ITS Policy Library

11.12 - Restricting Network Access for Insecure Systems

Information Technologies & Services

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

Policy Statement

The Information Technologies & Services (ITS) Security & Identity Management team at Weill Cornell Medical College must take appropriate action to assess, evaluate, and mitigate any threats that pose a serious risk or impact to WCMC information or clinical data. If an information system connected to the WCMC network appears to be vulnerable to a threat and has a high likelihood of compromise, ITS reserves the right to block the information system from accessing the network, including the internet. This policy specifies the guidelines and thresholds to determine the risk of a system compromise and if its network access must be blocked.

Reason for Policy

Information systems at Weill Cornell Medical College may contain confidential data. Systems that are accessible from the public internet are more vulnerable to attack from a malicious group or individual than a system that resides solely on the internal network. However, systems on the internal network are also exposed to threats if a compromised system exists on the network. As such, all systems must be secured and ITS reserves the right to turn off or restrict functionality of a system in order to contain an attack in the event of a compromise.

Entities Affected by this Policy

Weill Cornell Medical College and Graduate School of Medical Sciences

Who Should Read this Policy

All members of the Weill Cornell Medical College community

Web Address of this Policy

Contacts

Direct any questions about this policy, 11.12 - Restricting Network Access for Insecure 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, laptop, desktop, or appliance, 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 or third party.

iv) confidential As defined in ITS 11.03 – Data Classification, confidential data includes, without limitation, the following: PHI; PII; student records, including those protected under the Family Education Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA) and the information pertaining to credit cards covered by the Payment Card Industry Data Security Standard (PCI DSS); employment records, including pay, benefits, personnel evaluations, and other staff records; research data involving human subjects that are subject to the Federal Policy for the Protection of Human Subjects (Common Rule) as defined in Title 45 CFR §46.101 et seq.; and research grants and related information, such as applications, contracts, study protocols (including those involving animals), intellectual property belonging to Weill Cornell Medical College, and other sensitive research data.

v) threat Any activity that can be a possible danger. When a threat exploits a vulnerability, an organization can suffer losses.

vi) vulnerability A weakness. It can be a weakness in a system, a configuration, a process, hardware, software, or any other aspect of a system.

vii) compromise A system is compromised, either knowingly or unknowingly, when it has been taken over by another individual or information system without permission.

I. Principles

ITS Security & Identity Management has the authority to evaluate the seriousness and urgency of any threat to an information system on the Weill Cornell Medical College network. 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 of a system becoming infected, breached, or the confidentiality and integrity of WCMC data being compromised. Several factors and vulnerability reports are reviewed and considered before any action is taken on a system.

Any findings and appropriate action will be communicated with the appropriate system managers and administrators. All ITS systems must be configured in accordance with the *11.11 – Requirements for Securing Information Systems* policy.

Threats and vulnerabilities have been categorized into three severities that dicate remediation timeframes: critical, severe, and moderate.

Section 1.01 **CRITICAL**

A system with a **critical** risk rating has a **high to very high** likelihood of compromise and risking the confidentiality or integrity of the data and the availability of the system. Systems in this category must be remediated within 24 hours and may be shut off immediately depending on the threat. The system owner or manager will be notified upon discovery and blocking.

A critical severity may consist of any of the following vulnerabilities:

- A targeted attack against a system or the WCMC network has been launched
- A data compromise or breach has occurred
- Passwords or account credentials have been compromised, obtained, or used illegally
- A system has been compromised that has led to a reputational, legal, or financial liability for WCMC
- A system has been compromised and is being actively controlled by an outsider
- Malware has infected a system and is at risk for spreading to other systems on the network
- A default password is blank or has not been changed and the system is exposed to the internet

Section 1.02 **SEVERE**

A system with a **severe** risk rating has a **medium** likelihood of compromise and risking the confidentiality or integrity of the data and the availability of the system. The system owner or manager will be notified upon discovery and must acknowledge a plan to remediate the vulnerabilities within five (5) business days. If acknowledgement is not received within the initial notification, a second notification will be sent as a courtesy to alert the system owner. Failure to respond within two (2) business days of the second notification may result in the system being blocked from accessing the network.

A system with a severe risk rating may exhibit any of the following vulnerabilities:

- Malware has infected an isolated system, but it is identified and contained
- User access (not as an administrator) 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

Section 1.03 **MODERATE**

A system with a **moderate** risk rating has **low** likelihood of compromise and risking the confidentiality or integrity of the data and the availability of the system. The system owner or manager will be notified upon discovery and must acknowledge a plan to remediate the vulnerabilities within thirty (30) days. If acknowledgement is not received within the initial notification, a second notification will be sent as a courtesy to alert the system owner. Failure to respond within two (2) business days of the second notification may result in the system being secured with additional compensating controls or isolated from the network to mitigate any vulnerabilities or threats.

A system with a moderate risk rating may exhibit any of the following vulnerabilities:

- A system is out-of-date with security patches and the system is connected to the WCMC network, but it is not exposed to the internet
- Unnecessary services are running on the system, but they do not present a high risk of the system being compromised or exploited

Section 1.04 **LOW**

A system with a **low** risk rating has **very low** likelihood of compromise and risking the confidentiality or integrity of the data and the availability of the system. The system owner or manager will be notified upon discovery and must acknowledge a plan to remediate the vulnerabilities within ninety (90) days. If acknowledgement is not received within the initial notification, a second notification will be sent as a courtesy to alert the system owner. Failure to respond within two (2) business days of the second notification may result in the system being secured with additional compensating controls or isolated from the network to mitigate any vulnerabilities or threats.

A system with a low risk rating may exhibit any of the following vulnerabilities:

- A system is out-of-date with security patches, but the system is not connected to the network
- A system is running an obsolete or unsupported operating system, but the system is not connected to the network
- Unnecessary services are running on the system that may impact performance, but do not present any risk of the system being compromised

II. Related Documents

The following documents are also relevant to this policy:

viii) 11.11 – Requirements for Securing Information Systems

ix) Vulnerability Management Process