Weill Cornell Medicine	WCM Administrative Policy and Procedure	
	Policy Title	Restricting Access for Insecure Systems
	Policy Number	ITS-500.12
	Department/Office	ITS Security
	Effective Date	March 19, 2015
	Last Reviewed	September 11, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	October 21, 2025

Purpose

Information technology and data constitute valuable Weill Cornell Medicine (WCM) assets. Depending on their classification, these assets may be subject to state and federal regulations. This policy provides a framework for facilitating compliance with applicable regulations and adherence to established security best practices.

Scope

This policy applies to all WCM Workforce Members who use WCM information technology resources or are responsible for managing and safeguarding WCM data.

Policy

Information Technologies & Services Department ("ITS") is responsible for evaluating and managing threats that pose an unacceptable risk to WCM information systems and applications ("systems"), networks, or data. If a system is deemed vulnerable to a threat or at risk of compromise, the Chief Information Security Officer (CISO) or their delegate may block tits access to other systems, networks, and data. This policy specifies the standards and thresholds used to assess risk and determine when access restrictions are necessary.

Definitions

Common Vulnerability Scoring System (CVSS): Standardized framework for evaluating and ranking the severity of computer system vulnerabilities.

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

Pursuant to ITS policy 500.11 – *Requirements for Securing Systems*, the CISO has the authority to evaluate the seriousness and urgency of any threat to WCM systems, networks, and data. Actions such as powering off systems or restricting/ network access are based on a risk assessment that considers both the likelihood and impact of compromise. Relevant sources, such as vulnerability reports and industry alerts, should be reviewed and considered before any action is taken on a system.

Any findings and appropriate action will be communicated to the appropriate Administrators. All systems must be configured in accordance with the 500.11 – *Requirements for Securing Systems* policy. Any system

which cannot meet the minimum security requirements set forth in ITS policy must submit a variance request pursuant to ITS policy 500.20 – *Variances*.

Threats and vulnerabilities have been categorized into different risk ratings that dictate remediation timeframes: critical, high, medium, and low.

1.01 Critical

A **Critical Risk** rating has a **very significant** likelihood or impact of compromise to systems, networks, or data. Threats or vulnerabilities in this category must be appropriately managed within 24 hours, or relevant systems or networks may be shut off or disconnected with little or no prior notice.

By way of example, a **Critical Risk** rating may consist of any of the following:

- A targeted attack is suspected,
- A system is suspected to have been compromised by an unauthorized party,
- Malware is suspected of having infected a system or is at risk of spreading to other systems,
- A data compromise or breach is suspected,
- A vulnerability scanner has reported a “critical” vulnerability on a system,
- Passwords or account credentials are suspected to have been compromised, obtained, or used in violation of policy,
- A default password is blank or has not been changed,
- An event is suspected to have led to reputational, legal, or financial liability for WCM, or
- A vulnerability with a critical Common Vulnerability Scoring System (CVSS) score.

1.02 High

A system with a **High Risk** rating has an **elevated** likelihood or impact of compromise to systems, networks, or data. Threats or vulnerabilities in this category must be appropriately managed within 7 days, or relevant systems or networks may be shut off or disconnected with little or no prior notice.

By way of example, a **High Risk** rating may consist of any of the following:

- Malware is suspected of having infected an isolated system, but it is identified and contained in a timely manner,
- Non-privileged user access is gained by an unauthorized individual,
- A default password is blank or has not been changed, but the system is not exposed to the internet, or
- A vulnerability with a high CVSS score.

1.03 Medium

A system with a **Medium Risk** rating has a **reduced** likelihood or impact of compromise to systems, networks, or data. Threats or vulnerabilities in this category must be appropriately managed within 60 days, or relevant systems or networks may be shut off or disconnected with little or no prior notice.

By way of example, a **Medium Risk** rating may consist of any of the following:

- A system is out-of-date with security patches, but it is not exposed to the internet,
- Unnecessary services are running on the system, but they do not currently present a heightened risk of the system being compromised or exploited, or
- A vulnerability with a medium CVSS score.

1.04 Low

A system with a **Low Risk** rating has **minimal** likelihood or impact of compromise to systems, networks, or data. Threats or vulnerabilities in this category must be appropriately managed within 120 days, or relevant systems or networks may be shut off or disconnected with little or no prior notice.

By way of example, a **Low Risk** rating may consist of any of the following:

- A system is out-of-date with security patches, but the system is not connected to any network,
- A system is running an obsolete or unsupported operating system, but the system is not connected to any network,
- Unnecessary services are running on the system that may impact performance, but they do not present any reasonable risk of system compromise, or
- A vulnerability with a low CVSS score.

Compliance with this Policy

All WCM Workforce Members must comply with 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, ITS-500.12 – *Restricting Access for Insecure Systems,* to the Office of the CISO, using one of the methods below:

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

References

- WCM Policy ITS-500.11 – Requirements for Securing Systems
- 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
08/14/2023	Justin Barber	Updated risk ratings and definitions to align with NIST standards
08/14/2023	Brian J. Tschinkel	Updated policy template and language for branding
07/30/2024	Tom Horton	Updated contact information and some minor language updates
09/11/2024	Tom Horton	Update policy template and some minor language updates
10/21/2025	Office of the CISO	Updated policy template and minor language updates, and clarified that a vulnerability risk rating may include a CVSS score

Appendix

N/A