Weill Cornell Medicine

11.10

Device Minimum Security Requirements

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: November 3, 2016
Last Updated: September 26, 2023
Last Reviewed: September 26, 2023

Contents

Policy Statement

All members of the Weill Cornell Medicine community are responsible for protecting the confidentiality, integrity, and availability of information created, received, stored, transmitted, or otherwise used by the college, and for college activities performed by authorized parties (hereinafter referred to as “data”). All devices used for Weill Cornell Medicine purposes, regardless of ownership, must meet the minimum security requirements as defined in this policy.

Reason for Policy

Weill Cornell Medicine requires a minimum set of security requirements for devices accessing Weill Cornell Medicine networks, applications, and data or used for Weill Cornell Medicine purposes. By mandating a minimum set of security requirements, Weill Cornell Medicine can reduce the risk of an adverse event.

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, including devices not owned by Weill Cornell Medicine but used for Weill Cornell Medicine purposes.

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, 11.10 – Device Minimum Security Requirements, 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

All devices used for Weill Cornell Medicine purposes, regardless of ownership, must meet the minimum security requirements as defined in this policy. Individuals are responsible for complying with all ITS policies including mandatory training and attestations.

2. Devices Owned by Weill Cornell Medicine

Devices owned or issued by Weill Cornell Medicine must meet the minimum security requirements defined in this policy. Devices owned or issued by Weill Cornell Medicine must have ITS management and security software installed unless an approved and up-to-date variance is on file pursuant to ITS policy 11.20 – Variances.

3. Devices Not Owned by Weill Cornell Medicine

Individuals are responsible for safeguarding Weill Cornell Medicine data on devices not owned or issued by Weill Cornell Medicine.

Individuals are also responsible for ensuring such devices meet the minimum security requirements in this policy. If a device is known or suspected of not meeting the minimum security requirements, Weill Cornell Medicine reserves the right to disconnect the device from the network, prohibit the transfer or storage of Weill Cornell Medicine data to or from the device, or take other action as appropriate. Individuals must submit a variance request pursuant to ITS policy 11.20 – Variances if the device is unable to meet the minimum security requirements.

3.01 Personally Owned Devices

Personal devices are not required for Weill Cornell Medicine purposes. However, in the event an individual chooses to use a personal device for Weill Cornell Medicine purposes, the individual is responsible for ensuring the device meets the minimum security requirements as defined in this policy. Personally owned devices used for Weill Cornell Medicine purposes must be registered with ITS in the High Risk Attestation. If these devices need to connect to the Weill Cornell Medicine network or applications, they must pass an ITS Security scan to ensure compliance with this policy.

In accordance with ITS policy 11.02 – Privacy of the Weill Cornell Medicine Network and Systems, Weill Cornell Medicine reserves the right to access, review, quarantine, and release electronic information that is stored or transmitted using Weill Cornell Medicine information technology resources, including any devices personally owned or controlled which are used to access Weill Cornell Medicine systems or data or conduct Weill Cornell Medicine business.

3.02 Individual Devices Owned by Another Institution

Devices owned by another institution may be used for Weill Cornell Medicine purposes if permitted by the owning institution and if the device complies with the minimum security requirements in this policy. These devices must be registered with ITS in the High Risk Attestation. If these devices need to connect to the Weill Cornell Medicine network or applications, they must pass a security scan to ensure compliance with this policy.

3.03 Publicly Available Devices

Devices available for public use, such as those in a library, café, or hotel business center, will often not meet the minimum security requirements in this policy and must only be used temporarily for Weill Cornell Medicine purposes. Individuals are responsible for taking appropriate precautions to ensure Weill Cornell Medicine data is not saved locally or accessible by others.

4. Minimum Security Requirements

Unless an approved and up-to-date variance is on file as described in ITS policy 11.20 – Variances, devices used for Weill Cornell Medicine purposes must adhere to all the following minimum security requirements:

- Use of a modern operating system that regularly receives security updates from the manufacturer pursuant to ITS policy 11.11 – Requirements for Securing Systems,
- Security updates from the device manufacturer or application developers are configured to install regularly or automatically pursuant to ITS policy 11.11 – Requirements for Securing Systems,
- Whole-disk encryption must be enabled if the device will be used to access or store high risk data pursuant to ITS policy 11.06 – Device Encryption,
- An endpoint detection and response (EDR) or anti-virus (AV) product must be installed, enabled, and regularly updated pursuant to ITS policy 11.11 – Requirements for Securing Systems,
- A host-based firewall product must be installed, enabled, and configured to block unnecessary connections pursuant to ITS policy 11.11 – Requirements for Securing Systems,
- A unique account with a strong password pursuant to ITS policy 11.15 – Password Policy must be used to login to the device,
    - Individuals in a household that share the same personal device must not use the same account that is used to access Weill Cornell Medicine data, applications, or services,
- Local privileged or administrator-level access should only be used on an as-needed basis,
- Services which may make devices accessible to others should generally not be installed on an individual's computer (e.g., web hosting services, SSH, peer-to-peer file sharing, etc.), and
- Any applications or services prohibited for certain uses by local, state, or federal government, regulations, data use agreements, or other contractual clauses must not be installed on any device, whether or not the device is owned by Weill Cornell Medicine, if the device is used for any work related to the prohibited use, including checking email or accessing web-based services.

Revision History:

Date	Author	Revision
November 3, 2016	Brian J. Tschinkel	Initial release
May 30, 2023	Brian J. Tschinkel	Policy rewritten and renamed as 11.10
September 12, 2023	Brian J. Tschinkel	Updated minimum security requirements and associated policy references
September 26, 2023	Brian J. Tschinkel, Laura Bradford	Added a minimum security requirement for prohibited use clauses