CORNELL UNIVERSITY
POLICY LIBRARY

POLICY 5.10

Volume: 5, Information Technologies
Chapter: 10, Information Security
Responsible Executive: Chief Information Officer and Vice President/Chief Information Officer, WCM
Responsible Office: IT Security Office/WCM Privacy Office
Issued as Policy Statement and Interim Procedures: January 6, 2009
Final Issuance: July 20, 2010
Last updated: June 25, 2018

Information Security

POLICY STATEMENT

Cornell University expects all institutional information stewards and custodians who have access to and responsibilities for institutional information to manage it according to the rules regarding storage, disclosure, access, classification of information and minimum privacy and security standards as set forth in this policy.

REASON FOR POLICY

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

ENTITIES AFFECTED BY THIS POLICY

- All units of the university

WHO SHOULD READ THIS POLICY

- All stewards and custodians of institutional information

WEB ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/policy/policies/information-security
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 5, Information Technologies
Responsible Executive: Chief Information Officer and Vice President/Chief Information Officer, WCM
Responsible Office: IT Security Office/ WCM Privacy Office
Final Issuance: July 20, 2010
Last updated: June 25, 2018

POLICY 5.10

Information Security

CONTENTS

POLICY 5.10

Information Security

CONTENTS, continued

POLICY 5.10

Information Security

RELATED RESOURCES

University Policies and Documents 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 5.8, Authentication to Information Technology Resources

University Policies and Documents Applicable to Ithaca Campus Units Only
University Policy 4.12, Data Stewardship and Custodianship
University Policy 5.1, Responsible Use of Electronic Communications
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
CIT Encryption Guidelines

University Policies and Documents Applicable to Weill Cornell Medicine (WCM) Only
WCM Policy 11.2, Privacy of the Network
WCM Policy 11.3, Data Classification
WCM Policy 11.6, Laptop Encryption
WCM Policy 12.1, Integrity
WCM Policy 12.2, Physical Security
WCM Policy 12.3, Authentication and Authorization
WCM Policy 12.4, Administrative Security
WCM Encryption Guidelines
WCM Password Policy

External Documents Applicable to All Units of the University
Family Education Rights and Privacy Act (FERPA)
Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq.
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
New York State Information Breach and Notification Act (Section 899-aa)

Forms and Tools

Name	Description
Cornell Dropbox	Use to transfer files securely to other individuals with Cornell NetIDs. Files are encrypted during transport over SSL (https://) using strong encryption only.

POLICY 5.10

Information Security

RELATED RESOURCES, continued

WCM File Transfer Service	Use to exchange confidential information with individuals whose e-mail addresses does not end in “med.cornell.edu” or “nyp.org.” (For use by WCM staff members only.)
WCM Business Associates Agreement	Use to provide documentation for obtaining access to confidential information. Contact (212) 746-1179 to obtain the document.

CONTACTS, ITHACA CAMPUS UNITS

Direct any general questions about this policy to your department's administrative office. If you have questions about specific issues, call the following offices:

Subject	Contact	Telephone	Email/Web Address
General Interpretation and Clarification	Chief Information Security Officer	(607) 255-8421	security@cornell.edu it.cornell.edu/security-and-policy
Specific Procedural Requirements	Chief Information Security Officer	(607) 255-8421	security-services@cornell.edu it.cornell.edu/security-and-policy

CONTACTS, WEILL CORNELL CAMPUS UNITS

Subject	Contact	Telephone	Email/Web Address
General Interpretation and Clarification	WCM Privacy Office	(212) 746-7457	intranet.med.cornell.edu/hipaa/

DEFINITIONS, ITHACA CAMPUS UNITS

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

Custodian	An individual with access to institutional information, or who uses that information in the legitimate course of university business.
Handheld Device	An electronic, hand-held computing device such as a smartphone, cellphone, tablet, or personal digital assistant (PDA) used to conduct university business.
Institutional Information	Information generated in furtherance of the university's mission, not including research data.
Institutional Information Steward	A university office/official with executive responsibility over its institutional information.
Institutional Information, Classifications of	Categories of information that have different technical safeguard rules relative to their sensitivity as determined by law, regulations, and reputation, among other factors. For specific classifications of information, see the Procedures, Ithaca Campus Units--Overview section of this policy.
Legitimate Interest	A requirement for access to institutional information to perform one's authorized duties effectively and efficiently.
Specialized Device	A piece of electronic equipment that might use a non-traditional computing platform or that is used on a network, such as networkable copiers, printers and fax machines, supervisory control and data acquisition systems (SCADA), network-attached instrumentation, or other control systems.
Unit	A college, department, program, research center, business service center, office, or other operating unit.

DEFINITIONS, WEILL CORNELL CAMPUS UNITS

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

Custodian or Steward	Weill Cornell Medicine (WCM) faculty and staff members, researchers, students, and affiliates who create, store, send, or receive information or data in their capacity as members of the WCM community.
Institutional Information	All information created, stored, sent, or received by WCM faculty and staff members, researchers, students, and affiliates as part of their capacity as members of the WCM community.
Institutional Information, Classifications of	Categories of information that have different technical safeguard rules relative to their sensitivity as determined by law, regulations, and reputation, among other factors. • For specific classifications of information, see the Procedures, Weill Cornell Campus Units--Overview section of this policy.
ISPAC	The Information Security and Privacy Advisory Committee
WCM	Weill Cornell Medicine

POLICY 5.10

Information Security

RESPONSIBILITIES—ITHACA CAMPUS UNITS

Cornell Information Technologies (CIT)	Maintain overview responsibility for implementation of this policy. Train and educate the university community on this policy. Monitor technological developments, changes in the law, user behavior, and the market, and update this policy, as appropriate.
Custodian	Implement procedures for policy compliance. Execute unit's procedures for meeting minimum standards for information security according to information classification (see Cornell IT Ithaca Procedures). Report all information breach incidents, as detailed in University Policy 5.4.2, Reporting Electronic Security Incidents.
Institutional Information Steward	Categorize institutional information into one of three categories: • Level 1: Confidential • Level 2: Restricted • Level 3: Public Establish rules for disclosing and authorizing access to institutional information. Conduct annual risk assessments of privacy practices and security standards.
IT Security Office	In consultation with the IT Security Council, the IT Managers' Council, and other stakeholders, determine technical procedures related to this policy and review them annually, at a minimum.
Unit Head	Assume responsibility for policy compliance for the institutional information under his or her control. Deploy procedures to comply with the institutional information steward's rules for disclosing, categorizing, and authorizing access to institutional information. Deploy procedures for meeting minimum standards for institutional information security according to information classification (see Cornell IT Ithaca Procedures).
Unit Security Liaison	Receive and address requests for exceptions to security requirements. Maintain a current list of exceptions to security requirements. Review annually all exceptions to baseline IT security requirements. Receive and maintain an inventory of all systems holding confidential (Level 1) information.

RESPONSIBILITIES—WEILL CORNELL CAMPUS UNITS

Information Technologies and Services Department (ITS)	Categorize institutional information into one of three categories: • Level 1: Confidential • Level 2: Restricted • Level 3: Public Establish rules for disclosing and authorizing access to institutional information. Implement and manage technologies and processes that facilitate the automatic categorization of data. Create and manage security controls that achieve policy compliance. Monitor technological developments, changes in the law, user behavior, and the market, and update this policy, as appropriate.
Information Security and Privacy Advisory Committee (ISPAC)	Advise the institution as to how it might best adhere to the principles and procedures within this policy.
Weill Cornell Medicine faculty and staff members, students, and affiliates	Read, understand, and follow the principles and procedures in this policy. Assume responsibility for policy compliance for the institutional information under his or her control.

POLICY 5.10

Information Security

PRINCIPLES

Introduction

Privacy practices and security standards serve to preserve and protect institutional information. This policy incorporates a set of requirements for protecting the university's computers and networks as well as safeguarding the university's institutional information. These procedures set out the appropriate security standards for information at both the Ithaca campus and Weill Cornell Medicine.

The integration of information technologies in virtually every aspect of transmission and storage of institutional information 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 university community members are responsible for adhering to the procedures that follow.

While no one policy can absolutely ensure the protection of institutional information, this policy does provide Cornell University with a coherent plan integrating state-of-the-art administrative and logical security practices.

POLICY 5.10

Information Security

PROCEDURES, ITHACA CAMPUS UNITS—OVERVIEW

Classifications of Institutional Information

Confidential (Level 1) Information

Information that has been determined by institutional information stewards to require the highest level of privacy and security controls. Currently, any information that contains any of the following data elements, when appearing in conjunction with an individual's name or other identifier, is considered to be confidential (level 1) information:

- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)

◆**Notes:**

1. The data elements that comprise the category "Confidential (Level 1) Information" are reviewed regularly, and subject to change.
2. Copies you store of your own personal information do not fall under the requirements for safeguarding confidential data.

Restricted (Level 2) Information

All information used in the conduct of university business, unless categorized as public (level 3) or confidential (level 1).

Public (Level 3) Information

Information that the university has made available or published for the explicit use of the general public.

◆**Note:** The technical safeguards associated with these data elements and types are *required* by policy. Data stewards, deans, or supervisors may require staff members under their purview to apply these technical standards to other or additional types of data. This policy does not limit these safeguard provisions to only these data elements and types, but establishes the foundational rules beneath which no steward or custodian may allow.

Stewards, Unit Heads, and Custodians

Institutional information stewards (as established by University Policy 4.12, Data Stewardship and Custodianship) assume responsibility for the management practices of information under their purviews, including a general inventory of the kind of information specific to their roles, classification of information into one of the three categories that this policy creates for the purposes of establishing rules for the protection of that information and, most importantly, providing up-to-date

authorization for access to information. Unit heads have the responsibility to implement this policy within their units. Custodians must comply with the rules of this policy and the baseline standards for computer security, as well as the technical requirements for the protection of confidential (level 1) and restricted (level 2) information.

Security of Paper Documents

Anyone handling confidential (Level 1) information 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. Anyone in possession of institutional information should be mindful of the sensitivity of that information, and use appropriate judgment about its handling and storage management. The measures outlined below are mandatory for paper documents containing confidential (Level 1) information.

General Requirements

1. Documents containing confidential (Level 1) information must be secured so they are accessible only to authorized personnel. "Secured" means locked in a drawer, filing cabinet, or a hard-wall, private, or shared office.
2. Documents containing confidential (Level 1) information may never be left unattended in a public area.
3. When no longer needed for daily operations, documents containing confidential (Level 1) information must be destroyed or moved to a secure archive facility.
4. When documents containing confidential (Level 1) information are transmitted off-campus, a signed receipt of delivery is required.
5. When documents containing confidential (Level 1) information are transmitted via campus mail, the envelope must be sealed and stamped "Confidential."
6. When documents containing confidential (Level 1) information need to be destroyed, a secure disposal service or a crosscut shredder must be used.

Requirements Specific to Printers and Fax Machines

1. During business hours, the device should be in a location where it is accessible only to authorized personnel.

   ◆**Note**: On an occasional basis, sensitive documents can be sent to an unsecured device, as long as the recipient or another authorized receiver is sure to be present at the time of printing.

2. Off-hours, the device has to be in a physically secure (locked) environment.

   ◆**Suggestion**: If possible, periodic review of the device's record of received documents must be performed, to ensure that all documents are accounted for.

POLICY 5.10

Information Security

PROCEDURES, ITHACA CAMPUS UNITS — BASELINE IT SECURITY REQUIREMENTS

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, outsourced, or in a university facility, that is (a) used to conduct university business, and/or (b) connected to Cornell campus networks (including non-Cornell equipment).

These requirements, as well as the accompanying requirements for securing confidential (level 1) information, reflect an approach referred to as "layered defense" or "defense-in-depth." As a community, we need to build defenses on multiple levels — 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 will move the university towards a more secure IT environment.

◆ **Note**: For the purposes of this policy, "conducting university business" does *not* include viewing or updating your own individual university information.

Any item labeled as a "◆ **Suggestion**:" reflects a beneficial practice that might become a requirement at some future date.

Exceptions

The following exception process must be followed for all computers or other IT resources that are not able to meet these security requirements:

1. IT resources that cannot meet the following requirements must be identified to the appropriate Unit Security Liaison. The Unit Security Liaison will look for alternate methods to address the risk in question. If an alternate security solution can be found to address the specific risk, an exception is not required.
2. The Unit Security Liaison may identify a local solution or consult with the IT Security Office for assistance.
3. The Unit Security Liaison will maintain a list of all IT resources that require an exception, and review these exceptions on an annual basis.

Baseline Requirements Specific to Handheld Devices

Handheld devices include smartphones, cellphones, tablets, or personal digital assistants (PDAs) used to conduct university business.
Any handheld device that is used in conjunction with Cornell activities, including retrieval of e-mail or calendar data must be configured so that it can be locked or erased if it is lost or stolen.

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

In addition, the following measures are strongly recommended. Note that a local department may choose to require these measures under local policy or practice:

1. Configure the device to lock the console after a period of inactivity no greater than 30 minutes, with a password required to unlock the device. Use of the simple numeric code that is an option on some devices is discouraged.
2. Configure the device to erase all data after not more than ten failed attempts to enter the password.

◆ **Note**: For requirements applicable to handheld devices that access or store Confidential (Level 1) Information, see "Confidential (Level 1) Information--Requirements Specific to Handheld Devices."

Baseline Requirements for All Other Computers

1. Keep all relevant operating system, server, and application software up-to-date (patched).
   - Develop and document a patch management process such that all vendor-defined security or critical software updates are installed as soon as possible, but no later than 14 days after their release.
     i. The IT Security Office may, independent of a software vendor, issue a patch bulletin. Critical software updates identified either by a software vendor outside their normal release cycle or by the IT Security Office are subject to the 14-day requirement above, and will be announced through the IT website, the network administrators e-mail list, the IT Security e-mail list, and the IT Security Council.
   - A system that is currently not connected to the network does not need to be patched immediately. When it is brought back online, all the relevant updates must be installed immediately.
2. Configure user privileges to be as low as possible while still meeting operational needs. Consistent or regular use of any account with administrative privileges is inappropriate.
3. Ensure all accounts have strong passwords at least equivalent to the strength required for NetID passwords.

   ◆ **Note**: University Policy 5.8, Authentication to Information Technology Resources mandates that the password associated with one's NetID can only be used in conjunction with the central authentication infrastructure.
4. No electronic distribution of passwords in the clear, i.e., transmission, must be encrypted.
5. For any computer system that is not in a secure, private space, run a password-protected screen saver, or some other console-locking mechanism, that is

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

triggered after fifteen minutes (or less) of inactivity.

6. Ensure local/personal firewalls (Symantec Client Firewall, Windows Firewall, MacOS X firewall, etc.) and/or IPSec filters are installed and running.
7. On all Windows and Macintosh systems, run anti-malware (anti-virus, etc.) software with daily updates and active protection enabled.

   ◆ **Suggestion**: Run an anti-malware package on Linux systems, as well.

Baseline Requirements Specific to Desktops and Laptops

1. All university-owned desktops, laptops, smartphones, tablets, and other portable computing devices must utilize whole-disk-encryption software to protect all local, persistent storage when the system is powered off. Exceptions:
   - Virtual machines hosted in a data center. Virtual machine instances run on computers subject to this requirement need not be encrypted provided the host operating system is encrypted according to this requirement.
   - Systems tied to instrumentation, infrastructure, and desktop computers that do not leave a locked room in a university-owned or leased facility. Whole disk encryption is *highly recommended* on desktop computers in locked facilities.
   - Systems that automatically return to a fixed software configuration after user logout, on reboot, or after a specified interval of time.
   - Data-less workstations, i.e., those that are configured to prevent the local storage of end-user data.
   - Computers that are to be used in locations that legally prohibit encryption.

   ◆ Note: Unit-level Security Liaisons are required to maintain an inventory of systems that are not encrypted due to these or other exceptions.
2. All local shares and other mechanisms for file access must be password protected.

   This requirement forbids "open shares" (unauthenticated read/write access), "drop folders" (unauthenticated write-only access) and "public folders" (unauthenticated read-only access) on an individual's system.

   ◆**Suggestion**: Use a departmental file server instead of local shares.

   If multiple individuals use a system, each should have his or her own login account, or the system should be restored to a known, clean state prior to each individual use. This also applies to "loaner" systems.

   A desktop, laptop, netbook, or tablet that is left unattended in a public or otherwise insecure location must be physically secured.

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

◆**Suggestion**: Provide locking cables to staff members who travel with such mobile devices.

Baseline Requirements Specific to Application and File Servers

1. The operating system and all software applications must be secured according to the most current industry best practices. The operating system or software vendor is the definitive authority for these best practices; however, best practices issued by CIS, the NSA, SANS, FIRST, and the IT Security Office may also be used.
   - Servers must operate only the minimum software and application specific features that are necessary for the system to perform its function. Therefore, the rule is to disable all network services, including specific application features that are not needed for the system to fulfill its function.
   - Change any passwords with default values set by the vendor.
2. All Web applications developed for university use must be free of OWASP Top 10 vulnerabilities that are reported at or above "High" severity according to a vulnerability scan tool approved for this purpose by the IT Security Office.

   Exceptions:
   - Software as a Service (SaaS) applications: Effort should be made to require vendors to observe this requirement through their own development processes, or to allow remote vulnerability scanning by the IT Security Office.
   - On-premise commercial applications for which source code is not available must still be scanned, when first installed or whenever upgraded, and vulnerabilities reported to the vendor for correction.
   - If the entire application is placed behind 2-factor authentication.
   - Where the application has been placed behind a Web Application Firewall approved by the IT Security Office.
3. Shared accounts are prohibited, except where it is not technically possible to provision individual accounts.
   - Where a shared account *is* necessary, maintain a local inventory of who has access to the account.
   - Change the password for any shared account when there is any change in personnel or access requirements.

◆**Suggestion**: Keep servers, especially those that are open to users outside of the local workgroup, on a segregated network.

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

Baseline Requirements Specific to Public Workstations and Kiosks

◆ **Note**: These requirements do not apply to computer labs and similar environments with systems that are not for use by the general campus population and require a unique, individual login.

1. All systems made available for walk-up use must be configured to require a login using a credential assigned for individual use.
   - Use of the NetID is preferred. Where the NetID is not used, the system providing authentication must retain logs of login successes and failures for a minimum of 90 days. Such environments must be registered with the IT Security Office.
   - Systems in settings where a regulatory exception exists, or where unit mission or funding sources mandate public access are exempt from this requirement. Such exempt systems must be in highly visible public areas or monitored by university employees.
   - Teaching labs that are normally closed for walk-up use except during scheduled class times are exempt from this requirement.
   - Kiosks or walk-up terminals that reside in locked, limited-access rooms are exempt from this requirement.
   - Computers that are checked-out or released for temporary use in return for a photo-ID are exempt from this requirement provided records matching individual to computer MAC address are maintained by the department for a minimum of 30 days.
2. Such systems may not be on the same subnet as computers used to conduct university business.
3. Such systems must display an appropriate logon banner or bear signage with the following information:
   - A statement about responsible use
   - A warning about using the system for personal or sensitive information
   - A reminder to logout and/or clear any active credentials
4. No local file shares permitted.

   If a user needs system privileges (ability to write files), then the computer must be restored to a known, clean state between individual sessions.
5. Visually inspect such systems regularly, at the very least on a quarterly basis, to see if physical security has been compromised.

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

Baseline Requirements Specific to Specialized Devices

A specialized device is a piece of electronic equipment that might use a non-traditional computing platform or that is used on a network, such as networkable copiers, printers and fax machines, supervisory control and data acquisition systems (SCADA), network-attached instrumentation, or other control systems.

◆**Note:** The requirements of this section do not extend to smartphones, PDAs, tablets, or other handheld computing devices; these are addressed under "All Computers," above.

1. Vendor-defined security or critical software or firmware updates must be applied within 30 days of their release.
2. Passwords used to access such devices must be changed from their vendor-supplied defaults.
3. Where technically feasible, passwords must meet the complexity requirements outlined for NetIDs in University Policy 5.8, Authentication to Information Technology Resources.
4. Vendor-supplied accounts not necessary for maintenance support, or device functionality must be locked or disabled.
5. Services unnecessary for device function in its environment must be disabled where technically feasible.
6. Devices that can provide their own network access controls must be configured to restrict access to only those systems or networks necessary for the device to perform its function.
7. Devices that do not require Internet access, apart from software updates, must be addressed according to an Internet non-routable addressing scheme (RFC1918 space, 10-space, or functional equivalent.)
8. Remote use or administration must be performed via secure remote access mechanism such as SSH (secure shell) or virtual private network (VPN).
9. When devices of this type are removed from service (discarded, reassigned, recycled, sold, or returned to the vendor for service or replacement), any persistent onboard storage must be erased or destroyed according to the standards outlined elsewhere in this policy.
10. Recommendation: Use VLANs or other network segregation tools to separate these devices from networks containing servers or workstations. These VLANs become subject to the same network access restrictions applied to all computers as part of this policy (Baseline Requirements – Network Requirements for All Systems)

PROCEDURES, ITHACA CAMPUS UNITS—BASELINE IT SECURITY REQUIREMENTS, continued

11. Recommendation: Where feasible, control or laboratory systems should be placed on networks that cannot be reached from the Internet or from other campus networks.

Network Security

1. Implement network access controls, firewalls, or equivalent operations on any university network that is not used exclusively for public workstations, research equipment, or instructional systems.

   Host firewalls and similar measures can be used to supplement network ACL/firewall rules.

   ◆ **Suggestion**: Where off-campus connectivity is not needed, put the system into a non-routable space (10-Space).
2. 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.

Reviews and Assessments

The unit is responsible, at least annually, for assessing the local infrastructure and environment. This assessment should include the following:

1. Review edge ACLs and other network security mechanisms.
2. Run a vulnerability scanner, such as Nessus or GFI LANguard, on all unit subnets and remediate high-risk vulnerabilities.
3. Review the security of all file and application servers.
   - Check for vulnerabilities in websites, databases, etc.
   - Use a data discovery tool to scan file servers for confidential (level 1) information. (This requirement does not apply to databases or other structured data repositories or e-mail servers.)
4. For a sample set of staff computers, conduct content inventories using a data discovery tool to ensure no improper instances of confidential (level 1) information.

   ◆ **Suggestion**: Run annual, or more frequent, content scans of all systems.
5. Audit account distribution to ensure that only current, authorized personnel have access to departmental systems.

POLICY 5.10

Information Security

PROCEDURES, ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION

Introduction

To better safeguard the university's institutional information, the Information Technology (IT) Security Office requires the following practices for electronic transmission and storage of confidential (level 1) information. The following sections of this policy outline classifications of institutional information, and, for that which is classified at the highest level (level 1), its encryption requirements, scanning requirements, and other measures.

◆**Note:** These requirements are in addition to those outlined in the Procedures, Ithaca Campus Units—Baseline IT Security Requirements section of this policy.

Information Classification

This policy establishes three institutional information security classifications:

1. Confidential (level 1)
2. Restricted (level 2)
3. Public (level 3)

Unless otherwise classified, all information used in the conduct of university business is restricted (level 2). Institutional information that has been explicitly made available to the public, with no authentication required for network access, is public (level 3).

The confidential (level 1) information classification currently comprises the following data elements, when they appear in conjunction with an individual's name or other identifier:

- Social Security numbers
- Credit card numbers
- Driver's license numbers
- Bank account numbers
- Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)

This set may expand based on future regulatory requirements or designations made by the appropriate institutional information steward and with appropriate review.

These requirements apply to confidential (level 1) information that is under the custodianship of the university, and so do not pertain to your own personal information you may have stored on a computer or device.

Please note that some data elements classified as confidential (level 1) information are subject to legal or regulatory requirements that go beyond those given here. Such requirements for regulated information must be fulfilled, along with these Cornell

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

requirements. In particular, credit card numbers and how the university handles credit card transactions are subject to the Payment Card Industry Data Security Standard (PCI DSS). For more information, see University Policy 3.17, Accepting Credit Cards to Conduct University Business.

Systems Subject to These Requirements

These requirements apply to any system that holds confidential (level 1) information, both on- or off-campus, and even if not university-owned.

For the purposes of this policy, a system is considered to be "holding" confidential (level 1) information when such information is stored locally on the system, when the system accesses any storage volume (network or local) containing such information, or when the system is used to process, analyze, or transmit such information.

Thus, for example, a Windows system where the primary user's domain password is sufficient to mount a file server volume and access directories with confidential (Level 1) information would need to be secured as if such information was stored locally.

Encryption Standards

In several places, these requirements specify a need to encrypt information, either for storage or for transmission. Some examples are given of viable encryption implementations but no comprehensive list is provided here.

The IT Security Office will approve a given method of encryption for use with confidential (level 1) information if it both (a) employs a contemporary algorithm, and (b) is effectively implemented by the product in question. More information and a summary of approved encryption vehicles can be found at it.cornell.edu/security-and-policy/store-confidential-data.

Exceptions

The following exception process must be followed for all computers or other IT resources that are not able to meet these security requirements:

1. IT resources that cannot meet the requirements must be identified to the appropriate Unit Security Liaison. The Unit Security Liaison will work with the IT Security Office to determine alternate methods to remedy the specific risk being addressed.
2. If no alternative can be found, the applicable institutional information steward will be consulted to determine appropriate course of action.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

3. Both the IT Security Office and Unit Security Liaison will maintain a list of all IT resources that require an exception and review these exceptions on an annual basis.

Confidential (Level 1) Information--Requirements Specific to Handheld Devices

◆ **Note**: When a technology solution exists to help ensure compliance, this policy will be revised to require their implementation. For baseline requirements for devices, see "Baseline Requirements Specific to Handheld Devices."

1. For any handheld device that holds, stores, processes, or accesses confidential data:
    a. The password required to unlock the device must meet or exceed the password complexity requirements outlined for NetID passwords in University Policy 5.8, Authentication to Information Technology Resources.
    b. The device must lock after a period of inactivity not more than 15 minutes and require a password to unlock.
    c. The device, or the data in question, must be encrypted. If encryption is not supported, the device cannot store confidential data.

Confidential (Level 1) Information--Requirements for All Other Computers

1. Keep all relevant operating system, server and application software up to date.
    - Develop and document a patch management process such that all vendor-defined security or critical software updates are installed as soon as possible, and no later than seven days after their release.
        i. The IT Security Office may, independent of a software vendor, issue a patch bulletin. Critical software updates identified either by a software vendor outside their normal release cycle or by the IT Security Office are subject to the seven-day requirement above and will be announced through the IT website, the network administrators e-mail list, the IT Security e-mail list, and the IT Security Council.
2. The operating system and all software applications must be secured according to the most current industry best practices The operating system or software vendor is the definitive authority for these best practices; however, the best practices issued by CIS, the NSA, SANS, FIRST, and the IT Security Office may also be used.
    - Disable all network services, including specific application features, that are not needed for the system to fulfill its function.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

- Change any passwords with default values set by the vendor.

3. Confidential (level 1) information and information that is being made available for public access may not be on the same system.
   - An open website, i.e., one that does not require authentication for access, may not be run on a system holding confidential (level 1) information.
   - Peer-to-peer (P2P) file-sharing software may not be run on a system holding confidential (level 1) information.
   - Confidential (level 1) information and information available for public access may reside in different virtual machines running on the same system, as long as the host system and the host operating system meet all the requirements for a file or application server holding confidential (level 1) information.
4. Activate the operating system and, where possible, application logging, with logs that are retained for at least 90 days. At a minimum, the following must be logged:
   - Access to all audit logs.
   - Access to confidential (level 1) information.
   - Failed access attempts.
5. On a quarterly basis, audit and verify that only currently authorized personnel have accounts that grant access to confidential (level 1) information.

◆**Suggestion**: Audit file, application, and system privileges on a periodic basis.

Confidential (Level 1) Information--Requirements Specific to Desktops and Laptops

1. The account used for daily operations must be configured not to allow software installs, or must require the account password for an install.

   ◆**Suggestion**: Where feasible, do not give end users any accounts that permit software installation.

2. On any system holding confidential (level 1) information, use a unique password, not shared with other systems, for local administrator accounts (accounts with elevated privileges).

   In particular, the local administrator password used by IT support staff members must be different for each system that holds confidential (level 1) information.

   Such passwords can be generated algorithmically as long as the unique portion is not a string that is stored electronically on the system.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

3. Confidential (level 1) information stored locally on a system must be removed when no longer needed for an operational reason.

   ◆**Suggestion**: Do not permit storage of confidential (level 1) information on individual staff member machines.

4. In areas where confidential (level 1) information is handled on a regular basis, run a data discovery tool on all systems every six months.

   - Data-discovery tools are necessary, but not sufficient to fulfill this requirement due to their technical limitations. Data custodians must make a reasonable effort to determine whether confidential data is present on the device, in addition to that which the data discovery tool reveals.

5. Confidential (level 1) information must be encrypted on all of the following. Whole-disk-encryption alone is not sufficient to meet this requirement, though encryption of files or folders containing confidential (level 1) information is *highly recommended*:

   a. Any system that, even on a temporary basis, is not located on one of the Cornell campuses or some other formal university location.

   b. Any laptop, netbook, tablet, smart phone, PDA, or other mobile device.

      ◆**Suggestion**: Where feasible, use full-disk encryption on such devices.

   c. Any other system that is not physically secured or in a secure location accessible only to authorized university personnel.

   d. All removable storage devices attached to systems that store or process confidential (level 1) information must be encrypted.

   If full-volume encryption is used, the volume should be mounted only when the system is in active use, ensuring that the encryption does not interfere with the ability to create and retrieve backups.

   Protect encryption keys against disclosure, misuse, and loss. See University Policy 5.3, Use of Escrowed Encryption Keys.

   Examples of portable media include external hard drives, USB drives, CDs, DVDs, tapes, diskettes.

   While Microsoft Office 2007 includes a facility for appropriately strong encryption of documents, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

Acceptable encryption solutions include, but are not limited to, EFS under Windows 2000 and later, BitLocker under Windows Vista and Server 2008, FileVault under Mac OS X, CyberAngel, TrueCrypt, BestCrypt, and PGP.

Delete caches for Web browsers or operating system temporary files every 24 hours, or set the system to restart after a period of time not longer than every 24 hours.

◆ **Suggestion**: Encrypt all instances of confidential (level 1) information under the custodianship of individual staff members.

Confidential (Level 1) Information--Requirements Specific to Application and File Servers

1. All application servers and file servers must be housed in a physically secure computer room or data center. Entry must be logged and the logs retained for at least five days.
   ◆ **Suggestion**: Where feasible, log exits as well.
   ◆ **Note**: Video monitoring is an acceptable solution to this requirement.
   ◆ **Note**: Visitors are not permitted except under escort.
   - An individual's access to a store of confidential (level 1) information should be via an account assigned for the sole use of that individual. This requirement is not to be interpreted as disallowing access to an encrypted dataset via a shared encryption key.
2. Confidential (level 1) information should be removed from file servers when it is no longer needed on an operational basis. To the extent feasible, this also applies to confidential (level 1) information stored in databases and other application frameworks.
3. Access to university Confidential (level 1) information requires 2-factor authentication.
   a. **Note:** Where direct access to confidential data, for example through file shares or specialized applications, cannot be secured with 2-factor authentication, access must be restricted to a 2-factor bastion host or 2-factor VPN.
   b. **Note:** Duo or RSA SecurID meet this requirement. Other 2-factor technologies require the approval of the IT Security Office.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

4. Servers should use application whitelisting software to ensure only known, approved software processes are able to run. When the university licenses a commercial application whitelisting product, this recommendation will become a requirement.
5. Any confidential (level 1) information on development and test systems must be masked or redacted.

Confidential (Level 1) Information--Requirements Specific to Public Workstations and Kiosks

Such systems may never be used for administrative processing of confidential (level 1) information.

Confidential (Level 1) Information--Network Security

1. The edge ACL or other packet-filtering mechanism on any subnet with systems housing confidential (level 1) information must employ a default-deny strategy that prohibits unnecessary inbound, internal and external connections and that strictly limits access to the systems with confidential (level 1) information.

   ◆ **Suggestion**: Where off-campus connectivity is not needed, put the system into a non-routable space (10-Space).
2. Any system holding or accessing confidential (level 1) information that uses a campus wireless connection must use Eduroam, or a departmental wireless network with equivalent or stronger security (authentication required, encrypted transmission).
3. Any system accessing confidential (level 1) information via a wireless network OR any remote, off-campus access to a system containing such data must use an encrypted communication method. Examples of encrypted network transport include ssh/sftp, SSL/TLS, and VPN with encryption enabled.

   - Encrypting data prior to transmission, i.e., 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.
4. Fully document the list of services, protocols, and systems permitted access into such subnets.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

5. A subnet's ACL list or firewall rule set suffices to fulfill this requirement.
   - Review this documentation on a semiannual basis.
   - File a copy of the current documentation with the local IT head and the Unit Security Liaison.

Additional Confidential (Level 1) Information--Encryption Requirements

1. Confidential (level 1) information must be encrypted when it is transmitted via e-mail.
   - This applies to such information either in the body text or in an attachment.
   - While Microsoft Office 2007 includes a facility for appropriately strong encryption of e-mail attachments, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.

   ◆ **Note**: The Dropbox service (dropbox.cornell.edu) provides a secure, Web-based vehicle for exchanging files with other people holding Cornell NetIDs.
2. Confidential (level 1) information may not be transmitted via instant messaging (AIM, etc.) or text messaging (SMS).

   ◆ **Note**: The use of instant messaging to transport confidential data is allowed only if the transmission is encrypted, sender and recipient are identified by accounts assigned for individual use, and such activity is logged according to the requirements defined in item (4) of Confidential (Level 1) Information--Requirements for All Computers, above.
3. Confidential (level 1) information must be encrypted when it is accessed via the Web.
4. Confidential (level 1) information must be encrypted when it is transmitted over non-Cornell networks.

   ◆ **Suggestion**: Whenever feasible, it should also be encrypted when transmitted within Cornell networks.
5. If passwords that grant access to confidential (level 1) information are stored on a networked device, they must be encrypted. While Microsoft Office 2007 includes a facility for appropriately strong encryption, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

6. Any confidential (level 1) information on a storage device used to transport data physically must be encrypted.
    - This does not apply to media that is used exclusively to store data and is kept in a secure location. For example, CDs, DVDs, or tapes kept under lock and key.
    - Where this is not feasible, compensatory measures, such as increased physical security, must be taken.
7. Passwords or encryption keys used to access confidential (level 1) data must be protected as if the passwords and keys were confidential and, therefore, are subject to all requirements for confidential (level 1) information

Inventory of Confidential Information

Maintain an inventory of all systems holding confidential (level 1) information.

1. Review the inventory every six months.
2. File a copy of the current inventory with the local IT head and the Unit Security Liaison.
3. Both workstations (laptop and desktop) and servers (file, application, and database) need to be included in the inventory. Out of scope are mobile/smart phones, PDAs, USB drives, and removable media (DVDs, CDs, diskettes, and tapes).
4. The required information, detailed below, must be recorded explicitly for each system holding confidential (level 1) information. However, not all of this information needs to be in the inventory itself, as long as the rest of the required elements can all be retrieved on short notice. The inventory does need to contain sufficient detail, so that the mapping to the balance of the requested information is unambiguous.
    - Information required for workstations:
        - Date of entry into inventory
        - Date of last review or update
        - Assigned user (or, if not for use by a single individual, the administrator)
        - Role of the individual/function of system
        - Whether a desktop or a laptop
        - OS platform (Win, Mac, Linux, *nix, Solaris, etc.)

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

- Primary hostname
- As applicable, assigned IP(s) for wired interface(s)
- MAC address(es) of Ethernet and Wi-Fi interfaces
- Make, model, and serial number
- Inventory tag (optional)
- Number of associated external hard drives, if any
- Backup (none, local, departmental, or TSM)

- Information required for servers:
  - Date of entry into inventory
  - Date of last review or update
  - Primary administrator
  - Function(s)
  - Type of service (dev, test, or prod)
  - OS platform (Win, Mac, Linux, *nix, Solaris, etc.)
  - As applicable, DB platform (Oracle, MS SQL, FileMaker, etc.)
  - Primary hostname
  - Physical location
  - Assigned IP address(es)
  - MAC address(es) (optional)
  - Make and serial number
  - Inventory tag (optional)
  - Data storage (internal, external, or both)
  - Backup (none, local, departmental, or TSM)

5. Any of the following that are specific to the department or unit must be listed in the inventory:

   - E-mail servers (detail required for other types of servers does not need to be given)
   - Outsourced applications that process confidential data
   - Outsourced data repositories that hold confidential data

PROCEDURES , ITHACA CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INFORMATION, continued

Additional Process and Documentation Requirements

The IT Security Office will provide templates and specific guidelines for fulfilling items listed here.

1. Define and document incident response and escalation procedures for a potential loss of confidential (level 1) information. Review these processes on a semiannual basis.
2. Document how confidential (level 1) information flows into and out of the local business unit and local applications.

   Review this documentation on a semiannual basis.

   File a copy of the current documentation with the local IT head and the Unit Security Liaison.

   The relevant central unit will be responsible for fulfilling this requirement for any campus-wide application or service that handles confidential (level 1) information.
3. When a unit grants any non-governmental external entity access to confidential (level 1) information, that entity must provide documentation of the following:
   - How this information will be transmitted, processed, stored, secured, and destroyed when no longer needed.
   - How such information is monitored and what incident response mechanisms are in place.
4. Review this documentation on an annual basis.
   - Follow a documented process for disposing of confidential (level 1) information when it is no longer needed for legal, regulatory, or business purposes.
   - Recommended practices are available at it.cornell.edu/guides/creating-local-unit-data-cleanup-program.
   - Ensure that local and university information retention guidelines are met.
   - Review this documentation on an annual basis.
   - File a copy of the current documentation with the local IT head and the Unit Security Liaison.
5. All users with access to confidential (level 1) information must execute a yearly attestation of the awareness of the relevant policies, risk, and protective measures. An individual's electronic access to confidential (level 1) information does not convey any right to share that information with unauthorized personnel.

POLICY 5.10

Information Security

PROCEDURES, WEILL-CORNELL CAMPUS UNITS--OVERVIEW

Classification of Institutional Information

Information technology and data constitute valuable Weill Cornell Medicine (WCM) assets. Depending on their classification, these assets are additionally subject to state and federal regulation. This policy facilitates compliance with these regulations and adherence to commonly accepted security practices.

Classification

The following definitions must be adhered to when determining classification:

1. **Level 1 – Confidential**: Includes data protected by state and/or federal law against unauthorized use, disclosure, modification, or destruction. Confidential data includes, without limitation, the following:
    a. Patient billing or medical records (in any electronic form, including but not limited to databases, spreadsheets, audio/video recordings, transcripts, etc.), including data covered by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).
    b. Student records, including those protected under the Family Education Rights and Privacy Act (FERPA).
    c. Financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA) and credit card numbers.
    d. Employment records, including pay, benefits, personnel evaluations, and other staff records.
    e. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq.).
    f. Social Security numbers.
2. **Level 2 – Restricted**: Includes information that requires protection from unauthorized use, disclosure, modification, and/or destruction, but is not subject to any of the items listed in the "Confidential" definition above. Restricted (internal use only) data includes the following:
    a. Data related to WCM operations, finances, legal matters, audits, or other activities of a sensitive nature.
    b. Data related to donors or potential donors.
    c. Information security data, including passwords, and other data associated with security-related incidents occurring at the college.
    d. Internal WCM data, the distribution of which is limited by intention of the author, owner, or administrator.

PROCEDURES , WEILL-CORNELL CAMPUS UNITS—OVERVIEW, continued

3. **Level 3 – Public**: Includes data that can be disclosed to any individual or entity inside or outside of WCM. Security measures may or may not be needed to control the dissemination of this type of data. Examples include the following:
    a. Data on public WCM websites.
    b. Press releases.

Security of Paper Documents

Anyone handling confidential information in hard-copy (paper) form should take all appropriate measures to secure it physically. Those in possession of paper documents should be mindful of the sensitivity of the information they contain and use appropriate judgment around their handling and storage. The measures outlined below are mandatory for paper documents containing confidential information, and should also be followed for any with restricted information of a particularly sensitive nature.

General Requirements

1. Confidential documents must be secured so they are only accessible to authorized personnel. Secured means locked in a drawer, filing cabinet or a hard wall, private or shared office.
2. Confidential documents may never be left unattended in a public area.
3. When no longer needed for daily operations, confidential documents must be destroyed or moved to a secure archive facility.
4. When confidential documents are transmitted off-campus, a signed receipt of delivery is required.
5. When confidential documents are transmitted via campus mail, the envelope must be sealed and stamped "Confidential."
6. When confidential documents need to be destroyed, a secure disposal service or a crosscut shredder must be used.

Requirements Specific to Printers and Fax Machines

1. Printers and fax machines that may print confidential information should be accessible only to authorized personnel.

    ◆ **Note**: Confidential documents can be sent to a printer or fax machine so long as the recipient or another authorized receiver is sure to be present at the time of printing.

POLICY 5.10

Information Security

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—BASELINE IT REQUIREMENTS

Introduction

To safeguard the university's information and information technology (IT) resources, Weill Cornell Medicine (WCM) requires community member to adhere to the following practices. These requirements apply to any system that is (a) used to conduct university business, and/or (b) connected to the WCM campus networks (including equipment not owned by WCM).

Any item labeled as a "**Suggestion**:" reflects a beneficial security practice that should be followed, if possible.

Baseline Requirements for All Computers

1. Keep all relevant operating system, server, and application software up-to-date (patched).
   - All tagged computers running the Windows operating system that are part of the WCM domain[1] are patched automatically by the Information Technologies and Services department (ITS). Users who use these systems do not need to take any further action to install patches.
   - Apple Macintosh, Linux, and other computers that do not run the Windows operating system must be patched on a regular basis, at least monthly. These systems will not be patched automatically by ITS.
     - Some systems, such as Picture Archiving and Communication Systems (PACS), run operating systems that cannot be patched, either because of age or because the patches affect application stability. These systems should either be disconnected from the network or placed on a non-routable network that is blocked from both the rest of the WCM network and the Internet. Contact ITS at support@med.cornell.edu to get more information on this type of network configuration.
2. User privileges must be configured as low as possible while still meeting business needs. Consistent or regular use of the administrator or root account is rarely appropriate.
3. Ensure all accounts have passwords that contain at least 1 uppercase character, 1 lowercase character, and 1 number. Passwords cannot exactly match a word in

[1] The WCM domain is a technical term that denotes membership within a central directory of systems maintained by the Information Technologies and Services (ITS) department. Contact the ITS help desk at support@med.cornell.edu to determine if your computer is in the WCM domain.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—BASELINE IT REQUIREMENTS, continued

the dictionary, and they cannot be your center-wide ID (CWID). Sharing of individually assigned CWIDs or passwords not allowed under any circumstance.

4. Transmission of passwords must be encrypted. Any ITS-managed system that requires password transmission uses encrypted protocols in order to do so.
5. Antivirus and antimalware software are automatically installed and managed by ITS on all tagged computers running the Windows operating system that are part of the WCM domain. Users are not permitted to disable or remove antivirus or antimalware software without the express permission of ITS.
6. To the extent viable products are available, other operating systems such as OS X and Linux should have antivirus and antimalware software installed, as well.

Baseline Requirements Specific to Desktops and Laptops

1. All local shares and other mechanisms for file access must be password protected.
   - This requirement forbids "open shares" (unauthenticated read/write access), "drop folders" (unauthenticated write-only access) and "public folders" (unauthenticated read-only access) on an individual's system.

     ◆**Suggestion:** Use an ITS-managed file share instead of local shares. Contact ITS to setup a departmental file server. All ITS-managed file shares are password protected.
2. If multiple individuals use a system, each should have his or her own login account, or the system should be restored to a known, clean state prior to each individual use. This also applies to "loaner" computers.
   - If a system must use a shared account, contact ITS to create a specially secured account for this purpose. Where a shared account is necessary, maintain a local inventory of who has access to the account.
   - Change the password for any shared account when there is any change in associated personnel or access requirements.
   - Laptops must use password protected screen savers that start after, at minimum, 30 minutes of inactivity.

Baseline Requirements Specific to Application and File Servers

1. Services that are not required to achieve the business purpose or function of the system must be disabled. Examples of unnecessary services include, but are not limited to, FTP, Telnet, SMTP, Web services, etc.
2. Change any passwords with default values set by the vendor. Passwords must contain at least 1 uppercase character, 1 lowercase character, and 1 number. Passwords cannot exactly match a word in the dictionary, and they cannot be your CWID.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—BASELINE IT REQUIREMENTS, continued

Baseline Requirements Specific to Public Workstations and Kiosks

1. Such systems must display an appropriate logon banner or bear signage with the following information:
   - A statement about responsible use
   - A warning about using the system for personal or sensitive information
   - A reminder to logout and/or clear any active credentials
2. No local file shares permitted.
3. If a user needs system privileges (ability to write files), then the computer must be restored to a known, clean state between individual sessions.
4. Visually inspect such systems regularly, at the very least on a quarterly basis, to see if physical security has been compromised.

Network Security

1. Implement packet filtering on networks with servers.

   Packet filtering should be used to limit network access to servers, computers, and other critical resources. Packet filtering is used on all ITS-managed data networks.

POLICY 5.10

Information Security

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION

Introduction

To better safeguard the university's institutional information, the following practices for electronic transmission and storage of confidential information must be followed.

◆**Note:** These requirements are in addition to those outlined in the Procedures, Weill-Cornell Campus Units—Baseline IT Security Requirements section of this policy.

Information Classification

This policy establishes three institutional information security classifications:

1. Confidential
2. Restricted
3. Public

Unless otherwise classified, all information used in the conduct of university business is restricted. Institutional information that has been explicitly made available to the public, with no authentication required for network access, is public.

Confidential data includes, without limitation, the following:

a. Patient billing or medical records (in any electronic form, including but not limited to databases, spreadsheets, audio/video recordings, transcripts, etc.), including data covered by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).
b. Student records, including those protected under the Family Education Rights and Privacy Act (FERPA).
c. Financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA), and credit card numbers.
d. Employment records, including pay, benefits, personnel evaluations, and other staff records.
e. Research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 46 CFR 101 et seq.).
f. Social Security numbers.

This set may expand based on future regulatory requirements or designations made by WCM.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

Please note that some data elements classified as confidential information are subject to legal or regulatory requirements that go beyond those given here. Such requirements for regulated information must be fulfilled, along with these Cornell requirements. In particular, credit card numbers and how the university handles credit card transactions are subject to the Payment Card Industry Data Security Standard (PCI DSS). For more information, see University Policy 3.17, Accepting Credit Cards to Conduct University Business.

Systems Subject to These Requirements

These requirements apply to any systems that create, store, or receive confidential information, both on- or off-campus, and even if not WCM-owned.

For the purposes of this policy, a system is considered to be creating, storing, or receiving confidential information when such information is stored locally on the system, or when the system is used to access such information stored on network volumes or file systems.

A system used to access confidential information via an application, including database access, would *also* be viewed as creating, sending, or receiving such information.

Encryption Standards

This procedure lists recommendations for encryption under multiple headings. Encryption of desktops and laptops must be done using the Information Technologies and Services department (ITS)-managed encryption service (see its.weill.cornell.edu/security-and-privacy/safeguard-your-data). Users that need to store confidential data on USB drives must use encrypted drives. WCM strongly recommends the use of Iron Key drives, which can be purchased through CDWG. Contact support@med.cornell.edu for more information.

Confidential Information—Requirements for All Computers

1. Keep all relevant operating system, server and application software up to date.
   - As described above, this is done automatically for all Windows workstations and laptops that are part of the ITS-managed domain.
   - Users and administrators of workstations, laptops, servers, mobile devices, and network devices that are not part of the ITS-managed domain are responsible for updating operating system, server, and application software at least monthly.
2. Disabling unnecessary services
   - Disable services that are not required to achieve the business purpose or function of the system. Examples of unnecessary services include, but are not limited to SSH, FTP, Telnet, SMTP, Web services, etc.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

3. Protection from malicious software.
   - Systems with confidential data must be tagged with an ITS tag, which ensures ITS-offered protections from malicious software are installed. These protections include, but are not limited to, antivirus software, personal firewall software, and automated installation of security patches.
   - Change any passwords with default values set by the vendor. Passwords must contain at least 1 uppercase character, 1 lowercase character, and 1 number. Passwords cannot exactly match a word in the dictionary, and they cannot be your center-wide ID (CWID).
4. Confidential information and information that is being made available for public access may not be on the same system.
   - An open website, i.e., one that does not require authentication for access, may not be run on a system holding confidential information.
   - Peer-to-peer (P2P) file-sharing software may not be run on a system holding confidential information.
   - Confidential information and information available for public access may reside in different virtual machines running on the same system, as long as the host system and the host operating systems on both meet all the requirements for a file or application server holding confidential information.
5. Activate operating system and, where possible, application logging, with logs that are retained for at least 90 days. At a minimum, the following must be logged:
   - Access to all audit logs.
   - Access to confidential information.
   - Failed access attempts.
6. An individual's access to a store of confidential information should be via an account assigned for the sole use of that individual.

Confidential Information—Requirements Specific to Desktops and Laptops

1. When practical, the account used for daily operations must be configured not to allow software installs, or must require the account password for an install.
2. Confidential information stored locally on a system must be removed when no longer needed for an operational reason.
3. Confidential information must be encrypted using the ITS-managed encryption service on all of the following:
   - On all tagged laptops (see WCM Policy 11.6, Laptop Encryption).

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

- Any system that, even on a temporary basis, is not located on one of the Cornell campuses or some other formal university location.

4. Confidential information must additionally be encrypted on all of the following:
   - Any other mobile device, including flash/USB drives, PDAs, smart phones, and media.
   - Any other WCM system that is not physically secured or in a secure location accessible only to authorized WCM personnel.
5. While Microsoft Office 2007 and higher includes a facility for appropriately strong encryption of documents, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.
6. Users are expected to make reasonable efforts (e.g. by one more of the following: locking, logging out, using privacy screens, using logons with limited access, etc.) to restrict the viewable access to workstations when they will be out of viewable range of those workstations.
7. After a predetermined amount of inactivity, at most 120 minutes, workstations must automatically lock or log off. Electronic access from workstations to Confidential Systems should be automatically terminated after a predetermined period of activity.

Confidential Information—Requirements Specific to Facilities

1. Facilities containing confidential systems must be access-controlled. Physical access controls must be logged and audited at least every 12 months, and must include 1 or more of the following: multi-factor authentication (e.g., token and pin number), key-card access, biometric access controls.
2. Facility environmental controls that make reasonable attempts to protect against power outages, fire, water damage, temperature extremes, and other environmental hazards.

Confidential Information—Requirements Specific to Servers

1. Confidential information should be removed from file servers when it is no longer needed on an operational basis. To the extent feasible, this also applies to confidential information stored in databases and other application frameworks.
2. Backup tapes containing confidential data must be encrypted using contemporary encryption standards.
3. Dual-factor authentication with periodically (at most 60-seconds) changing pass codes must be used at least once to authenticate to these systems before root/administrator privileges are invoked.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

- All ITS-managed systems must use the RSA SecureID system for root/administer access to these systems.
- Authenticating to one system using dual-factor, plus periodically changing passwords before then authenticating to another system with single-factor (password only), is supported only if root/administrator access to the second system is available only to users who have successfully dual-factor authenticated (plus periodically changing password) to the first system.

Confidential Information—Requirements Specific to Public Workstations and Kiosks

Such systems may never be used for creating, receiving, storing, or transmitting confidential information. This does not include patient examination or other similar rooms.

Confidential Information—Network Security

1. The edge ACL or other packet-filtering mechanism on any subnet with systems housing confidential information must employ a default-deny strategy that prohibits unnecessary connections and that strictly limits access to the systems with confidential information.
   - Where internet connectivity is not needed, put the system into a non-routable IP space.
2. Any system storing, sending, or receiving confidential information that uses a campus wireless connection must use either the NewYork-Presbyterian Hospital or the WCM secure wireless services.
3. Any remote, off-campus access to a system containing confidential information must either use the ITS-managed client or Web VPN, or use an encrypted communication protocol such as ssh, sftp, SSL, or TLS.
4. Any transmission of confidential data over public networks must be encrypted.

Confidential Information—Messaging Requirements

1. Confidential information may be sent via the ITS-managed e-mail system *only if* every recipient e-mail address ends in med.cornell.edu or nyp.org.
2. Anyone who may send or receive confidential information in e-mail may not use e-mail forwarding to automatically forward messages to an outside service such as Gmail or Hotmail.
3. Confidential information may not be sent using e-mail to recipients whose e-mail addresses do not end in "med.cornell.edu" or "nyp.org."

   ◆**Note**: This applies to information either in the body text or in an attachment.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

4. Use the WCM File Transfer Service (transfer.med.cornell.edu) to exchange confidential information with users whose e-mail addresses do not end in "med.cornell.edu" or "nyp.org."
5. Unless the communicating parties are certain that communications are protected effectively against unauthorized use or disclosure, such as through the WCM encrypted instant messaging service (talk.med.cornell.edu), confidential data may not be sent through instant messaging or other similar technologies.
6. Confidential information must be encrypted when it is accessed via the Web.
7. If passwords that grant access to confidential information are stored on a networked device, they must be encrypted. While Microsoft Office 2007 and higher includes a facility for appropriately strong encryption, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.

Process and Documentation Requirements

ITS will provide specific guidelines for fulfilling the following items:

1. Define and document incident response and escalation procedures for a potential loss of confidential information.
2. Provide end-user incident response and escalation training.
3. When granting an external entity access to confidential information, that entity must sign a WCM Business Associates Agreement (available by calling (212) 746-1179) and provide documentation of the following:
   - How this information will be transmitted, processed, stored and secured
   - How such information is monitored and what incident response mechanisms are in place
   - The process for disposal of confidential information when no longer needed for legal, regulatory, or business needs
   - How local and university information retention guidelines are met

     ◆**Note**: This process needs to include an approach to information/media destruction.

PROCEDURES, WEILL-CORNELL CAMPUS UNITS—IT SECURITY REQUIREMENTS FOR CONFIDENTIAL INFORMATION, continued

Exceptions

For all computers or other IT resources that are not able to meet these security requirements, the following exception process must be followed:

1. IT resources that cannot meet the following requirements must be identified to the appropriate department. The department will look for alternate methods to address the risk in question. If an alternate security solution can be found to address the specific risk, an exception is not required.
2. If an alternate security solution cannot be found, the department should consult with ITS to determine a solution.

POLICY 5.10

Information Security

INDEX

INDEX, continued