Weill Cornell Medicine

11.12

Restricting Access for Insecure Systems

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: March 19, 2015
Last Updated: August 24, 2023
Last Reviewed: August 24, 2023

Contents

Policy Statement

Under the general direction of the *Stephen and Suzanne Weiss Dean of Weill Cornell Medicine*, the Information Technologies & Services Department ("ITS") must take appropriate action to assess, evaluate, and appropriately manage threats that pose a serious risk of impact to Weill Cornell Medicine information systems or applications ("systems") or data. If a system appears to be vulnerable to a threat and has a reasonable likelihood of compromise, the Chief Information Security Officer and/or their delegate reserves the right to block the system from accessing other systems, networks, and/or data. This Policy specifies the standards and thresholds to determine the risk of a system compromise and if any type of access must be blocked.

Reason for Policy

Systems at Weill Cornell Medicine may contain high risk data as defined in ITS policy 11.03 – Data Classification. Systems that are accessible from the public internet are more exposed to attack than a system that resides solely on the internal network. Of course, systems on the internal network are also exposed to threats to some degree, even if they are not networked. As such, all systems must be reasonably secured or they may be disabled, disconnected, powered down, or otherwise have their functionality significantly reduced in order to contain the possibility of a security incident.

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, 11.12 – Restricting Access for Insecure 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. Principles

Pursuant to ITS policy 11.11 – Requirements for Securing Systems, the Chief Information Security Officer has the authority to evaluate the seriousness and urgency of any threat to an information system to Weill Cornell Medicine systems and/or data. Any action taken (e.g., powering off systems and/or restricting/limiting access to the network) is based on a risk assessment that considers the likelihood and impact of a system becoming infected, breached, or the confidentiality and/or integrity of Weill Cornell Medicine data being compromised. Several factors, such as vulnerability reports and industry news sources, 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 11.11 – 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 11.20 – Variances.

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

1.01 Critical

A **critical** risk rating has a **very significant** likelihood or impact of compromise to the system or data. Systems or data in this category must be remediated within 24 hours or may be shut off or disconnected from the network with little or no prior notice to the Administrator, although notice should be timely provided afterwards.

By way of example, a critical risk rating may consist of any of the following:

- A targeted attack against a system or the Weill Cornell Medicine network is suspected,
- A system is suspected to have been compromised or actively controlled 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 Weill Cornell Medicine policy,
- A default password is blank or has not been changed, or
- An event is suspected to have led to a reputational, legal, or financial liability for Weill Cornell Medicine.

1.02 High

A system with a **high** risk rating has an **elevated** likelihood or impact of compromise to the system or data. The system Administrator will be notified upon determination of the risk and has two (2) business days to respond with a plan to appropriately manage the risk. Once the plan is provided, it must be completed within five (5) business days. Failure to respond or complete the provided plan may result in the system being shut off or disconnected from the network.

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, or
- A default password is blank or has not been changed, but the system is not exposed to the internet.

1.03 Medium

A system with a **medium** risk rating has a **reduced** likelihood or impact of compromise to the system or data. The system Administrator will be notified upon determination of the risk and has seven (7) business days to respond with a plan to appropriately manage the risk. Once the plan is provided, it must be completed within thirty (30) days. Failure to respond or complete the provided plan may result in the system being shut off or disconnected from the network.

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, or
- Unnecessary services are running on the system, but they do not present a heightened risk of the system being compromised or exploited.

1.04 Low

A system with a **low** risk rating has **minimal** likelihood or impact of compromise to the system or data. The system Administrator will be notified upon determination of the risk and has thirty (30) business days to respond with a plan to appropriately manage the risk. Once the plan is provided, it must be completed within ninety (90) days. Failure to respond or complete the provided plan may result in the system being shut off or disconnected from the network.

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.

Revision History:

Date	Author	Revision
March 29, 2015	Brian J. Tschinkel	Policy created
August 14, 2023	Justin Barber	Updated risk ratings and definitions to align with NIST standards
August 24, 2023	Brian J. Tschinkel	Updated policy template and language for branding