CORNELL UNIVERSITY
POLICY LIBRARY

Responsible Use of Information Technology Resources

POLICY 5.1

Volume: 5, Information Technology
Chapter: 1, Responsible Use of Information Technology Resources
Responsible Executive: Chief Information Officer and Vice President
Responsible Offices: Information Technology Policy/WCM Privacy
Originally Issued: April 1994
Last Updated: July 19, 2018

POLICY STATEMENT

Cornell University requires people who use its information technology resources to do so in a responsible manner, abiding by all applicable laws, policies, and regulations.

REASON FOR POLICY

The university must uphold the tenets of academic freedom, while recognizing that protecting information technology and data requires community members to act responsibly when using these resources.

ENTITIES AFFECTED BY THIS POLICY

- All units of the university

WHO SHOULD READ THIS POLICY

- All members of the university community

WEB ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/policy/policies/responsible-use-information-technology-resources
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 5, Information Technologies
Responsible Executive: Chief Information Officer and Vice President
Responsible Offices: Information Technology Policy/ WCM Privacy
Originally Issued: April 1994
Last Updated: July 19, 2018

POLICY 5.1

Responsible Use of Information Technology Resources

CONTENTS

POLICY 5.1

Responsible Use of Information Technology Resources

RELATED RESOURCES

University Policies and Documentation Applicable to All Units of the University
University Policy 3.6, Financial Irregularities, Reporting and Investigation
University Policy 4.6, Standards of Ethical Conduct
University Policy 5.5, Stewardship and Custodianship of Electronic Mail
University Policy 5.6, Recording and Registration of Domain Names
University Policy 5.8, Authentication to Information Technology Resources
University Policy 5.9, Access to Information Technology Data and Monitoring Network Transmissions
University Policy 5.10, Information Security
University Policy 6.4, Prohibited Bias, Discrimination, Harassment, and Sexual and Related Misconduct
Educational and Implementation Resources on the IT website

University Policies and Documentation Applicable to Ithaca Campus Units
Campus Code of Conduct
University Policy 5.2, Mass Electronic Mailing
University Policy 5.3, Use of Escrowed Encryption Keys
University Policy 5.4.1, Security of Information Technology Resources
University Policy 5.4.2, Reporting Electronic Security Incidents
University Policy 5.7, Network Registry

University Policies and Documentation Applicable to Weill Cornell Campus Units
Weill Cornell Medicine Information Technologies Policies

POLICY 5.1

Responsible Use of Information Technology Resources

CONTACTS, ITHACA CAMPUS UNITS

Direct any general questions about this policy to your college or unit administrative office. If you have questions about specific issues, contact the following offices.

Contacts, Ithaca Campus Units

Subject	Contact	Telephone	E-mail/Web Address
Policy Clarification and Interpretation	IT Security Office	(607) 255-8421	security@cornell.edu
Campus Code of Conduct	Office of the Judicial Administrator	(607) 255-4680	judicialadministrator.cornell.edu
Commercial Use	Vice President and Chief Information Officer	(607) 255-7445	it.cornell.edu/office-cio
Criminal or Illegal Acts	Cornell University Police Department (CUPD)	911 - Emergencies (607) 255-1111 – Non-emergencies	www.cupolice.cornell.edu
Reporting Alleged Violations of Computer and Network Policies	IT Security Office	(607) 255-8421	abuse@cornell.edu
Reporting Alleged Copyright Infringement	IT Security Office	(607) 255-8421	copyright_abuse@cornell.edu
Reporting Alleged Harassment, Discrimination, or Bias Incidents, and Other Human Resources Issues	Local Human Resources Representative	Unit-specific	hr.cornell.edu/find-your-hr-representative
Reporting Real or Suspected Financial Irregularities	University Audit	(607) 255-9300	audit@cornell.edu audit.cornell.edu
	Cornell Hotline	(866) 293-3077	www.hotline.cornell.edu
Security Incidents	IT Security Office	(607) 255-8421	security@cornell.edu

POLICY 5.1

Responsible Use of Information Technology Resources

CONTACTS, WEILL CORNELL CAMPUS UNITS

Direct any general questions about this policy to your unit administrative office. If you have questions about specific issues, contact the following offices.

Contacts, Weill Cornell Campus Units

Subject	Contact	Telephone	E-mail/Web Address
Policy Clarification and Interpretation, Weill Cornell Medicine (WCM)	WCM Privacy Officer	(212) 746-1121	its-security-compliance@med.cornell.edu
Reporting Security Violations	Office of Academic Computing		support@med.cornell.edu *(monitored 24 hours a day)*
Reporting Violations of Privacy Rules and Regulations, Including Loss or Theft of Confidential Data	WCM Privacy Officer	(212) 746-1121	its-security-compliance@med.cornell.edu

POLICY 5.1

Responsible Use of Information Technology Resources

DEFINITIONS

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

Denial-of-Service Attack	An act initiated by a person or people using any electronic means to cause computer resources to become unavailable to its intended users for any length of time.
Information Technology Resources	The full set of information technology devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, accessing, and transmission of information.
Phishing	The process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
Sniffing	Employing a program that monitors and analyzes network traffic, to capture data being transmitted on a network.
Spamming	The process of sending unauthorized bulk messages.

POLICY 5.1

Responsible Use of Information Technology Resources

RESPONSIBILITIES, ITHACA CAMPUS UNITS

The following are major responsibilities each party has in connection with this policy.

Director of Information Technology Policy	Interpret this policy, and provide clarification and education.
User	Abide by all of Cornell's information technology (IT) policies, available at www.dfa.cornell.edu/policy-library.

RESPONSIBILITIES, WEILL CORNELL CAMPUS UNITS

The following are major responsibilities each party has in connection with this policy.

Department	Implement operational, physical, and technical controls for access, use, transmission, and disposal of Weill Cornell Medicine (WCM) data in compliance with all WCM privacy and security policies, procedures, and guidelines.
User	Use all WCM information technology (IT) resources and data in a manner that is legal, ethical, and consistent with the mission of education, research, and patient care. Abide by all of Cornell's applicable IT policies, available at www.dfa.cornell.edu/policy-library . Abide by all WCM IT policies, available at its.weill.cornell.edu/policies.
WCM Privacy Office	Interpret this policy, and provide clarification and education.

POLICY 5.1

Responsible Use of Information Technology Resources

PRINCIPLES

Overview

Each member of the Cornell University community is responsible for his or her actions, including the use of information technology (IT) resources. The university's missions, law, and policy define appropriate use of IT resources, rather than whatever a user is capable of doing with these resources.

This policy applies to anyone using Cornell's networks, including faculty and staff members, students, guests, and other members of the university community.

Special Workplace Considerations for Employees

In support of Cornell University's mission, employees are provided computing, networking, and information resources for use as business tools to support their efforts to meet their employment-related objectives. In keeping with our environment of freedom with responsibility, employees assume responsibility for their appropriate usage and are responsible for exercising good judgment regarding the reasonableness of personal use. Individuals are expected to be careful, honest, responsible, and civil in the use of computers and networks. Employees must respect the rights of others, respect the integrity of the systems and related resources, and use these resources in strict compliance with the law, university policies, and contractual obligations.

Using IT resources in the work environment in a manner that results in inappropriate conduct will be addressed as an employee performance issue, even if such conduct does not rise to the level of a university policy violation. Any use of university computers and networks by employees that is inappropriate to the workplace, or otherwise contributes to creating a harassing or uncomfortable workplace, or creates a legal risk, will subject the employee to counseling, formal disciplinary action and/or termination. Such performance concerns should be directed to the supervisor or the unit Human Resources representative.

POLICY 5.1

Responsible Use of Information Technology Resources

PROCEDURES, ITHACA CAMPUS UNITS

Introduction

This policy acts as an overarching document for all other Cornell information technology (IT) policies. These policies, along with other university policies, such as University Policy 4.6, Standards of Ethical Conduct, the Code of Academic Integrity, and the Campus Code of Conduct, establish a framework of expected behavior for users of the university's IT resources.

Violations

Federal, state, and local laws apply to the Internet and "cyberspace" just as they do to physical space. Using the university's IT resources in a way that violates the law constitutes a violation of university policy.

◆**Note**: Anyone with access to institutional information should abide by policy and good judgment regarding the use of that information on Cornell systems (for more information, see University Policy 4.12, Data Stewardship and Custodianship).

Listed below are examples of specific violations of university policy (this list is illustrative, not exhaustive).

- Breach of confidentiality rules
- Unauthorized access to IT resources
- Unauthorized use of IT resources
- Unauthorized commercial use of IT Resources
- Copyright infringement through peer-to-peer file sharing or other means
- Dissemination, hosting, or posting of child pornography, or obscene material
- Initiating a denial-of-service attack
- Releasing a virus, worm, or other malware
- Fraud
- Phishing
- Spamming

Reporting Violations

A legal or policy violation perpetrated using IT resources should be reported through the appropriate office for handling the alleged offense. For example (this list is not exhaustive):

- Report electronic security violations to the IT Security Office at (607) 255-6664 or security@cornell.edu.
- Report Campus Code of Conduct violations to the Judicial Administrator at (607) 255-4680.
- Report human resources policy violations and workplace issues to your local

PROCEDURES, ITHACA CAMPUS UNITS, continued

human resources representative. A list of unit human resources leadership is available at hr.cornell.edu/find-your-hr-representative.

- Report financial irregularities to the Cornell Hotline at www.hotline.cornell.edu, or call University Audit at (607) 255-9300.
- Report criminal violations to the Cornell University Police Department at (607) 255-1111.

When reporting these violations, include as much information as possible about the alleged perpetrator.

POLICY 5.1

Responsible Use of Information Technology Resources

PROCEDURES, WEILL CORNELL CAMPUS UNITS

Introduction

All members of the Weill Cornell Medicine (WCM) community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college, irrespective of the media on which the data reside and regardless of the format (e.g., electronic, paper, fax, CD, or other physical form).

Departments are responsible for implementing operational, physical, and technical controls for access, use, transmission, and disposal of WCM data in compliance with all WCM privacy and security policies, procedures, and guidelines, which is available at its.weill.cornell.edu/policies.

WCM expects community members, including, but not limited to, faculty and staff members and students, to use all WCM information technology (IT) resources and data in a manner that is legal, ethical, and consistent with the missions of education, research, and patient care.

Acceptable Use

Acceptable use of WCM IT resources and data includes, but is not limited to, the following:

1. Respecting system security mechanisms, and not taking measures designed to circumvent, ignore, or break these mechanisms
2. Showing consideration for the consumption and utilization of IT resources
3. Understanding and complying with policies, procedures, and guidelines concerning the security of the WCM IT and data
4. Assisting in the performance of remediation steps in the event of a detected vulnerability or compromise

Unacceptable Use

Unacceptable use of IT resources and data includes, but is not limited to, the following:

1. Unauthorized access to or unauthorized use of WCM IT resources
2. Use of resources in violation of any applicable law or regulation
3. Any activity designed to hinder another person's or institution's use of its own resources and data
4. Installation, distribution, or intentional use of malicious software (spyware, viruses, etc.)
5. Security breaches, intentional or otherwise, including negligent management of a server or workstation resulting in its unauthorized use or compromise
6. Sharing a password

POLICY 5.1

Responsible Use of Information Technology Resources

PROCEDURES, WEILL CORNELL CAMPUS UNITS, continued

Information Technologies and Services (ITS) Liaison

In order to facilitate compliance with this and other security policies, each department must appoint an Information Technologies and Services (ITS) liaison. ITS liaisons will be responsible for the following:

1. Understanding security policies and assisting in disseminating and evangelizing policies, procedures, and guidelines to the greater WCM community
2. Meeting with appropriate ITS staff members on a predetermined, regular basis to discuss security and other IT and data related issues
3. Providing documented authorization and de-authorization for data and IT resource access requests to ITS whenever appropriate
4. Assisting in performing remediation steps in the event of data loss, theft, compromise, detected vulnerability, etc.
5. Assisting in coordinating all activities related to electronic discovery (e-discovery)

Departments may choose to appoint multiple liaisons, when appropriate. Liaison appointments must be reviewed by the ITS Security Officer or his or her designee.

Reporting Violations

IT security questions or incidents should be reported to support@med.cornell.edu.

Violations of privacy rules and regulations, including loss or theft of confidential data (see WCM Policy 11.3 – Data Classification at its.weill.cornell.edu/policies/1103-data-classification for the full definition of confidential data) should be reported to the WCM Privacy Officer at (212) 746-1121.

POLICY 5.1

Responsible Use of Information Technology Resources

INDEX