Weill Cornell Medicine

11.11

Requirements for Securing Systems

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: March 19, 2015
Last Updated: September 12, 2023
Last Reviewed: September 12, 2023

Contents

Policy Statement

Weill Cornell Medicine mandates that its information systems and applications (“systems”) are secured and hardened according to industry best practices in order to maintain a reasonable level of security commensurate to the anticipated risk, and to prevent insecure access to Weill Cornell Medicine data.

Reason for Policy

In order for Weill Cornell Medicine systems to interact with Weill Cornell Medicine data or networks, certain security controls must be implemented to manage the risk of a security incident. This policy establishes a standard to ensure the use of securely configured systems.

Entities Affected by this Policy

All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources. All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

https://its.weill.cornell.edu/policies

Contacts

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

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

1. Roles and Responsibilities

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

1.01 Chief Information Officer

The Chief Information Officer provides oversight to policies and standards in accordance with applicable laws and best practices to help better secure Weill Cornell Medicine data and systems. The Chief Information Officer is responsible for establishing an appropriate level of visibility for these policies and information risk to the medical college.

1.02 Chief Information Security Officer

The Chief Information Security Officer is responsible for developing and implementing ITS security strategy and serves as a liaison for regulatory compliance in the medical college. The Chief Information Security Officer oversees and actively participates in the development of policies, standards, and guidelines for securing systems. In addition, the Chief Information Security Officer conducts risk assessments and analysis in accordance with applicable laws and standards to help better secure Weill Cornell Medicine data and systems. Risk findings, including non-compliant or vulnerable systems, may be reported to the Information Security Privacy & Advisory Committee (ISPAC). In their sole discretion, the Chief Information Security Officer reserves the right to restrict and/or delegate the right to restrict network or user access to non-compliant or vulnerable systems in accordance with ITS policy 11.12 – Restricting Access for Insecure Systems. It is the Chief Information Security Officer's responsibility to follow up with system administrators to ensure that corrective action plans are completed and system or data integrity is not compromised.

1.03 ITS Leadership

ITS Leadership—such as assistant directors, associate directors, and directors—are responsible for ensuring their teams comply with ITS security policies. ITS Leadership oversee teams that manage and monitor systems supporting Weill Cornell Medicine's security infrastructure, are responsible for maintaining awareness of the security of their resources, and ensure that security-related activities are well documented and completed in a consistent and auditable manner. ITS Leadership are responsible for ongoing reevaluation of current operational processes to identify possible areas for improvement in security. The Chief Information Security Officer will evaluate security risk to new and existing systems with ITS Leadership in accordance with this policy. ITS Leadership must strive to ensure that appropriate security controls are implemented commensurate with the acceptable level of risk.

1.04 Administrators of Systems

Individuals who administer Weill Cornell Medicine's systems are responsible for complying with policies that govern the security of those resources. Administrators must ensure that appropriate security controls are implemented as specified in Weill Cornell Medicine policies and standards. Administrators should provide information to the Chief Information Security Officer to facilitate risk assessment activities and are responsible for timely implementing corrective actions as recommended by the ITS Security team. In addition, Administrators are responsible for maintaining sufficient documentation about system configuration, maintenance, and overall management of their respective systems.

In order to maintain a reasonably secure environment and to protect Weill Cornell Medicine systems and data, Administrators who fail to maintain the security of and/or neglect their systems after notification or discovery of a significant risk (i.e., a zero-day threat or vulnerability) may face disciplinary action up to and including termination of employment.

2. Securing the System

2.01 Planning and Risk Assessment

All new and existing systems, including virtual or physical appliances supplied by a vendor, must undergo an initial intake 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 inform 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 Chief Information Security Officer for the system to be certified for use.

3. Securing the Operating System

This section applies to controls necessary for securing the base configuration of operating systems. A support agreement must be in place with any system to ensure compliance with the following security requirements.

3.01 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 variance is on file pursuant to ITS policy 11.20 – Variances. In order to maintain compliance and mitigate risk, all operating systems must have security patches installed as defined in ITS policy 11.12 – Restricting Access for Insecure Systems.

All systems must undergo a routine vulnerability scan. Detected vulnerabilities shall be managed as defined in ITS policy 11.12 – Restricting Access for Insecure Systems.

New systems should not be placed into production until all relevant security patches have been installed. All patches should be tested prior to deployment on production systems as patches that are installed without testing could have an undesirable impact or make data irrecoverable.

3.02 Harden and Configure the Operating System

Administrators are responsible for the secure configuration of operating systems. Systems shall be configured to offer the least functionality needed in order to limit the attack surface and lessen the number of potential vulnerabilities.

3.02.1 Hardening Standards

The use of industry standard hardening and secure configuration recommendations, such as those from the Center for Internet Security, shall be utilized.

Remove or Disable Unnecessary Services, Applications, and Network Protocols

Where possible, all systems should be a dedicated, single-use host running one application or one set of tightly-integrated or dependent applications. All services, applications, network protocols, etc. that are not required 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:

- File and printer sharing services
- Wireless networking services
- Remote control and remote access programs
- Directory services
- Web servers and services
- Email services
- Language compilers
- System development tools

System and Network Management Tools and Utilities

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

Configure System and Service Authentication

All systems shall be configured to authenticate with centrally managed authentication platforms. Systems shall be configured to use the latest Security Assertion Markup Language (SAML) protocols. In the event SAML is not feasible, the latest Active Directory, Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS), or OAuth protocols can be used. All authentication must be performed over a secure connection. Local accounts shall only be created and used if centralized directory accounts are not technically possible, shall be limited in quantity to those only absolutely necessary, and shall comply with the controls identified in ITS policy 11.15 – Password Policy and Guidelines. Local accounts granting elevated privileges shall be restricted for use only by Administrators in an emergency, such as when web or centralized directory authentication is inoperable, and passwords must be securely stored in the sanctioned privileged access management system.

In addition, the following precautions should be followed for system and service authentication:

- Remove or disable unneeded default accounts,
- Disable non-interactive accounts,
- Assign access rights to user groups instead of individual accounts,
- Configure automated time synchronization (required for web-based authentication),
- Ensure compliance with ITS policies 11.15 – Password Policy and 11.17 – Identity and Access Management,
- Configure systems to prevent brute force attacks or password guessing,
- Implement multi-factor authentication for critical, high risk, or public-facing systems, and
- Implement other precautions as required by Weill Cornell Medicine policies, standards, or ITS Security personnel.

3.03 Configure Additional Security Controls

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

- Install Weill Cornell Medicine's centrally managed anti-malware software and ensure it is updated properly,
- Ensure the system is monitored by Weill Cornell Medicine's centrally managed intrusion detection software,
- Enable the local host-based firewall,
- Use Weill Cornell Medicine's web application firewall for high risk or public-facing systems, where applicable,
- Install Weill Cornell Medicine's centrally managed system management agent,
- Configure logging to store logs on the centrally managed log management server, where applicable,
- Ensure encryption is implemented for data in transit between systems,
- Implement full-disk encryption for systems storing high risk data, where applicable, and
- Implement other controls as required by Weill Cornell Medicine policies, standards, or ITS Security personnel.

3.04 Security Test the Operating System

In order to test the hardening and secure configuration of the operating system, the system needs to be scanned by the vulnerability management software on a routine basis. A report should show no unmanaged vulnerabilities pursuant to ITS policy 11.12 – Restricting Access for Insecure Systems, and any vulnerabilities that cannot be appropriately managed must follow the variance process defined in ITS policy 11.20 – Variances.

4. 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, unless absolutely needed for operation, system software should not run with administrative privileges.

5. Maintaining the System Security

5.01 Logging

The ability to collect accurate and detailed system application and security logs is vital for investigations, troubleshooting, and support of systems and software. At a minimum, all systems shall be configured to log account logins (both successes and failures), account login types, access to high risk files or shares, and changes to those high risk files or shares. Additional logs should be configured as needed.

All logs for high risk systems should be sent to the centrally managed log management server for isolation and protection from potential attacks. To ensure accuracy and synchronization, all logging shall be configured with a synchronized time server (e.g., ntp.med.cornell.edu).

Logs must be retained for a minimum of 180 days and be available quickly for analysis. Logs may need to be retrieved for legal and regulatory requirements, incident response initiatives, or other diagnostic and troubleshooting purposes.

5.02 Data Loss Prevention

All members of the Weill Cornell Medicine community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college pursuant to ITS policy 11.03 – Data Classification. Email messages and cloud storage services containing high risk data shall be configured to be scanned and managed regularly by the centralized data loss prevention system.

5.03 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 high risk systems should be securely stored offsite.

5.04 Maintaining Development and/or Test Environments

Development and/or test systems, where feasible, shall be maintained for high risk systems to help limit the impact of patches and other changes. The development and/or test systems should have hardware and software configurations that are as identical to production systems as possible. System changes, patches, and other deployments should be tested on development and/or test systems prior to being promoted to the production environment. Development and/or test systems should not store identifiable high risk data to the maximum extent possible.

5.05 Configuration Change Control Management

All system configurations and changes shall be filed in accordance with ITS change management policies and procedures. The centrally managed system management agent shall be installed on all systems and configured accordingly based on the system and applications present.

Revision History:

Date	Author	Revision
March 29, 2015	Brian J. Tschinkel	Policy created
March 21, 2016	Brian J. Tschinkel	Updated authentication and time synchronization parameters
August 12, 2023	Justin Barber	Revised policy statement and principles, roles, hardening standards
September 12, 2023	Brian J. Tschinkel	Updated policy template and language for branding