**13.2 Policy on the Use of Information Technology Resources**

Information technology policies ensure that everyone's use of the Institute's information technology resources supports its educational, research, public service, and administrative mission in the best possible way. Effective support of the Institute's mission requires complying with relevant legal, contractual, professional, and policy obligations whenever information technology resources are used. Effective support also means that individuals not interfere with the appropriate uses of information technology resources by others.

This policy broadly covers all of the Institute’s information technology resources – hardware, software, and content; this includes but is not limited to electronic networks, systems, computers, devices, telephones, software, data, files, and all content residing in any of these (referred to as “IT resources”). This policy applies to all records of the Institute and to the information in those records, regardless of the form or the location.

**13.2.1 Privacy and Confidentiality of Institute Records**

All members of the MIT community are responsible for ensuring that their handling of information about individuals is consistent with the Institute's policy on privacy of personal information (see [Section 11.2 Use of Personal Information](http://web.mit.edu/policies/11/11.2.html)).  In addition, other Institute records (that is, records that do not contain personal information) must be handled with due regard for privacy and confidentiality concerns. (See [Section 13.2.2.2 Security of Information](http://web.mit.edu/policies/13/13.2.html#sub2) and [13.2.4 Privacy of Electronic Communications, Electronic Files, and Other Files](http://web.mit.edu/policies/13/13.2.html#sub4)).

**13.2.2 Information Preservation and Security**

**13.2.2.1 Preservation of Information**

MIT has an obligation to provide accurate, reliable information to authorized recipients and to preserve vital records (see [Section 13.3 Archival Policy](http://web.mit.edu/policies/13/13.3.html)). MIT is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and on the computing and networking resources that store, process, and transmit this information. Records created and maintained in electronic form are included in the Institute's definition of archival materials. In addition, upon direction from the Office of the General Counsel, records must sometimes be preserved for prescribed periods of time for litigation or other legal purposes.

**13.2.2.2 Security of Information**

Individuals who manage or use IT resources required by the Institute to carry out its mission must take reasonable steps to protect them from unauthorized modification, disclosure, and destruction.  Data and software are to be protected, regardless of the form, medium, or storage location of the information. The level of protection shall be commensurate with the risk of exposure and with the value of the information and of the IT resources.

Some information has additional legal protection, like certain medical information, education records (see Section [11.3 Privacy of Student Records](http://web.mit.edu/policies/11/11.3.html)), certain financial records, and specific categories of personal information covered in [MIT’s Written Information Security Program](http://web.mit.edu/infoprotect/wisp/).  As described in the Written Information Security Program, departments that regularly use specified categories of personal information should have written procedures on protecting that data, and should also implement specific procedures concerning how that data is destroyed when no longer needed.

**13.2.3 Responsible Use of IT Resources**

**13.2.3.1 Approved Use of IT Resources**

All members of the MIT community are obligated to use MIT’s IT resources in accordance with applicable laws, with Institute policies (including its policy against harassment, and its standards of honesty and personal conduct), and in ways that are responsible, ethical, and professional. Users of MIT’s network must also comply with the [MITnet Rules of Use](http://ist.mit.edu/network/rules).

The use of MIT's IT resources is restricted to Institute business and incidental personal use. Incidental personal use may not interfere with MIT work, nor may it result in additional direct cost to MIT.  MIT's computers and other IT resources must be used in a manner consistent with MIT’s status as a non-profit organization, and so, for example, cannot be used for the benefit of personal businesses or other organizations unless permitted by MIT policy (for example, permitted under [Section 4.5 Outside Professional Activities](http://web.mit.edu/policies/4/4.5.html)) or otherwise authorized.  Unauthorized access to and use of MIT’s IT resources violates this policy.

**13.2.3.2 Interference with IT Resources**

Members of the Institute community should not take unauthorized actions to interfere with, disrupt, or alter the integrity of MIT’s IT resources.  Efforts to restrict or deny access by legitimate users of the Institute's IT resources are unacceptable. Individuals should not use MIT facilities to interfere with or alter the integrity of any IT resources, irrespective of their location.

Destruction, alteration, or disclosure without authorization of data, programs, or other content  that belongs to others but that is accessed through MIT’s IT resources is also prohibited. MIT may block an individual or group’s access to its IT resources in order to protect its IT resources and the information contained in them.

**13.2.4 Privacy of Electronic Communications, Electronic Files, and Other Files**

As noted in [Section 13.2.2.2 Security of Information](http://web.mit.edu/policies/13/13.2.html#sub2), members of the MIT community should exercise caution to protect information (and particularly personal information) from unauthorized disclosure.  Particular caution should be used with electronic communications, because of the ease with which such communications can be distributed and due to concerns about unauthorized access.  Unauthorized interception of email and other electronic communications is prohibited by MIT policy and may also violate state and federal law.

For legitimate business reasons, representatives of the Institute may need to access electronic or other records (including paper files) without the consent of the individuals having custody of them; examples of these business reasons include access required by law, where the individual is unavailable due to illness, in the course of an investigation, or in cases of alleged misconduct.   Departments, labs, or centers may determine additional reasons for access, for example, due to sponsor requirements (as at Lincoln Laboratory).  Any member of the MIT community who accesses information from records maintained by another individual without the individual's consent must seek prior approval from the applicable [Senior Officer](http://web.mit.edu/orgchart/replist.html) or his or her designee for such access and related disclosure; the Senior Officer or designee may consult the Office of the General Counsel. This process applies to requests for access from an outside entity or from another office within MIT.

**13.2.5 Third-Party Products and Services**

**13.2.5.1 Restrictions on Use of Certain IT Resources from Outside Sources**

Special restrictions are often placed on the use of IT resources — such as hardware, software, databases, and documentation — acquired from outside sources. Use of such IT resources may be further restricted by patent law, as a trade secret, or by contract in the form of a license or other agreement. Members of the MIT community are required to abide by the restrictions imposed by law or by contract on IT Resources acquired for use at the Institute. Any individual who arranges for authorized distribution of information technology products and services from outside sources must advise the people having access to the products and services of all the associated usage restrictions.

**13.2.5.2 Copyright**

Unless it has been placed in the public domain, most third-party software is protected by copyright law and may be subject to restrictions on use, copying, and distribution.  More information on copyright can be found at [Section 13.5 Reproduction of Copyrighted Materials](http://web.mit.edu/policies/13/13.5.html).