CORNELL UNIVERSITY
POLICY LIBRARY

# Access to Information Technology Data and Monitoring Network Transmissions

POLICY 5.9

Volume: 5, Information Technology
Chapter: 9, Access to Information Technology Data and Monitoring Network Transmissions
Responsible Executive: Chief Information Officer and Vice President
Responsible Office: Information Technology Security/WCMC Privacy
Originally Issued: January 20, 2006
Last Updated: June 27, 2011

## POLICY STATEMENT

Information technology data will be disclosed only according to the procedures outlined in this policy.

Cornell University does not monitor the content of network traffic except for legal, policy, or contractual compliance; in the case of a health or safety emergency; or for the maintenance and technical security of the network.

The university reserves the right to restrict the use of its information technology resources and to remove or limit access to information technology resources.

## REASON FOR POLICY

The university maintains its network and computer systems in a manner that supports its missions in teaching, research, and outreach, while complying with legal, policy, and contractual obligations.

## ENTITIES AFFECTED BY THIS POLICY

– All units of the university

## WHO SHOULD READ THIS POLICY

– All members of the university community

## WEB SITE ADDRESS FOR THIS POLICY

– This policy: www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/itdata.cfm
– University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 5, Information Technology
Responsible Executive: Chief Information Officer and Vice President
Responsible Office: Information Technology Security/WCMC Privacy
Originally Issued: January 20, 2006
Last Updated: June 27, 2011

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## CONTENTS

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## RELATED RESOURCES

| University Policies and Documentation Applicable to All Units |
|---|
| University Policy 5.1, Responsible Use of Information Technology Resources |
| Educational and Implementation Resources on the CIT Web site |

| University Policies and Documentation Applicable to Ithaca Campus Units |
|---|
| University Policy 4.12, Data Stewardship and Custodianship |
| University Policy 4.13, Acceptance of Legal Papers |
| University Policy 5.5, Stewardship and Custodianship of Electronic Mail |

| External Documentation |
|---|
| Electronic Communications Privacy Act, 1986 |
| Federal Rules of Civil Procedure 16, 26, 33 and 34 |
| U.S. Patriot Act of 2001 |

POLICY 5.9

Access to Information Technology Data and Monitoring Network Transmissions

## CONTACTS, ITHACA CAMPUS UNITS

Direct any general questions about this policy to your college or unit's administrative office. Direct questions about specific issues to the following offices.

*Contacts, Ithaca Campus Units*

| Subject | Contact | Telephone | E-mail/Web Address |
|---|---|---|---|
| **Policy Interpretation** | IT Security Office | (607) 255-8421 | security@cornell.edu<br>www.it.cornell.edu/security/ |
| **Requests for Information Technology Data** | Chief Information Officer and Vice President | (607) 255-8054 | www.cit.cornell.edu/oit/ |

## CONTACTS, WEILL CORNELL CAMPUS UNITS

Direct any general questions about this policy to your college or unit's administrative office. Direct questions about specific issues to the following offices.

*Contacts, Weill Cornell Campus Units*

| Subject | Contact | Telephone | E-mail/Web Address |
|---|---|---|---|
| **Policy Clarification and Interpretation** | WCMC Privacy Officer | (212) 746-1121 | Frank Maurer: fmaurer@med.cornell.edu |
| **Reporting Security Violations** | Office of Academic Computing | | support@med.cornell.edu<br>*(monitored 24 hours a day)* |
| **Reporting Violations of Privacy Rules and Regulations, Including Loss or Theft of Confidential Data** | WCMC Privacy Officer | (212) 746-1121 | Frank Maurer: fmaurer@med.cornell.edu |

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## DEFINITIONS

These definitions apply to these terms as they are used in this policy.

| | |
|---|---|
| **Content** | User-generated information contained in applications or programs running on information technology systems, such as text in an e-mail or voice message, a telephone conversation, a spreadsheet, word document, etc. |
| **Information Technology (IT) Data** | Data produced by computer systems or by voice and data network devices, such as routers, switches, private branch exchanges (PBXs), and firewalls. Examples of computer system data include records of a user's logins and logouts, services used, and file names created or modified. Examples of network device data include visited Internet addresses, and sizes and types of files sent or received.<br>◆ **Note**: IT data does not include the content of any voice or data communications. |
| **Information Technology (IT) Resource** | The full set of information technology devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, and transmission of information. |
| **Legal Papers** | Documents issued by a court, officer of the court, attorney, government agency, or administrative agency requiring the university or any unit of the university to appear in court, provide testimony, documents, records, or property, or to take or refrain from taking some action. Examples of legal papers include subpoenas, court pleadings (summonses, complaints, court orders, interrogatories, notices of deposition, requests for production of documents, notices to admit, and all other forms of demands for disclosure), restraining orders, garnishments, and mechanics liens. |
| **Monitoring** | Automated or manual observation. |
| **Network** | Cornell University's system of interconnected IT components (e.g., switches, routers, optical fibers, and wires) used to support transmission of electronic data between attachable endpoints. |
| **Transmission** | An electronic signal, while it is moving from an origin to a destination point. |

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## RESPONSIBILITIES, ITHACA CAMPUS UNITS

| | |
|---|---|
| **Chief Information Officer and Vice President** | Accept and review requests for information technology (IT) data, and approve, if appropriate.<br>Notify IT Policy and Security directors of the outcome of the request for IT data. |
| **Information Technologies (IT) Policy Director** | Provide clarification on University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions. |
| **Network Administrators** | Disclose IT data only for the purposes of security, maintenance, or billing, or as approved by the Chief Information Officer and Vice President. |
| **Requestors of IT Data** | Request IT data from the Chief Information Officer and Vice President, as appropriate.<br>◆ **Note:** For requests for IT data from law enforcement, proceed as directed in University Policy 4.13, Acceptance of Legal Papers. |

## RESPONSIBILITIES, WEILL CORNELL CAMPUS UNITS

| | |
|---|---|
| **Information Technologies and Services Department (ITS)** | Receive and evaluate requests for access, review, and/or release of stored or transmitted electronic information.<br>Allow access, review, and/or release of stored or transmitted electronic information in accordance with this policy. |

Cornell Policy Library
Volume: 5, Information Technology
Responsible Executive: Chief Information Officer and Vice President
Responsible Office: Information Technology Security/WCMC Privacy
Originally Issued: January 20, 2006
Last Updated: June 27, 2011

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## PRINCIPLES

**General Provisions**

Cornell University owns, manages, and maintains its data and telecommunications services as a private network. Under certain conditions, for reasons of legal and policy compliance, contractual obligations, or for maintenance or security, the university will monitor its network transmissions for content and reserves the right to remove or limit access to information technology resources.

This policy enables the safeguarding of the privacy of the university's information technology data by establishing controls over access to such data, including limiting conditions under which that data may be disclosed.

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## PROCEDURES, ITHACA CAMPUS UNITS

**Access to Information Technology Data**

Under the authority of University Policy 4.12, Data Stewardship and Custodianship, the Chief Information Officer and Vice President is responsible to establish rules for such disclosure in a way that promotes collaboration among data stewards and other university officials in an environment of trust within the Cornell community.

◆ **Note:** In accordance with University Policy 4.12, this policy concerns only administrative data and does not apply to information technology (IT) data used for research purposes.

The Chief Information Officer and Vice President may approve disclosure of IT data only in the following limited circumstances:

1. When requested by the Office of University Counsel, a court order, or other entity with legal authority to do so
2. When requested by an appropriate university official, including, but not limited to, the Office of University Counsel, Division of Human Resources, or the Chief Information Officer and Vice President
3. When fulfilling the legal, regulatory, or other applicable duties of the college
4. When responding to an electronic or physical security issue or incident
5. In the event of a health or safety concern
6. To ensure the security, confidentiality, integrity, and availability of data stored or transmitted by WCMC information technology resources

◆ **Notes:**

1. Nothing in this policy is intended to prohibit or inhibit data custodians who handle IT data from performing their duties in the normal course of business.
2. The Chief Information Officer and Vice President has delegated to IT professionals the authority to disclose IT data for the purposes of security, maintenance, or billing.
3. Any data under this policy disclosed in response to reasonable requests to assist IT-related research will be anonymous.
4. For rules regarding the disclosure of institutional information stored on university-owned devices, please refer to University Policy 4.12, Data Stewardship and Custodianship.
5. For rules regarding the disclosure of electronic mail, see University Policy 5.5, Stewardship and Custodianship of Electronic Mail.

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## PROCEDURES, ITHACA CAMPUS UNITS, CONTINUED

**Requests for Information Technology Data**

All requests for IT data must be submitted to the Chief Information Officer and Vice President.

Requests must include all of the following:

1. Reason for the request, which must correspond to the disclosure rules provided by this policy
2. Who requests receipt of the data
3. Intended use of the received data

◆ **Note:** In the event of requests for IT data from law enforcement, University Policy 4.13, Acceptance of Legal Papers applies.

# POLICY 5.9

# Access to Information Technology Data and Monitoring Network Transmissions

## PROCEDURES, WEILL CORNELL CAMPUS UNITS

**Overview**

Weill Cornell Medical College (WCMC) provides computer, e-mail, network, Internet, and telephone access to faculty, staff, and students for the purpose of furthering the mission of education, research, and patient care and for conducting general college business. While incidental and occasional personal use of such systems is permissible, personal communications and data transmitted or stored on WCMC information technology resources are treated as business communications, and are subject to automated surveillance by security systems managed by the Information Technologies and Services Department (ITS). WCMC community members should not expect that personal communications will remain private and/or confidential. While the college permits generally unhindered use of its information technology resources, those who use WCMC information technology resources do not acquire, and should not expect, a right of privacy.

WCMC reserves the right to access, review, and release electronic information that is stored or transmitted using WCMC information technology resources. WCMC will initiate this access, review, or release only under one or more of the following circumstances:

1. When requested by the Office of University Counsel, a court order, or other entity with legal authority to do so
2. When requested by an appropriate WCMC official, including, but not limited to, the Office of University Counsel, Human Resources, the WCMC Privacy Officer, or the WCMC Security Officer
3. When fulfilling the legal, regulatory, or other applicable duties of the college
4. When responding to an electronic or physical security issue or incident
5. In the event of a health or safety concern
6. To ensure the security, confidentiality, integrity, and availability of data stored or transmitted by WCMC information technology resources

In cases where more stringent controls, such as state regulations for psychiatric data, maintain a higher standard for authorized access, review, or release of data, the more stringent control will always take precedent.

Whenever access, review, or release of WCMC data is necessary, care will be taken to treat the event with sensitivity and respect.

POLICY 5.9

Access to Information Technology Data and Monitoring Network Transmissions

# INDEX