| Weill Cornell Medicine | WCM Administrative Policy and Procedure | |
|---|---|---|
| | **Policy Title** | Requirements for Securing Systems |
| | **Policy Number** | ITS-500.11 |
| | **Department/Office** | ITS Security |
| | **Effective Date** | March 19, 2015 |
| | **Last Reviewed** | September 24, 2024 |
| | **Approved By** | WCM-Executive Policy Review Group |
| | **Approval Date** | October 21, 2025 |

## Purpose

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

## Scope

This policy applies to all WCM Workforce Members who utilize WCM information technology resources as well as those responsible for managing and safeguarding WCM data.

## Policy

WCM 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 help prevent insecure access to WCM data.

## Definitions

**Workforce Members**: Any Faculty; Staff; Students; Volunteers; Trainees; and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether or not they are paid by WCM.

## Procedure

### 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 they pertain to building, implementing, configuring, 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 WCM 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 the designated HIPAA security officer and is responsible for developing and implementing ITS Security strategy and serves as a liaison for security compliance. 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 oversees the security risk assessment process in accordance with applicable laws and standards to help better secure WCM 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 500.12 – *Restricting Access for Insecure Systems*. It is the Chief Information Security Officer's responsibility to ensure that corrective action plans are completed, and system or data integrity is not subject to unacceptable risk.

## 1.03 ITS Leadership

ITS Leadership members—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 WCM's security and ITS 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 members are responsible for ongoing reevaluation of current operational processes to identify possible areas for security improvement. ITS Leadership will evaluate security risk to new and existing systems with the Chief Information Security Officer 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 WCM's systems are responsible for complying with applicable security 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 WCM data and systems, 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 appropriately manage the risk. 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 ITS Security Team.

# 3. Securing the Operating System

This section applies to controls necessary for securing the base configuration of operating systems.

## 3.01 Patch and Upgrade the Operating System

All systems must be configured with a supported version of the operating system and have security patches installed as defined in ITS policy 500.12 – *Restricting Access for Insecure Systems*. 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 500.20 – *Variances*.

New systems should not be placed into production or be accessible from the public internet 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 vendor or 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 to prevent installation of unnecessary components. 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. 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 (e.g. RDP, SSH)
- Directory services
- Web servers and services
- Email services
- Language compilers
- System development tools

***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 500.15 – Password Policy. 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 500.15 – *Password Policy* and 500.17 – *Identity and Access Management,*
- Configure systems to prevent or slow brute force attacks or password guessing,
- Implement multi-factor authentication, and
- Implement other precautions as required by WCM 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 WCM's centrally managed anti-malware software and ensure it is updated properly,
- Ensure the system is monitored by WCM's centrally managed intrusion detection system,
- Enable the local host-based firewall,
- Use WCM's web application firewall for High Risk or public-facing systems, where applicable,
- Install WCM'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 whole disk encryption for all systems, where applicable, and
- Implement other controls as required by WCM policies, standards, or ITS Security personnel.

## 3.04 Scan the Operating System for Vulnerabilities

In order to test the hardening and secure configuration of the operating system, all systems must be scanned by vulnerability management software on a routine basis. A report should show no unmanaged vulnerabilities pursuant to ITS policy 500.12 – *Restricting Access for Insecure Systems*, and any vulnerabilities that cannot be appropriately managed must follow the variance process defined in ITS policy 500.20 – *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.

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. All systems should, at a minimum, be configured to log system, security, and application-specific events—especially those involving access to or modifications of High Risk files or shared resources. Additional logs should be configured as needed.

All available logs across systems should be retained for a minimum of 180 days and be immediately available 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 WCM 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 500.03 – *Data Classification*. Email messages and cloud storage services containing High Risk data should be configured to be scanned and managed regularly by the centralized data loss prevention system.

## 5.03 Data Backup Procedures

Data should be backed up based on risk level, criticality, and availability requirements. Backups for High Risk data should have at least one offline securely stored copy. All backups should be regularly tested as part of the disaster recovery plan.

## 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 the same security controls as if they were a production system. System changes, patches, and other deployments should be tested on development and/or test systems prior to being promoted to production. 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 managed in accordance with ITS change management policies and procedures. The centrally managed system management agent should be installed on all systems and configured accordingly based on the system and applications present unless a specific variance is on file pursuant to ITS policy 500.20 – *Variances.*

## Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

## Contact Information

Direct any questions about this policy, 500.11 – *Requirements for Securing Systems*, to the Office of the Chief Information Security Officer, using one of the methods below:

Office: (646) 962-3609
Email: ciso@med.cornell.edu

## References

- WCM Policy ITS-500.03 – Data Classification
- WCM Policy ITS-500.12 – Restricting Access for Insecure Systems
- WCM Policy ITS-500.15 – Password Policy
- WCM Policy ITS-500.17 – Identity and Access Management,
- WCM Policy ITS-500.20 – Variances

## Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on September 18, 2025.
- WCM-Executive Policy Review Group (WCM-EPRG) on October 21, 2025.

## Version History

| Date | Author | Revisions |
|---|---|---|
| 03/29/2015 | Brian J. Tschinkel | Policy created |
| 03/21/2016 | Brian J. Tschinkel | Updated authentication and time synchronization parameters |
| 08/12/2023 | Justin Barber | Revised policy statement and principles, roles, hardening standards |
| 09/12/2023 | Brian J. Tschinkel | Updated policy template and language for branding |
| 09/24/2024 | Tom Horton | Updated CISO contact information and other minor language changes, added new template |
| 10/21/2025 | Office of the CISO | Updated policy template and other minor language changes, updated logging section to align with Cornell policy |

## Appendix

N/A