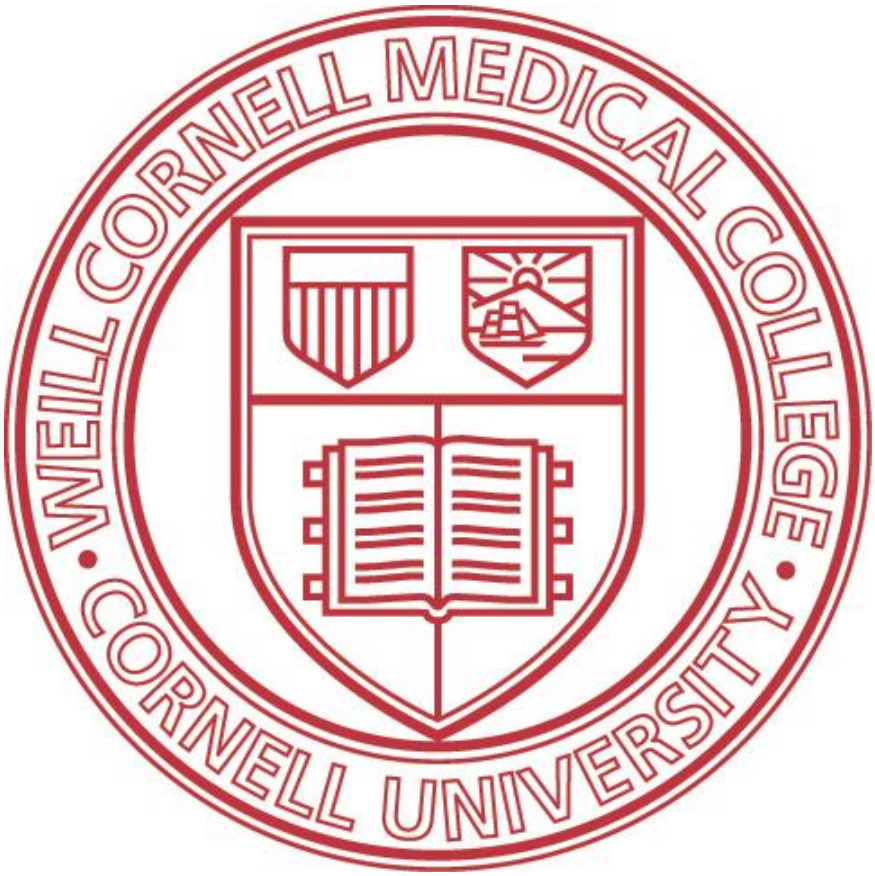

ITS Policy Library

11.11 - Requirements for Securing Information Systems

Information Technologies & Services

Responsible Executive:	Chief Information Officer, WCMC
Original Issued:	March 19, 2015
Last Updated:	March 21, 2016

Policy Statement

Information systems must be secured according to a set of standards and principles in order to prevent unauthorized access to Weill Cornell Medical College data and applications.

Reason for Policy

In order for Weill Cornell Medical College to allow information systems to reside on the Weill Cornell Medical College network, certain security protocols and controls must be implemented in order to mitigate the risk of a security breach or attack. This policy establishes a standard for securely configuring information systems residing on its network in order to ensure a hardened, tested, and baseline security configuration profile is employed across all information systems.

Entities Affected by this Policy

Weill Cornell Medical College and Graduate School of Medical Sciences

Who Should Read this Policy

All individuals responsible for configuring, maintaining, and monitoring information systems on the Weill Cornell Medical College network. Individuals may include Weill Cornell Medical College faculty, staff, vendors, contractors, or managed service providers.

Web Address of this Policy

http://weill.cornell.edu/its/policy/security/1111-requirements-for-securing-information-systems.html

Contacts

Direct any questions about this policy, 11.11 - Requirements for Securing Information Systems, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

Definitions

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

i)	ITS	Information Technologies & Services Department
ii)	WCMC	Weill Cornell Medical College
iii)	information system	A server or appliance (laptops/desktops excluded), whether physical or virtual, that contains, stores, or provides access to WCMC data and resides on the WCMC network; the system may also be installed and/or supported by an outside vendor

I. Principles

Weill Cornell Medical College mandates that its information systems are secured and hardened according to a set of controls and principles, based not only on the data residing on the system, but also on the type of access users have to the system. The controls below, though not exhaustive, are to be implemented based on the initial system risk assessment in order to achieve the appropriate level of security.

II. Roles and Responsibilities

The lifecycle of a system involves many teams within the Information Technologies & Services Department as well as external stakeholders. This section identifies general roles and responsibilities as it pertains to building, configuring, implementing, and maintaining an information system.

Section 2.01 **CHIEF INFORMATION OFFICER**

The Chief Information Officer, Curtis L. Cole (ccole), provides oversight to the policies and standards in accordance with applicable laws and standards to help the organization secure Weill Cornell Medical College data and information systems. The Chief Information Officer is responsible for establishing an appropriate level of visibility for these policies and information risk to the medical college.

Section 2.02 **ITS ASSOCIATE DIRECTORS**

The ITS Associate Directors are responsible for complying with security policies within ITS. The ITS Associate Directors manage and monitor information systems that support Weill Cornell Medical College's information security infrastructure, and are responsible for maintaining awareness of the security of the resources they manage by working with the ITS Security group, and assure that security related activities are well documented and completed in a consistent and auditable manner. As directed by senior management, the ITS Associate Directors are responsible for periodic reevaluation of current operational methods to identify possible areas for improvement in security. The Information Security Officer will evaluate security risks to new and existing systems with Associate Directors in accordance with this policy. ITS Associate Directors must assure that appropriate security controls are implemented commensurate with the acceptable level of risk.

Section 2.03 **INFORMATION SECURITY OFFICER**

The Information Security Officer, Brian J. Tschinkel (brt2008), is responsible for developing and implementing strategy for security compliance within the ITS department and serves as a liaison for regulatory compliance in the medical college. The Information Security Officer develops policies, standards, and guidelines for securing information systems. In addition, the Information Security Officer conducts risk assessments and analysis in accordance with applicable laws and

standards to help the organization secure Weill Cornell Medical College data and information systems. Risk findings, including non-compliant and vulnerable systems, may be reported to the Information Security Privacy & Advisory Committee (ISPAC). The Information Security Officer reserves the right to restrict access to vulnerable systems, in accordance with the Restricting Network Access for Information Systems policy. It is the Information Security Officer's responsibility to ensure that corrective active plans are completed and information system integrity is not compromised.

Section 2.04 **ADMINISTRATORS OF INFORMATION SYSTEMS**

Individuals who manage Weill Cornell Medical College's information systems are responsible for complying with policies that govern the security of the resources they manage. The Information Security Officer will establish protocols with the Systems Administrators and Systems Managers to ensure that appropriate security controls are implemented as specified in this document and related technical hardening guidelines. Systems Administrators and Systems Managers provide information to the Information Security Officer to facilitate risk assessment activities, and are responsible for implementing corrective actions as recommended. In addition, System Administrators and System Managers are responsible for maintaining sufficient documentation about system configuration, maintenance, and overall management of information systems.

In order to maintain a secure environment and to protect Weill Cornell Medical College data, ITS administrators who fail to maintain and/or neglect their information systems after notification or discovery of a significant threat or vulnerability may face disciplinary action up to and including termination of employment.

III. Securing the Information System

Section 3.01 **PLANNING AND RISK ASSESSMENT**

All new and existing systems, including virtual or physical appliances supplied by a vendor, must undergo an initial risk assessment in order to determine the network zone placement and inherent risk of the system. The risk assessment is a process that takes into consideration several legal and regulatory controls as well as the intended use and access of the system. The results of the risk assessment are then used to evaluate risk and recommend a set of controls that should be implemented to ensure the appropriate level of security. Systems that are deemed high risk or contain sensitive information may require an in-depth assessment by the Information Security Officer in order for the system to be certified for use.

IV. Securing the Operating System

This section applies to controls necessary for securing the base configuration of the system, typically at an operating system-level. A support agreement must be in place with any system

installed and/or supported by an outside vendor to ensure compliance with the following security requirements.

Section 4.01 **PATCH AND UPGRADE THE OPERATING SYSTEM**

All systems must be configured with a supported version of the operating system. Operating systems that are deemed “end of life” or “out of support” by the vendor shall not be used, unless a specific exemption has been approved by ITS. In order to maintain compliance and mitigate risks, all systems must be patched on a monthly basis in accordance with the WCMC ITS patch management cycle.

All systems must undergo a routine vulnerability scan. Any vulnerabilities detected from the scan shall be identified by ITS Security and mitigated or remediated as soon as possible. Critical systems, including those that are publicly facing or are accessible via the internet, must have all vulnerabilities remediated with a permanent patch or a temporary fix to lessen the attack surface.

During preparation of a new system, the system shall remain in an isolated network until the system is deemed to be adequately protected by ITS Security. All patches shall be tested prior to deployment on production systems as patches that are installed automatically without testing could render a system inaccessible or make system data irrecoverable.

Section 4.02 **HARDEN AND CONFIGURE THE OPERATING SYSTEM**

System administrators are responsible for the secure configuration of the operating system. Systems shall be configured to offer the least functionality possible in order to limit the attack surface and lessen the number of potential vulnerabilities that may exist or appear on the system.

i) Remove or Disable Unnecessary Services, Applications, and Network Protocols

   a) Where possible, all systems should be a dedicated, single-host meant to run one application (or one set of tightly-related or dependent applications). All services, applications, and network protocols that are not required for the system shall be removed or disabled. When available, “core” or “lightweight” versions of the operating system shall be used in order to prevent installation of unnecessary components. The following list of services and applications, while not exhaustive, shall be removed or disabled if not necessary:

      i) File and printer sharing services

      ii) Wireless networking services

      iii) Remote control and remote access programs

      iv) Directory services

v) Web servers and services

vi) Email services

vii) Language compilers

viii) System development tools

ix) System and network management tools and utilities

b) By reducing the number of running services and applications on a system, the attack surface is lessened, system logs are reduced, and the likelihood of a compromise is generally lower.

ii) Configure System and Service Authentication

a) All systems shall be configured to authenticate with the centrally-managed authentication platforms. Web-based systems shall be configured to use the SAML 2.0 protocol (or the CAS 2.0 or 3.0 protocols if SAML 2.0 is not feasible), and must be performed over a secure connection. Non web-based systems shall be configured to use Active Directory or Lightweight Directory Access Protocol, and must be performed over a secure connection. Local system accounts shall be limited in quantity and restricted for use by system administrators in an emergency, such as when web or directory authentication is inoperable. In addition, the following precautions should be followed:

i) Remove or disable unneeded default accounts

ii) Disable non-interactive accounts

iii) Assign access rights to user groups instead of individual accounts

iv) Configure automated time synchronization (required for web-based authentication)

v) Ensure account passwords adhere to the WCMC ITS Password Policy & Guidelines document

vi) Configure systems to prevent brute force attacks or password guessing

vii) Implement multi-factor authentication for critical, high risk, or public-facing systems

Section 4.03 **CONFIGURE ADDITIONAL SECURITY CONTROLS**

In addition to the system hardening controls already outlined, it is imperative to configure additional security controls to implement a defense-in-depth strategy:

- Install the centrally-managed anti-malware software and ensure it is updated properly
- Ensure the system is detected by the centrally-managed intrusion detection software
- Install a host-based intrusion detection/prevention software agent
- Enable the local host-based firewall for high risk systems
- Use a web-application firewall for high risk or public-facing systems, where applicable
- Install the change management and change detection agent
- Configure logging to store logs on the centrally-managed log management server
- Ensure encryption is implemented for data in transit between information systems
- Where possible, implement full-disk encryption for systems storing confidential data

Section 4.04 **SECURITY TEST THE OPERATING SYSTEM**

In order to test the secure configuration of the operating system, the system needs to be scanned by the vulnerability management software. A report should show no open vulnerabilities and any vulnerabilities that cannot be remediated must be documented as a temporary exception and mitigating security controls shall be implemented.

V. Securing the System Software

The software being installed on the system shall be secured in the same manner as described in *Securing the Operating System* above. All software shall be updated to a vendor- or ITS-supported version with the latest security patches to minimize the threat landscape.

In addition to the controls in the previous section, system software should not have excessive access to the operating system where a vulnerability to the software could extrapolate data or manipulate critical files that reside on the operating system.

VI. Maintaining the System Security

Section 6.01 **LOGGING**

The ability to collect accurate and detailed system and application logs is vital for investigations, troubleshooting, and support of systems and software. All systems shall be setup to log account logins (both successes and failures), account login types, access to files or shares, and changes to those files or shares. Additional system utilization and application logs should be configured as well.

All logs for critical, high risk, or public-facing systems should be sent to the centralized logging server for isolation and protection from any potential attacks to the host system. To ensure accuracy and synchronization, all systems shall be configured with a synchronized time server (ntp.med.cornell.edu).

Logs shall be maintained in accordance with the centralized logging server storage levels. Logs may need to be retrieved for legal and regulatory requirements, incident response initiatives, or other diagnostic and troubleshooting purposes.

Section 6.02 **DATA LOSS PREVENTION**

All members of the Weill Cornell Medical College community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college. All systems containing WCMC confidential data (as classified in the ITS policy, 11.03 – Data Classification) shall be configured to be scanned regularly by the centralized data loss prevention system.

Section 6.03 **SERVER BACKUP PROCEDURES**

Systems shall be backed up based on risk level, criticality of the system, and availability requirements. Full, incremental, and differential backups shall exist in accordance with the system type and existing backup policies. Backups for critical systems should be stored offsite in a secure location.

Section 6.04 **MAINTAINING A TEST SERVER**

A test or development server, where feasible, shall be maintained for critical, high risk, or public-facing production systems to limit the impact of patches and other system changes. The development system should have hardware and software configurations that are identical to the production system. System changes, patches, and other deployments should be tested on the development server prior to being promoted to the production environment.

Section 6.05 **CONFIGURATION CHANGE CONTROL MANAGEMENT**

All system configurations and changes shall be filed in accordance with the ITS Change Management policy. The change management agent software shall be installed on all systems and configured accordingly based on the system and applications present.

VII. Related Documents

The following documents are also relevant to this policy:

i) 11.12 – Restricting Network Access for Insecure Systems

ii) 12.02 – Physical Security

iii) ITS Change Management

iv) Password Policy & Guidelines

v) Vulnerability Management Process

vi) Technology-specific Hardening Guidelines