others.

MIT faculty, students, and staff produce and consume a vast amount of intellectual property, much of it in digital form, as part of our education and research missions. This includes materials covered by the patent, copyright, and trademark laws, as well as license or other contractual terms.

Members of the MIT community also avail themselves of a wide variety of entertainment content that is available on the Internet, most of which is protected by copyright or subject to other legal restrictions on use.

All users need to insure that their use of all these protected digital materials respects the rights of the owners.

Digital materials that may be covered by this rule, without limitation, are:

- Data
- E-books
- Games
- Journals and periodicals
- Logos
- Movies
- Music
- Photographs and other graphics
- Software
- Textbooks
- Television programs
- Other forms of video content

You should assume that all materials are subject to these legal protections, and may have some restrictions on use. Ease of access, downloading, sharing, etc., should not be interpreted as a license for use and re-distribution.

Of particular concern is the prevalence of peer-to-peer file sharing as a medium for the unauthorized exchange of copyrighted materials, including movies, music, games, and other software programs. As required by the Higher Education Opportunity Act, MIT has developed and implemented a written plan to effectively combat the unauthorized distribution of copyrighted materials by users of MIT's network. For more information, see Copyright at MIT.

5. Don't use MITnet to harass anyone in any way.

We define "harassment" according to MIT's Policies and Procedures (Section 9.5).

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to stopit@mit.edu. If you believe you are in danger, call the Campus Police *immediately* at x3-1212.

Assuring Proper Use of the System

MITnet's resources, as well as the resources MITnet gives you access to (e.g., computing facilities, email and calendaring services, instant messaging, wikis, the web), are powerful tools that provide maximum benefit to the entire MIT community when used reasonably and in manners consistent with the intended uses of those resources.

6. Don't misuse electronic communications and collaboration services.

MIT provides electronic communications and collaboration services to members of the MIT community. These services include, but are not limited to, electronic mail, mailing lists, instant messaging, message boards, websites, wikis, blogs, social networking sites, forums, collaborative spaces, Voice over IP (VoIP) and video services.

Some members of the MIT community access similar, or additional, 3rd party services on the Internet.

Users of all such services have a responsibility to use these services properly and to respect the rights of others in their use of these services, and in accordance with published terms of service.

Users may not use these services in violation of any applicable law.

All relevant MIT policies apply to the use of these services, but in particular:

- Any use that might contribute to the creation of a hostile academic or work environment is prohibited,
- Any commercial use not required for coursework, research or the conduct of MIT business is prohibited,
- Any non-incidental personal use such as advertisements, solicitations or promotions is prohibited [Note: some services exist on campus that have been designed for buying, selling and exchanging items within the MIT community, and those are allowed].

MIT Senior Leadership has authorized certain individuals to send electronic mail to large groups, e.g., all faculty, all employees, all undergraduates, Class of 2022, or to the entire MIT community. These lists are not open to posts from the community at large. Contact the owners of these lists for further information.

Users should understand a service's policies prior to use. Service operators and providers should, to the extent feasible, publish their terms of service.

Any content posted to a service that is inconsistent with these rules, as well as unsolicited mail from outside of MIT (e.g., spam), may be subject to automated interception, quarantine and disposal.

7. No hubs/switches/routers allowed on MITnet.

A hub is designed as anything that converts one UTP connector to many UTP connectors. A switch counts as a hub for MITNet purposes. Routers (cable/DSL routers,= "broadband routers", or anything else that does routing or NAT) are prohibited from MITnet as they interfere with the operation of the network.

RELATED PAGES AND HOW TO

Athena Rules of Use

Athena Computing Environment

MIT Kerberos Accounts

servicedesk@mit.edu | 617.253.1101
Accessibility

FOR FACULTY & STAFF

FOR STUDENTS

FOR VISITORS

FOR IS&T STAFF