	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Device Encryption
	Policy Number	ITS-500.06
	Department/Office	ITS Security
	Effective Date	July 15, 2008
	Last Reviewed	April 1, 2026
	Approved By	WCM-Executive Policy Review Group
	Approval Date	June 16, 2026

Purpose

Encryption provides strong protection by making data inaccessible to those without proper access credentials. Additionally, encryption can exempt Weill Cornell Medicine (WCM) from reporting requirements in the event of a theft or loss under the New York State Information Security Breach and Notification Act, and it meets many of the security standards defined under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

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 Workforce Members must take care to protect High Risk Data on their laptops, desktops, smartphones, tablets, and removable storage devices. 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 defined in this policy to protect High Risk Data. All removable storage drives, such as external hard drives or USB flash drives, must be encrypted if they contain High Risk Data. Any variances to this policy must meet the requirements defined in WCM Policy ITS-500.20 – *Variances*.

Definitions

Encryption: Encryption is the process of converting information into a coded format to prevent unauthorized access.

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

Workforce Members: Faculty; Non-Faculty Academics; Staff; Students; Volunteers; 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.

Standards

1. Encryption of Devices Owned by Weill Cornell Medicine

Encryption shall be provided, at no additional charge, for all institutionally owned devices used by WCM Workforce Members that are not otherwise exempted from this rule.

2. Encryption of Devices Not Owned by Weill Cornell Medicine

Pursuant to WCM Policy ITS-500.10 – *Device Minimum Security Requirements*, Workforce Members are responsible for safeguarding WCM data on devices not owned or issued by WCM. Such devices may include personally owned devices, individual devices owned by another institution, or publicly available devices such as those in a library, café, or hotel business center.

Workforce Members must ensure whole-disk Encryption is enabled on their personally owned devices or individual devices owned by another institution if they will be using the devices to access or store High Risk Data. These devices must also be registered with ITS in the High Risk Attestation.

Devices available for public use, such as those in a library, café, or hotel business center, will often not support Encryption and must only be used temporarily for WCM purposes and must never be used to process or store High Risk Data. Individuals are responsible for taking appropriate precautions to ensure WCM data is not saved locally or accessible by others.

ITS is available to assist and provide “best effort” support to encrypt devices not owned by WCM. Devices owned by another institution, such as those which are owned by affiliates of WCM, should utilize the Encryption software approved by that institution’s IT department. Individuals are strongly encouraged to make a backup of the personal data on their device and verify it for accuracy and completeness before seeking assistance from ITS to encrypt their device for WCM purposes.

3. Removable Storage Devices

High Risk Data stored on removable storage devices must be encrypted. Examples of removable storage devices include, but are not limited to, flash drives, external hard drives, memory cards, and optical discs. Strong hardware or software-based Encryption algorithms such as the Advanced Encryption Standard (AES) with at least 256-bit keys should be used. When encrypted removable storage devices are used to share High Risk Data, the Encryption password must be shared separately and in a secure manner, such as encrypted email.

4. Variances to this Policy

There is significant risk in not encrypting devices used to access WCM data, and a breach may result in regulatory sanctions and fines for the college and the individual responsible for the data. Variances shall be considered in relatively unusual circumstances and must meet the requirements defined in WCM Policy ITS-500.20 – *Variances*.

5. Device Decommission and Decryption

Upon leaving WCM, individuals with devices owned by WCM must turn their devices into their supervisor. These devices will remain encrypted and will be securely repurposed or reprovisioned. Individuals with devices not owned by WCM which have been used for WCM purposes must inform ITS and their supervisor prior to termination so that WCM data can be removed; the devices can then be decrypted.

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, 500.06 – Device Encryption, to the Office of 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-500.10 – Device Minimum Security Requirements
- New York State Information Security Breach and Notification Act
- Health Insurance Portability and Accountability Act (HIPAA)

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on June 4, 2026; and
- WCM-Executive Policy Review Group (WCM-EPRG) on June 16, 2026.

Version History

Date	Author	Revisions
7/15/2008	Office of the CISO	Original date of issue.
10/3/2014	Office of the CISO	Expanded policy to include end user devices beyond laptops; clarified exemptions
1/4/2015	Office of the CISO	Modified guidelines for exemptions
11/8/2018	Office of the CISO	Removed references to obsolete ITS services
11/7/2021	Office of the CISO	Added Revision History and Removable Storage Devices sections
5/11/2023	Office of the CISO	Updated policy template and language for branding
5/13/2023	Office of the CISO	Changed nomenclature around “tagged” and “untagged” to ownership
9/12/2023	Office of the CISO	Added reference to new policy for variances
9/15/2023	Office of the CISO	Ensured consistent language with 11.10 policy
9/24/2024	Office of the CISO	Updated policy template and language
03/12/2025	Office of the CISO	Updated policy template, language, and policy was assigned a new number, “ITS-500.06” (formerly numbered “11.06”)
06/16/2026	Office of the CISO	Updated policy template and language, removed specific encryption software examples

Appendix

N/A