CORNELL UNIVERSITY
POLICY LIBRARY

POLICY 5.10

Volume: 5, Information Technologies

Chapter: 10, Information Security

Responsible Executive: Vice President for Information Technology and Chief Information Officer; Chief Information Officer, Weill Cornell Medicine

Responsible Office: IT Security Office; Weill Cornell Medicine Privacy Office

Originally Issued: July 20, 2010

Last Updated: July 24, 2020

# Information Security

## POLICY STATEMENT

Cornell University expects all data stewards and custodians who have access to and responsibilities for university data to manage it as set forth in this policy. This is in accordance with the rules regarding collection, storage, disclosure, access, processing, destruction, and classification of information and minimum privacy and security standards.

## REASON FOR POLICY

Cornell must maintain and protect its informational assets and comply with applicable international, federal, and state legislation.

## ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based locations

☑ Cornell Tech campus

☑ Weill Cornell Medicine campuses, which will administer and implement the policy under separate procedures.

## WHO SHOULD READ THIS POLICY

– All stewards and custodians of university data

## MOST CURRENT VERSION OF THIS POLICY

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

## CONTENTS

# RELATED RESOURCES

**University Policies and Information Applicable to All Units of the University**

University Policy 3.17, Accepting Credit Cards to Conduct University Business

University Policy 4.7, Retention of University Records

University Policy 5.4.2, Reporting Electronic Security Incidents

University Policy 5.8, Authentication to Information Technology Resources

CIT Encryption Guidelines

Security Essentials for IT Professionals Articles (Data Hygiene)

**University Policies and Information Applicable to Only Ithaca-Based Locations and Cornell Tech**

University Policy 4.12, Data Stewardship and Custodianship

University Policy 5.11, Administrative Data Store Registry

Cornell University Privacy Office

Cornell University Registrar - FERPA

**University Policies and Information Applicable to Only Weill Cornell Medicine Campuses**

Weill Cornell Medicine Information Technologies & Services Policies

**External Documentation**

Family Education Rights and Privacy Act (FERPA)

Federal Policy for the Protection of Human Subjects ('Common Rule')

Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq.

General Data Protection Regulation (GDPR, 2016/679) (English PDF Version)

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

New York State Information Breach and Notification Act (Section 899-aa)

NIST 800 Series

Title 45 – Public Welfare Department of Health and Human Services Part 46, Protection of Human Subjects

CIS Top 20 Critical Security Controls

Payment Card Industry Data Security Standards (PCI-DSS)

## University Forms and Systems

***Ithaca-Based Locations***

Certified Desktop

Cornell Secure File Transfer - Use to transfer files securely to other individuals. Files are encrypted during transport.

Cornell Two-Step Login

Secure Password Management

Security Exception Form

Vulnerability Management

# CONTACTS

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:

*Ithaca-Based Locations and Cornell Tech*

| Subject | Contact | Telephone | Email/Web Address |
|---|---|---|---|
| Policy Clarification and Interpretation | Chief Information Security Officer | (607) 255-4654 | it.cornell.edu/security<br>security-services@cornell.edu |

*Weill Cornell Medicine Campuses*

| Subject | Contact | Telephone | Email/Web Address |
|---|---|---|---|
| ITS Security | Chief Information Security Officer | (646) 962-2768 | its-security@med.cornell.edu |

# DEFINITIONS

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

| | |
|---|---|
| **Application** | Also referred to as *application program* or *application software*. A computer software package that performs a specific function directly for an end user or, in some cases, for another application. |
| **Data Steward** | The identified vice president, vice provost, or committee responsible for data types as defined in University Policy 4.12, Data Stewardship and Custodianship. |
| **Endpoint** | A laptop, desktop, or virtual desktop used to conduct university business. Tablets that run Microsoft Windows are considered endpoints. |
| **External Storage Media** | A USB drive, external hard drive, CD, or DVD. |
| **Individual Custodian** | An individual or contracted third party who possesses or has access to university data, regardless of form. |
| **Information Security and Privacy Advisory Committee (ISPAC)** | A focused steering committee for advising the chief information officer on information technology security, privacy, and related policy and compliance matters. |
| **Legitimate Interest** | A requirement for access to and processing of university data to perform one’s authorized duties effectively and efficiently. |
| **Mobile Device** | A device used to conduct university business, including a smartphone, cellphone, or tablet. |
| **Network** | Any of Cornell’s physical Ethernet or wireless networks, or Infrastructure as a Service (IaaS) providers contracted for university business. |
| **Server** | Any system that hosts applications, data, or services for consumption. |
| **Specialized Device** | A piece of electronic equipment that might use a non-traditional computing platform or that is used on a network, such as a network-capable copier, printer, or fax machine; supervisory control and data acquisition system (SCADA); or a network-attached instrumentation, internet of things (IoT) device, or other control system. |
| **University Data** | Data steward-regulated data, in any form, stored on or off campus, locally generated or acquired from an external service. |
| **Unit** | A college department, program, research center, business service center, office, or other operating unit. |
| **Unit Head** | The operating unit head, dean, or vice president with responsibility for an operating unit. |

# RESPONSIBILITIES—ITHACA-BASED LOCATIONS AND CORNELL TECH

The major responsibilities each party has regarding this policy are as follows:

| | |
|---|---|
| **Data Steward** | Define appropriate use of assigned data types.<br>Understand all legislation that regulates data class use.<br>Work in concert with the vice president for information technologies to define baseline security rules and/or policies for those data sets. |
| **Individual Custodian** | Access and/or release university data only as allowed by university policy and as authorized by the operating unit.<br>Access, use, and disclose university data responsibly.<br>Recognize the consequences of improper custodianship of university data.. |
| **Information Security and Privacy Advisory Committee (ISPAC)** | Advise the chief information officer on information technology security, privacy, and related policy and compliance matters.<br>Assure that information security and privacy risk management efforts are aligned with regulatory requirements, system availability and integrity requirements, and Cornell's overall values and mission. |
| **IT Security Office** | In consultation with the IT Security Council, the IT Service Group Directors, and other stakeholders, determine technical procedures related to this policy and review them, at a minimum, annually.<br>Review and approve unit-level exceptions to this policy, as appropriate.<br>Maintain overview responsibility for implementation of this policy.<br>Educate the university community on this policy.<br>Monitor technological developments, changes in the law, user behavior, and the market, and update this policy, as appropriate. |
| **IT Service Groups (ITSG)** | Provide customized services to colleges and units, as well as some infrastructure in instances where there is a need unique to the service group. |
| **Privacy Office** | Advise data stewards, unit heads, and the IT Security Office on data classification and data protection measures required by applicable international, federal, and state legislation |
| **Unit Head** | Assume responsibility for policy compliance for the university data under the unit head's control.<br>Deploy procedures to comply with the data steward's rules for disclosing, categorizing, and authorizing access to university data.<br>Deploy procedures for meeting minimum standards for university data security according to information classification.<br>Conduct annual risk assessments of privacy practices and security standards.<br>Document how high-risk university data flows into and out of the local business unit and local applications. |
| **Unit Security Liaison** | Receive and address requests for exceptions to security requirements.<br>Maintain a current list of exceptions to security requirements.<br>Review annually all exceptions to baseline IT security requirements. |

Cornell Policy Library
Volume: 5, Information Technologies
Chapter: 10, Information Security
Responsible Executive: Vice President for Information Technology and Chief Information Officer; Chief Information Officer, Weill Cornell Medicine
Responsible Office: IT Security Office; Weill Cornell Medicine Privacy Office

# POLICY 5.10

# Information Security

Originally Issued: July 20, 2010
Last Updated: July 24, 2020

## PRINCIPLES

### Overview

Privacy practices and security standards serve to preserve and protect university data. This policy incorporates a set of requirements for protecting the university’s resources as well as safeguarding university data. These procedures set out the appropriate security standards for information at Ithaca-based locations, Cornell Tech, and Weill Cornell Medicine.

The integration of information technologies in virtually every aspect of transmission and storage of university data requires responsible administrative, technical, and physical security practices and standards. The focus on these procedures falls mainly on the administrative and technical aspects of privacy and security practices. All stewards and custodians of university data are responsible for adhering to the procedures that follow.

# PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH

## Introduction

To safeguard the university's information and information technology (IT) resources, the IT Security Office requires the following practices. These requirements apply to any system, whether contracted, cloud-hosted, or in a university facility, that is used to conduct university business.

These requirements, as detailed throughout this policy, reflect an approach referred to as "layered defense" or "defense-in-depth." This approach entails defenses on multiple levels—personnel, network, system, application, information—so that if the integrity of one is weakened, another may still be able to provide sufficient protection. It is the sum of all these measures, and not reliance on any particular aspect of security, that moves the university toward a more secure IT environment.

The unit head is responsible for assessing, at least annually, the local infrastructure and environment against this policy. This assessment aids in development of the unit Written Information Security Plan (WISP).

## Classification of University Data

High Risk

High-risk university data is information that has been determined by data stewards to require the highest level of privacy and security controls. Specifically, any information that contains any of the following data elements, when appearing in conjunction with an individual's legal name or other identifier (for example, email address), is considered to be high-risk university data:

- Social Security number
- Credit or debit card number
- Driver's license (or non-driver identification) number
- Bank account number
- Visa or passport number
- Protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA)
- Personal financial information subject to the Gramm-Leach-Bliley Act (GLBA)

◆**Note:** Copies you store of your own personal information do not fall under the requirements for safeguarding high-risk university data.

Consult with the IT Security Office or policy owner for clarification.

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

Moderate Risk

Moderate-risk university data is any information used in the conduct of university business, unless categorized as high-risk or low-risk university data. This includes, but is not limited to, protected student information as defined in the Family Educational Rights and Privacy Act (FERPA).

◆ **Note:** The majority of university data falls into the moderate risk category.

Low Risk

Low-risk university data is any information that the university has made available or published for the explicit use of the general public.

While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent its unauthorized modification or destruction.

### Exceptions

The following exception process must be followed for all endpoints, servers, mobile devices, specialized devices, and applications or other IT resources that are not able to meet the security requirements outlined by this policy:

IT resources that cannot meet the requirements contained within this policy must be identified to the appropriate unit security liaison, who will submit a request for a security exception by filling out a Security Exception Form (see the Related Resources section of this policy).

All IT exception requests must provide appropriate risk mitigation strategies and must be renewed annually. The IT Security Office will maintain the central list of exceptions, both granted and denied.

### Baseline Security Requirements

Data Hygiene

- Ensure that systems designed to host low-risk data do not process, transmit, or store high-risk university data.
- Remove high-risk university data when no longer needed for an operational reason.
- Dispose of data securely when no longer needed or required by University Policy 4.7, Retention of University Records.

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

- Mask or redact high-risk university data on development or test systems.

Encryption

- Escrow encrypted data keys used as part of university operations to allow successful recovery during business continuity and disaster recovery procedures.
- Encrypt, with proof, all portable media and/or external storage media containing high-risk university data. Examples of proof are an email, spreadsheet, picture, etc.
- Encrypt network transmission of high-risk university data.
- Store in an encrypted format any password for accounts with access to high-risk university data.

Authentication and Authorization

- Ensure that access to Cornell resources requires unique accounts, where technically feasible, to allow for auditability.
- Configure any account regularly used for operations for least privilege. Consistent or regular use of any account with administrative privileges is inappropriate.
- Ensure that all accounts have strong passwords, at least equivalent to the strength required for NetID passwords.
- Protect all shared file access by authorization and authentication.
- Encrypt electronic distribution of passwords.
- Change any passwords with default values set by the vendor.

◆ **Note:** For more information, see University Policy 5.8, Authentication to Information Technology Resources.

### Network Security Baseline Requirements

Implement network access controls, firewalls, or equivalent operations on any university network that transmits high-risk or moderate-risk university data. A default-deny strategy that prohibits unnecessary inbound, internal, and external connections and that strictly limits access to the systems with high-risk university data is required. Host firewalls and similar measures can be used to supplement network access control list (ACL)/ firewall rules.

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

Run a vulnerability scanning tool, at least every six months, on all unit subnets and remediate high-risk vulnerabilities as quickly as the environment allows, but not later than 30 days after such vulnerabilities are found.

Use encrypted communications for any system holding or accessing high-risk university data. Examples include, but are not limited to, eduroam, secure shell (SSH) / SSH file transfer protocol (SFTP), transport layer security (TLS), https, and/or virtual private network (VPN). Encrypting data prior to transmission, that is, batch encryption or file-level encryption, is considered sufficient to meet this requirement, provided that the authentication or other access control mechanism meets the complexity, individual identity, and encryption requirements elsewhere in this section.

Fully document the list of services, protocols, and systems permitted access into such subnets.

◆ **Note:** Where off-campus connectivity is not needed, put systems into a non-routable network (10-Space).

### Endpoints

Determine data classification and follow the minimum-security requirements in the table below to secure endpoints. For example, an endpoint storing moderate-risk university data but used to access a high-risk application is designated as high risk.

◆ **Note:** An endpoint is defined as any laptop, desktop, or virtual desktop used to conduct university business.

| Subject | Requirements | Low Risk | Moderate Risk | High Risk |
|---|---|---|---|---|
| Patching | Apply all security patches within 30 days of publish.Update or decommission endpoints prior to the vendor-defined operating system end of life. Maintain MacOS within the three most recent releases. | X | X | X |
| Malware Protection | Deploy university-approved malware protection and review and remediate alerts. | X | X | X |
| Operating System Hardening | Enable screen or console lock after 30 minutes of inactivity and enable local firewalls for traffic restriction. | X | X | X |

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

| | | | | |
|---|---|---|---|---|
| Inventory | At the unit level, maintain an inventory with records updated at least quarterly. Inventory should denote systems with high-risk data. | **X** | **X** | **X** |
| Confidential Data Discovery | Run confidential data discovery tools at least monthly for endpoints that store or process high-risk data, and at least every six months for all other systems. | **X** | **X** | **X** |
| Encryption | Apply whole-disk encryption for all endpoints, including personally owned devices, that access university data. | | **X** | **X** |
| Backups | Back up user data at least once per week. | | **X** | **X** |
| Regulated Data Security Controls | Implement PCI DSS, HIPAA, FISMA, GLBA, GDPR, or export controls as applicable. | | **X** | **X** |
| Configuration Management | Use configuration management controlled by Certified Desktop. | | | **X** |
| Logging | Log, at minimum, system, security, and application-specific logs. Logs must be retained for a minimum of 180 days and be immediately available for analysis. | | | **X** |

### Mobile Devices

Determine data classification and follow the minimum-security requirements in the table below to secure  mobile devices. For example, a mobile device storing moderate-risk university data but used to access a high-risk application is designated as high risk.

◆ **Note:** Mobile devices include smartphones, cellphones, or tablets used to conduct university business. Tablets that run Microsoft Windows are considered endpoints.

It is recommended that mobile devices have the most recent vendor supplied patches.

| **Subject** | **Requirements** | **Low Risk** | **Moderate Risk** | **High Risk** |
|---|---|---|---|---|
| Credentials and Access Control | Implement, at minimum, a six-digit passcode or a biometric control. | **X** | **X** | **X** |
| Device Lockout | Enable device locking after a period of inactivity not more than two minutes, and require a passcode or a biometric control to unlock. | **X** | **X** | **X** |

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

| | | | | |
|---|---|---|---|---|
| Encryption | Encrypt the device or the data in question.<br>Note: For most modern mobile devices, locking the device with a passcode or biometric control encrypts the device. If encryption is not supported, the device is prohibited from storing university data. | | X | X |

### Servers

Determine data classification and follow the minimum-security requirements in the table below to secure servers. For example, a server storing moderate-risk university data but used to access a high-risk application is designated as high risk.

◆ **Note:** A server is defined as any system that hosts applications, data, or services for consumption, including servers hosted in the cloud.

| Subject | Requirements | Low Risk | Moderate Risk | High Risk |
|---|---|---|---|---|
| Patching | Based on National Vulnerability Database (NVD) ratings or on vendor recommendation, apply high-severity security patches within 14 days of publish and all other security patches within 90 days. Update or decommission servers prior to the vendor-defined operating systems end of life. | X | X | X |
| Vulnerability Management | Perform a vulnerability scan at least monthly. Remediate critical and high vulnerabilities within 14 days and all other vulnerabilities within 90 days. | X | X | X |
| Inventory | At the unit level, maintain an inventory with records updated at least quarterly. Inventory should denote systems with high-risk data. Refer to University Policy 5.11, Administrative Data Store Registry, where appropriate. | X | X | X |
| Firewall | Enable host-based firewalls in default deny mode and permit the minimum necessary services. | X | X | X |
| Credentials and Access Control | Review existing accounts and privileges quarterly, and leverage the principle of least privilege. | X | X | X |

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

| | | | | |
|---|---|---|---|---|
| Logging | Log, at minimum, system, security, and application-specific logs. Logs must be retained for a minimum of 180 days and be immediately available for analysis. | X | X | X |
| Malware Protection | Deploy university-approved malware protection and review and remediate alerts. | | X | X |
| Regulated Data Security Controls | Implement PCI DSS, HIPAA, FISMA, GLBA, GDPR, or export controls as applicable. | | | X |
| Intrusion Detection | Deploy enhanced system protection, such as application whitelisting or endpoint detection and response (EDR). | | | X |
| Physical Protection | Place on-premise system hardware in a CIT data center. | | | X |
| Multi-factor Authentication | Require multi-factor authentication for access to high-risk data. Where direct access to confidential data, for example through file shares or specialized applications, cannot be secured with multi-factor authentication, access must be restricted to a multi-factor bastion host or multi-factor virtual private network (VPN). | | | X |
| Confidential Data Discovery | Run confidential data discovery tools at least annually. Securely delete discovered high-risk data or move it to a system designed to host high-risk data. | X | X | |

### Applications

Determine data classification and follow the minimum-security requirements in the table below to secure applications. For example, an application storing moderate-risk university data but used to access a high-risk application is designated as high risk.

◆ **Note:** A server is defined as any system that hosts applications, data, or services for consumption, including servers hosted in the cloud.

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

| Subject | Requirements | Low Risk | Moderate Risk | High Risk |
|---|---|---|---|---|
| Patching | Based on National Vulnerability Database (NVD) ratings or on vendor recommendation, apply high-severity security patches within 14 days of publish and all other security patches within 90 days. Update or decommission servers prior to the vendor-defined operating systems end of life. | X | X | X |
| Vulnerability Management | Perform scans at initial rollout and after major changes, including upgrades. All applications developed for university use must be free of OWASP Top 10 vulnerabilities that are reported at or above “high” severity. | X | X | X |
| Inventory | Maintain an inventory of applications with their associated data classifications. Review and update records quarterly. Refer to University Policy 5.11, Administrative Data Store Registry, where appropriate. | X | X | X |
| Credentials and Access Control | Review existing accounts and privileges quarterly. Enforce password complexity. Shared accounts are prohibited, except where it is not technically possible to provision individual accounts.<br>**Recommendation:** Federated logins with NetID credentials are preferred. | X | X | X |
| Firewall | Disable all network services, including specific application features that are not needed for the system to fulfill its function. | X | X | X |
| Logging | Logs must be retained for a minimum of 180 days and be immediately available for analysis. |  | X | X |
| Secure Software Development | Include security and privacy as a design requirement. Review all code and correct identified security flaws prior to deployment. Code repositories are required, provided authentication, high- or medium-risk data is not stored in public repositories. |  | X | X |

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

| | | | | |
|---|---|---|---|---|
| Backups | Back up application data at least weekly. Encrypt backup data in transit and at rest. | | X | X |
| Regulated Data Security Controls | Implement PCI DSS, HIPAA, FISMA, GLBA, GDPR, or export controls, as applicable. | | | X |
| Multi-factor Authentication | Require multi-factor authentication for access to high-risk data. Where direct access to confidential data, for example through file shares or specialized applications, cannot be secured with multi-factor authentication, access must be restricted to a multi-factor bastion host or multi-factor virtual private network (VPN). | | | X |

### Security of Paper Documents

Anyone handling high-risk university data in hard copy should take all appropriate measures to secure it physically, which includes, but is not limited to, maintaining it while stored in a locked office or cabinet and, during use, under close personal supervision. The measures outlined below are mandatory for paper documents containing high-risk university data.

Requirements

- Documents containing high-risk university data must locked in a drawer, filing cabinet, or a hard-wall, private, or shared office, such that they are accessible only to authorized personnel.
- Documents containing high-risk university data must never be left unattended in a public area.
- When no longer needed for daily operations, documents containing high-risk university data must be destroyed or moved to a secure archive facility. Please refer to University Policy 4.7, Retention of University Records, for more information.
- When documents containing high-risk university data are sent via third-party courier off-campus, a signed receipt of delivery is required.
- When documents containing high-risk university data are sent via campus mail, the envelope must be sealed and marked “Confidential.”

## PROCEDURES, ITHACA-BASED LOCATIONS AND CORNELL TECH, CONTINUED

- When documents containing high-risk university data need to be destroyed, a secure disposal service or a crosscut shredder must be used.