Weill Cornell Medicine	WCM Administrative Policy and Procedure	
	Policy Title	Device Minimum Security Requirements
	Policy Number	ITS–500.10
	Department/Office	ITS Security
	Effective Date	November 3, 2016
	Last Reviewed	March 12, 2025
	Approved By	WCM-Executive Policy Review Group
	Approval Date	September 23, 2025

Purpose

Weill Cornell Medicine (WCM) requires a minimum set of security requirements for devices accessing WCM networks, applications, and data or used for WCM purposes. By establishing a minimum set of security requirements, WCM can better manage the risk of an adverse event.

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

All WCM Workforce Members are responsible for protecting the confidentiality, integrity, and availability of information created, received, stored, transmitted, or otherwise used by WCM (hereinafter referred to as "data"), and for WCM activities performed by authorized parties.

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

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

For more information on complying with WCM's minimum device security requirements, reference this page.

1. Devices Owned by Weill Cornell Medicine

Devices owned or issued by WCM must have ITS management and security software installed and properly configured unless an approved and up-to-date variance is on file pursuant to *ITS policy 500.20 – Variances*.

2. Devices Not Owned by Weill Cornell Medicine

Workforce Members are responsible for safeguarding WCM data on devices not owned or issued by WCM.

Workforce Members are also responsible for ensuring their devices not owned or issued by WCM meet the minimum security requirements in this policy. If a device is known or suspected of not meeting these minimum security requirements, WCM reserves the right to disconnect the device from the network, prohibit the transfer or storage of WCM data to or from the device, or take any other action as appropriate. If the device is unable to meet the minimum security requirements, individuals must submit a variance request pursuant to *ITS policy 500.20 – Variances*.

2.01 Publicly Available Devices

Devices available for public use (such as those in a library, café, or hotel business center), are presumed to not meet this policy's minimum security requirements. They must only be used temporarily for WCM purposes and must never be used to store or process High Risk Data. Workforce Members are responsible for taking appropriate precautions to ensure WCM data is not saved locally or accessible by others on public devices.

3. Minimum Security Requirements

Unless an approved and up-to-date variance is on file as described in *ITS policy 500.20 – Variances*, devices used for WCM purposes must adhere to all of the following minimum security requirements:

- Use of an operating system that regularly receives security updates from the manufacturer pursuant to *ITS policy 500.11 – Requirements for Securing Systems*,
- Security updates from the device manufacturer or application developers are configured to install regularly or automatically pursuant to *ITS policy 500.11 – Requirements for Securing Systems*,
- Full disk encryption must be enabled on all fixed drives pursuant to *ITS policy 500.06 – Device Encryption*,
- An endpoint detection and response (EDR) or anti-virus (AV) product must be installed, enabled, and regularly updated pursuant to *ITS policy 500.11 – Requirements for Securing Systems*,
- A host-based firewall product must be installed, enabled, and configured to block unnecessary connections pursuant to *ITS policy 500.11 – Requirements for Securing Systems*,
- Accounts must be unique, used by a single individual, and traceable to that individual,
- A strong password pursuant to *ITS policy 500.15 – 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 WCM networks, applications, or data,
- Privileged or administrator-level access should only be used on an as-needed basis,
- Services which may make devices accessible to others should only be used on an as-needed basis (e.g., web hosting services, SSH, RDP, VNC, remote support, peer-to-peer file sharing, etc.), and disabled at all other times, 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 if the device is used for any work related to the prohibited use, including checking email or accessing web-based services.

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, ITS-*500.10 - Device Minimum Security Requirements*, to the Chief Information Security Officer, using one of the methods below:

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

References

- WCM Policy ITS-500.20 – Variances
- WCM Policy ITS-500.11 – Requirements for Securing Systems
- WCM Policy ITS-500.15 – Password Policy
- WCM External KB - HowTo: Ensure your non-managed personal devices are compliant with ITS standards?

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on July 17, 2025.
- WCM-Executive Policy Review Group (WCM-EPRG) on September 23, 2025.

Version History

Date	Author	Revisions
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.
September 24, 2024	Tom Horton	Updated contact information, other general language changes, and updated policy template
March 12, 2025	Office of the CISO	Updated policy template, simplified language. Assigned new policy number “ITS-500.10” (formerly numbered 11.10).
September 23, 2025	Office of the CISO	Substantial updates to clarify expectations and requirements.

Appendix

N/A