CORNELL UNIVERSITY
POLICY LIBRARY

Security of Information Technology Resources

POLICY 5.4.1

Volume: 5, Information Technologies

Chapter: 4, Security

Responsible Executive: CIO and Vice President for Information Technologies

Responsible Office: Office of Information Technologies

Originally Issued: June 1, 2004

Last Full Review: December 13, 2017

Last Updated: December 13, 2017

POLICY STATEMENT

Cornell University expects all individuals using information technology resources to take appropriate measures to manage the security of those resources. In addition, the university establishes roles and responsibilities surrounding the procedures required for the security of these resources.

REASON FOR POLICY

The university must preserve its information technology resources, comply with applicable laws and regulations, and comply with other university or unit policy regarding protection and preservation of data. Given the distributed nature of information technologies and complexity of managing the security of information technology devices, the university wishes to set forth a foundation for the alignment of roles and responsibilities with regard to specific procedures.

ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based locations

☑ Cornell Tech campus

☐ Weill Cornell Medicine campuses

WHO SHOULD READ THIS POLICY

– All university community members

MOST CURRENT VERSION OF THIS POLICY

– https://www.dfa.cornell.edu/policy/policies/security-information-technology-resources

CONTENTS

RELATED RESOURCES

University Policies and Documents

University Policy 4.2, Transaction Authority and Payment Approval
University Policy 4.6, Standards of Ethical Conduct

University Policy 4.12, Data Stewardship and Custodianship

University Policy 5.1, Responsible Use of Information Technology Resources

University Policy 5.4.2, Reporting Electronic Security Incidents

University Policy 5.8. Authentication to Information Technology Resources

University Policy 6.11.3, Employee Discipline

Campus Code of Conduct

Code of Academic Integrity

Cornell University's Policy on Abuse of Computers and Network Systems

Data Privacy Incident Response Team (DPIRT)
Ithaca Information Security and Privacy Advisory Committee (ISPAC)
Securing your Computer

External Documentation

Financial Services Modernization Act

Health Insurance Portability Accountability Act (HIPAA)

New York State Penal Law Article 156 Offenses Involving Computers

CONTACTS – ITHACA-BASED LOCATIONS AND CORNELL TECH

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	Email/Web Address
Initial Contact for Questions	Local support provider	Unit-specific	
Policy Clarification	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Best Practices for Configuring and Securing IT Devices	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Computers and Network Systems	Chief Information Officer and Vice President for Information Technologies	(607) 255-8054	www.cio.cornell.edu
Legal Issues	Office of University Counsel	(607) 255-5125	counsel.cornell.edu
Security of Network Systems	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/

DEFINITIONS

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

Critical Security Notice	A memo that identifies operational or systemic information technology (IT) deficiencies or omissions that have the potential to pose risk to the university.
Data Privacy Incident Response Team (DPIRT)	A committee that determines and guides the institution's response to the loss or exposure of university data. It is composed of representatives of University Counsel, Risk Management and Insurance, University Communications, Audit, IT Security, IT Policy, and is chaired by the chief information officer.
Electronic Security Incident	Electronic activities that result in the damage to or misuse of the Cornell network or a device connected to it.
Information Technology (IT) Device	Any device involved with the processing, storage, or forwarding of information making use of the Cornell IT infrastructure or attached to the Cornell network. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, servers, and network devices such as routers or switches, and printers.
Information Technology (IT) Resources	The full set of IT devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, and transmission of information.
Local Support Provider	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device (e.g., system administrator or network administrator).
Operating Unit	An operating unit of the university, as defined in University Policy 4.2, Transaction Authority and Payment Approval.
Operating Unit Head	The dean or vice president with responsibility for an operating unit.
Software Patch	Software that is distributed to fix a specific set of problems or vulnerabilities in such things as computer programs or operating systems. A computer vendor will usually distribute a patch as a replacement for or an insertion in compiled code within computer operating systems or applications.
Unit Security Liaison	The person whom the operating unit head designates as the primary contact for the chief information security officer (CISO).
User	Any individual who uses an IT device, such as a computer.
Virus	A computer program that typically hides in the background and replicates itself from one IT device to another by attaching itself to existing programs or parts of the operating system. A virus often automatically spreads to other IT devices via the sharing of computer media, mail attachments, or website transfers.

RESPONSIBILITIES – ITHACA-BASED LOCATIONS AND CORNELL TECH

The major responsibilities each party has in connection with this policy are as follows:

Chief Information Security Officer (CISO)	Develop a comprehensive security program that includes risk assessment, best practices, education, and training. Identify, analyze, resolve, and report Cornell electronic security incidents. Assist or lead electronic security incident resolution for the university and individual units, and specifically in the Data Privacy Incident Response Team (DPIRT) process. Issue critical security notices to unit heads and security liaisons. Develop, implement, and support university-level security monitoring and analysis. Support and verify compliance with federal, state, and local legislation.
Ithaca Information Security and Privacy Advisory Committee (ISPAC)	Advise the chief information officer on information technology security, privacy, and related policy and compliance matters.
Local Support Provider	Maintain knowledge of IT devices under his or her control through identification and understanding of their usage. Follow safe security practices when administering IT devices under his or her control. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.
Operating Unit Head	Assume responsibility for the security of IT resources within the operating unit. Understand and accept the nature of risk for the operating unit that may be created as a result of the use of IT resources. Identify a unit security liaison. Implement unit security programs consistent with this policy.
Unit IT Manager	Provides operational oversight for operating unit's IT resources. Consults with CIT regarding campus IT issues.
Unit Security Liaison	Act as the unit point of contact with chief information security officer. Implement and document an information security program consistent with (a) requirements of this policy (for example, the implementation of risk assessment, best practices, education, and training), (b) the recommendations and guidelines supplied by the IT Security Office, and (c) the specific IT security needs of the operating unit. Act as the security coordinator for the local support providers (in operating units where the unit security liaison is not the local support provider). Implement unit procedures and protocols for the reporting of electronic security incidents in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

RESPONSIBILITIES – ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

	Work with the operating unit head, IT manager, director, and other relevant personnel to address critical security notices issued by the IT Security Office.
User	Comply with the current policies, requirements, guidelines, procedures, and protocols concerning the security of the university’s electronic networks and devices. Protect IT resources under his or her control with measures such as the responsible use of secure passwords, appropriately establishing an administrator password, and timely antivirus updates. Assist in the performance of remediation steps in the event of a detected vulnerability or compromise. Comply with directives of university officials, such as the security officer and his or her delegates, to maintain secure devices attached to the network regarding software patches and/or virus protection. Take note of circumstances in which he or she may assume the responsibilities of a local support provider, e.g., by attaching a personal computer to the Cornell network or working remotely from home. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

Cornell Policy Library
Volume: 5, Information Techologies
Responsible Executive: CIO and Vice President for Information Technologies
Responsible Office: Office of Information Technologies
Originally Issued: June 4, 2004
Last Updated: December 13, 2017

POLICY 5.4.1

Security of Information Technology Resources

PRINCIPLES

Introduction

In order to manage information technology (IT) security comprehensively, this policy serves six major purposes.

1. It establishes the principle that every IT device connected to the Cornell network and/or which processes Cornell data, must have at least one individual managing the security of that device.
2. It establishes that the operating unit head is responsible for the secure use of IT resources by the operating unit. This includes adoption of Cornell IT policy and, with guidance from the chief information security officer, adoption of other IT security practices as appropriate for the operating unit's mission.
3. It requires units to designate unit security liaisons (see the Obligations of the Unit Security Liaison segment of procedures).
4. It creates the following five categories of individuals, each with specific obligations regarding the security of IT devices:
   - User
   - Local support provider
   - Unit security liaison
   - Operating unit head
   - Chief information security officer.
5. It delineates specific responsibilities for each category of user.
6. It creates the foundation for the university's administrative approaches to IT security by aligning roles and responsibilities with technical procedures.

◆**Note:** All users of IT devices must follow the procedures outlined in the Obligations of Users section of the procedures.

◆**Note:** The focus of this policy is on the security of IT devices and resources, and not on specifics for the management of data or any particular class of data. For information concerning data, please consult University Policy 4.12, Data Stewardship and Custodianship, which provides the authority for and guidance towards the development of policy for the preservation and proper management of data in specific functional areas.

◆**Note:** As a foundational policy, this policy relies on other university policies; see Related Resources for more information about those policies.

PROCEDURES – ITHACA-BASED LOCATIONS AND CORNELL TECH

Obligations of the User

Any individual who uses an information technology (IT) device (see Definitions) is a user. Each of these devices may or may not have a local support provider assigned to it. Users have different obligations, based upon whether a local support provider has been assigned to a particular device.

Typically, university-owned IT devices located in campus workspaces have local support providers assigned to them. On the other hand, personally owned computers used to connect to the Cornell network from any location (home, off campus, residence hall, or other on-campus location) usually do not.

◆**Note:** If you cannot perform or do not understand any of the obligations assigned to users, contact the IT Service Desk, at itservicedesk@cornell.edu.

Obligations of a User Whose Device Does Have a Local Support Provider

1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the university’s electronic networks and devices (see Related Resources).
2. Comply with guidelines and practices established by the local support provider for the IT device.
3. Contact your local support provider whenever a questionable situation arises regarding the security of your IT device.
4. Report all electronic security incidents to your local support provider immediately, as detailed in University Policy 5.4.2, Reporting Electronic Security Incidents.

Obligations of a User Whose Device Does Not Have a Local Support Provider

(If you cannot perform or do not understand any of the obligations below, contact the IT Service Desk, at itservicedesk@cornell.edu)

1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the university’s electronic networks and IT devices (see Related Resources).
2. Update campus-wide security applications, including antivirus software and operating system updates, in a timely fashion.
3. Protect the resources under your control with the responsible use of secure passwords and by appropriately establishing an administrator password.
4. Assist in the performance of remediation steps in the event of a detected vulnerability or compromise.

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

5. Comply with directives of university officials, such as the chief information security officer (CISO), unit security liaison, or local support provider(s), to maintain secure devices attached to the network.
6. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

Obligations of a Local Support Provider

A local support provider is the individual with principal responsibility for the installation, configuration, and ongoing maintenance of an IT device (e.g., system administrator or network administrator). A local support provider seeking guidance or clarification should contact his or her unit security liaison or the CISO.

The local support provider is responsible to do the following:

1. Be knowledgeable and comply with the current policies, requirements, guidelines, procedures, and protocols concerning the security of the university's IT resources.
2. Follow appropriate best practices guidelines for configuring and securing IT devices. See https://it.cornell.edu/device-security.
3. Understand and document the specific configurations and characteristics of the IT devices he or she supports to be able to respond to emerging IT threats and to support security event mitigation efforts appropriately.
4. Understand and recommend the appropriate measures to provide security to the resources under his or her control, including, but not limited to the following:

- Physical security to protect resources such as keys, doors, and/or rooms maintained to the level of security commensurate with the value of the resources stored in those locations.
- Administrative security to protect resources such as:
    - Full implementation of the most current authentication and authorization technologies utilized by the architecture of the university network and/or its technology resources.
    - The most recently tested and approved software patches available.
    - The most contemporary and available security configurations.
    - The most contemporary and available virus protection.
    - Configuration of secure passwords on all IT devices (eliminating all default or administrative passwords).

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

5. Follow electronic security incident reporting requirements in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

◆**Note:** Local support providers should be mindful of potential responsibilities they may have as custodians of administrative data transmitted or stored on IT devices under their control. For further guidance, consult University Policy 4.12, Data Stewardship and Custodianship.

Obligations of the Unit Security Liaison

The unit security liaison is the person designated by the operating unit head as the primary contact for the CISO. For further guidance or clarification, contact the CISO.

The unit security liaison is responsible to do the following:

1. Act as the operating unit point of contact with the CISO.
2. Implement and document an information security program consistent with the requirements of this policy (for example, the implementation of security assessment, best practices, education and training), requirements and guidelines set forth by the IT Security Office, and consistent with university guidelines and practices and in keeping with the specific IT security needs of the operating unit. This will include the following:
    a. Develop a written information security plan in accord with templates, guidance, and recommendations given by the IT Security Office. Update this plan no less frequently than annually.
    b. Identify the IT resources under his or her control.
    c. Oversee compliance with all IT security regulations under federal, state, and local law.
    d. Provide proper information and documentation about those resources.
    e. Participate in and support security risk assessments of his or her IT resources, including the following:
        - The degree of sensitivity or importance of the data transmitted or stored on those resources.
        - The criticality of its connection to the network and a continuity plan in the event that it must be disconnected or blocked for security reasons.
        - The vulnerability of a particular resource to be used for illegal or destructive acts.

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

- The vulnerability of a particular resource to be compromised.
- The plan to be followed in the event of disaster for recovery.
- The measures routinely taken to ensure security for each device.

3. Act as the security coordinator for the local support provider(s) within the operating unit (in operating units where the unit security liaison is not the local support provider), including the following:
   a. Developing intermediate and harmonizing processes between university and unit policy and procedure.
   b. Assisting the IT Security Office in the investigation of security issues and incidents, and, in the case of a loss or breach of institutional data and information, representing the unit in the Data Privacy Incident Response Team (DPIRT) process. For more information, see Related Resources.
   c. Disseminating information and communications about security policy, procedures, and other information from the IT Security Office to users within the unit.
4. Implement unit procedures and protocols for the reporting of electronic security incidents in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.
5. Work with the operating unit head, the unit IT manager, director and/or other relevant personnel to address critical security notices issued by the CISO or his or her staff.

◆**Note:** The unit security liaison may want to take specific measures toward the protection of data stored or transmitted on the IT devices under his or her management and/or be mindful of any potential responsibilities as custodians of administrative data. Please consult with University Policy 4.12, Data Stewardship and Custodianship, for guidance.

Obligations of the Operating Unit Head

Operating unit heads (i.e., vice presidents or deans) have overall, local responsibility for the security of IT resources under their control. For further guidance, contact your unit security liaison or the CISO.

The operating unit head's oversight responsibilities in relation to security IT resources include, but are not limited to, the following:

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

1. Identify a unit security liaison to the CISO, who may in some cases also be the local support provider (depending upon the size of the operating unit and discretion of the unit head).
2. Ensure that, through the unit security liaison, a security program is implemented for the operating unit consistent with requirements of this policy (for example, the implementation of security assessment, best practices, education and training), consistent with university guidelines and practices and in keeping with the specific IT security needs of the operating unit.
3. Provide administrative control over continuity of support over all the IT devices in the operating unit such that, for example, a change in employment of an individual local support provider does not result in the abandonment of responsibility over IT devices attached to the network.
4. Oversee the creation and implementation of procedures for the reporting of electronic security incidents in accordance with University Policy 5.4.2, Reporting Electronic Security Incidents.

◆**Note:** Operating unit heads may want to take specific measures toward the protection of data stored or transmitted on the IT devices under their management. Please consult with University Policy 4.12, Data Stewardship and Custodianship, for guidance.

Limits of Operating Unit Head Delegation of Responsibility

Delegation is limited to:

- Direct reports, and/or
- A signed service-level agreement (SLA) with CIT, and/or
- A signed SLA with an external IT operations and security agency approved by the Office of the Vice President for Information Technologies.

Note: Delegation does not remove Operating Unit Head’s responsibility for the effective oversight and security of the operating unit’s IT resources.

Note: All SLAs must be signed by the operating unit head and the CIO and vice president for information technologies.

◆**Note:** All delegations of responsibilities must be reported to and recorded by the IT Security Office.

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

Obligations of the Chief Information Security Officer (CISO)

The CISO is the university officer with the authority to coordinate campus IT security. The following are obligations of the CISO:

1. Develop a comprehensive security program that includes risk assessment, best practices, education, and training.
2. Strive for proper identification, analysis, resolution, and reporting of Cornell electronic security incidents; assist or lead electronic security incident resolution for the university and individual units, specifically in the DPIRT process.
3. Issue critical security notices (risk notifications) to unit heads and security liaisons.
4. Develop, implement, and support university-level security monitoring and analysis.
5. Support and verify compliance with federal, state, and local legislation.
6. Regularly convene and lead ISPAC (see Related Resources).

Violations

Legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with it. Although some rules are built into the system itself, these restrictions cannot limit completely what an individual can do or can see. In any event, each member of the community is responsible for his or her actions, whether or not rules are built in, and whether or not they can be circumvented.

It is an explicit violation of this policy to do any of the following:

1. Knowingly or intentionally maintain insecure passwords on IT devices attached to the network (e.g., absence of administrative password, password written and stored in insecure location, shared passwords, etc.).
2. Knowingly or intentionally attach misconfigured IT devices to the network.
3. Knowingly or intentionally compromise an IT device attached to the network or intentionally use an application or computing system with a known compromise.
4. Knowingly or intentionally, (or negligently after receiving notice from an IT officer or professional), transmit any computer virus or other form of malicious software.
5. Knowingly or intentionally access or exploit resources for which you do not have authorization.

PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, continued

6. Knowingly or intentionally perform network or system scans on resources not authorized by the IT Security Office, unit head, unit security liaison, or local support provider.

Enforcement

Suspected violations will be investigated by the appropriate office, and disciplinary actions may be taken in accordance with the Campus Code of Conduct, applicable regulations, or other university policy.

Reporting Suspected Violations

All violations of this policy must be reported to the CISO. The CISO will refer these cases for disciplinary action to the following officers:

- If the alleged violator is a student, the judicial administrator
- If the alleged violator is a non-academic employee, the Office of Human Resources, Workforce Policy and Labor Relations
- If the alleged violator is an academic employee, the associated dean of the college, director of the library, or director of the research center
- Non-compliance by unit head, the CIO.

INDEX