Weill Cornell Medicine	WCM Administrative Policy and Procedure	
	Policy Title	ITS Security Policy Exceptions
	Policy Number	ITS-500.20
	Department/Office	ITS Security
	Effective Date	September 12, 2023
	Last Reviewed	September 23, 2025
	Approved By	WCM-Executive Policy Review Group
	Approval Date	July 21, 2026

Purpose

By mandating a minimum set of security requirements, Weill Cornell Medicine (WCM) can reduce the risk of an adverse event. In the event that a security requirement cannot be met, WCM must still ensure that networks, applications, and data is protected. ITS Security Policy Exceptions will be evaluated in extenuating circumstances and may be approved with adequate business justification and appropriate compensating controls.

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 activities performed by authorized parties (hereinafter referred to as “data”). All devices used for WCM purposes, regardless of ownership, must meet the minimum security and system requirements defined in ITS policies. In the event that compliance with ITS policies cannot be achieved, an ITS Security Policy Exception request must be submitted along with an appropriate business justification and compensating controls.

Definitions

High Risk Data: Refer to WCM Policy ITS-500.03 – *Data Classification*.

ITS Security Policy Exceptions: A formal, documented exception to an established information security policy or standard that is approved by WCM ITS.

Workforce Members: Faculty; Non-Faculty Academics; Staff; Students; Volunteers; and others whose conduct in the performance of work for WCM, is under its direction and control, whether or not they are paid by WCM.

Procedure

ITS Security Policy Exceptions may increase the risk of an adverse event or loss of WCM’s networks, applications, and data. Approval of ITS Security Policy Exceptions shall be considered in relatively limited circumstances only when certain criteria are met. ITS Security Policy Exceptions are temporary and must be renewed at least annually, must have adequate business justification, and must have demonstrated

compensating controls to manage the risk of an adverse event to an acceptable level. ITS Security Policy Exceptions must be submitted to ITS with approval from the Workforce Member's Department Administrator.

ITS Security Policy Exception Types

1. Encryption

Pursuant to WCM Policy ITS 500.06 – *Device Encryption*, all Workforce Members must take care to protect High Risk Data (as defined in WCM Policy ITS 500.03 – *Data Classification*) on their devices, including laptops, desktops, smartphones, and tablets. All devices owned by WCM must be encrypted, and devices not owned by WCM but used for WCM purposes must adhere to the appropriate safeguards (as defined in ITS-500.06 - *Device Encryption*).

An ITS Security Policy Exception to device encryption shall be considered only when the following conditions are met:

1. The device is demonstrated not to contain High Risk Data,
2. The Workforce Member attests that the device will never be used for High Risk Data,
3. The device does not meet the minimum hardware requirements to support encryption and cannot be upgraded, or encryption is known to be incompatible with a WCM application,
4. No practical encrypted alternative is available such as centralized file storage services or self-encrypting hard drives, and
5. The device is demonstrated to be physically secured from loss or theft.

There is significant risk in not encrypting devices used to access WCM High Risk Data, and a breach may result in regulatory sanctions and fines for WCM and the individual responsible for the data.

2. Operating System Upgrades or Updates

Pursuant to WCM Policies ITS 500.10 – *Device Minimum Security Requirements* (ITS-500.10) and ITS 500.11 – *Requirements for Securing Systems* (ITS-500.11), devices used for WCM purposes must use a modern operating system that regularly receives security updates from the manufacturer.

ITS management software ensures operating systems are kept up to date by regularly deploying upgrades and updates. An ITS Security Policy Exception to operating system upgrades or updates (or installation of management software) shall be considered only when either of the following conditions are met:

1. The operating system upgrade or update is known to be incompatible with a WCM application, or
2. A third-party vendor is managing and deploying operating system upgrades or updates pursuant to our security policies.

Devices that are able to receive operating system upgrades and updates from ITS but require a different deployment schedule do not require a ITS Security Policy Exception. A request for a different deployment schedule may be submitted to ITS.

3. Application Upgrades or Updates

Pursuant to WCM Policies ITS-500.10 and ITS-500.11, devices used for WCM purposes must be configured to regularly or automatically install security updates from application developers.

ITS management software ensures applications are kept up to date by regularly deploying upgrades and updates. An ITS Security Policy Exception to application upgrades or updates (or installation of management software) shall be considered only when either of the following conditions are met:

1. The application upgrade or update is known to be incompatible with a WCM application, or
2. A third-party vendor is managing and deploying application upgrades or updates pursuant to our security policies.

4. Endpoint Detection and Response/Anti-virus/Anti-malware

Pursuant to WCM Policies ITS-500.10 and ITS-500.11, devices used for WCM purposes must have endpoint detection and response (EDR), anti-virus (AV), or anti-malware (AM) software that is installed, enabled, and regularly updated.

There is no ITS Security Policy Exception for this EDR/AV/AM requirement. If the software is conflicting with another application or process, specific exclusions can be created so as to mitigate or eliminate any issues. To request such an exclusion, users must submit a General IT request and be available to work with ITS personnel to troubleshoot the issue. Exclusions will not be created if the issues are not attributable to the EDR/AV/AM software or not otherwise avoidable. ITS management software ensures EDR/AV/AM software is installed, enabled, and regularly updated. If ITS management software is not utilized, then the owner or administrator of the device is solely responsible for this requirement.

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-500.20 – ITS Security Policy Exceptions*, to the Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email:ciso@med.cornell.edu

References

- WCM Policy ITS-500.06 – Device Encryption
- WCM Policy ITS-500.03 – Data Classification
- WCM Policy ITS-500.10 – Device Minimum Security Requirements
- WCM Policy ITS-500.11 – Requirements for Securing Systems

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 July 21, 2026.

Version History

Date	Author	Revisions
09/12/2023	Brian J. Tschinkel	Initial release
09/26/2024	Tom Horton	Updated policy template and minor language updates
05/06/2025	Office of the CISO	Updated policy template and language updates. Assigned new policy number, “500.20” (formerly numbered 11.20).
09/23/2025	Office of the CISO	Updated policy to improve clarity on responsibilities and procedures for requesting a variance.
07/21/2026	Office of the CISO	Title change. Formerly titled, “ITS Security Policy Exceptions,” and updated the Workforce Members definition to ensure consistency.

Appendix

N/A