	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Data Loss Prevention
	Policy Number	ITS-500.09
	Department/Office	ITS Security
	Effective Date	April 7, 2011
	Last Reviewed	July 12, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	June 16, 2026

Purpose

Weill Cornell Medicine (WCM) is legally responsible for protecting institutional data, including High Risk Data as defined in ITS policy 500.03 – *Data Classification*. High Risk Data must be treated with extreme care to avoid inappropriate loss or disclosure with possible attendant fines or mandated notifications.

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

WCM community members are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by WCM. In accordance with policies 500.01 – *Responsible Use of Information Technology Resources* and 500.02 – *Privacy of the Weill Cornell Medicine Network and Systems*, WCM reserves the right to restrict the use of its resources in order to preserve data security or comply with law or policy. While WCM permits generally unhindered use of its information technology resources, those who use WCM do not acquire, and should not expect, a right of privacy.

In order to further secure data and improve regulatory compliance, WCM has implemented a data loss prevention ("DLP") system. The DLP system is used to identify High Risk Data on the WCM network and, in cases where intentional or unintentional use violates policy, WCM may block the creation, reception, storage, or transmission of High Risk Data.

Definitions

Data in Motion: Any digital information that is currently traveling from one place to another. Whenever you send, receive, upload, or download files, records, or documents, that information is in this active state of travel.

Data at Rest: Any digital information that is stationary and physically saved on a storage device. Whenever files, records, or documents are archived and not actively moving or being edited, that information is in this inactive state.

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.

Procedure

The DLP system identifies High Risk Data that may be transmitted without proper safeguards and flags it for further investigation. In some cases, the DLP system will stop the flow of data, such as an email containing High Risk Data that is sent to an outside entity without the use of encryption.

The DLP system has the ability to:

- Monitor for and analyze Data in Motion
- Search for and analyze Data at Rest

By gathering this information, the DLP system can determine if the data is High Risk and appropriately secure it to prevent security policy violations and maintain regulatory compliance.

WCM handles a large amount of High Risk Data on a daily basis. Technologies that enable WCM to function efficiently and make data easy to access and share also increase the risk of unauthorized disclosure and loss of confidentiality. This has potentially serious consequences, including financial penalties, customer dissatisfaction, increased regulatory scrutiny, and reputational damage.

The DLP system may be used in conjunction with other security tools to protect High Risk Data and reduce the risk of it being compromised. This helps protect both WCM data as well as the WCM community from the consequences of losing High Risk Data.

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, 500.09 – Data Loss Prevention, 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-500.01 - Responsible Use of Information Technology Resources
- WCM Policy ITS-500.02 - Privacy of the Weill Cornell Medicine Network and Systems
- WCM Policy ITS-500.03 - Data Classification

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
04/07/2011		Initial draft completed
05/13/2023	Office of the CISO	Updated policy template and language
07/03/2024	Office of the CISO	Updated contact information and fixed a typographical error
07/12/2024	Office of the CISO	Updated policy template and language
06/16/2026	Office of the CISO	Updated policy template and language, and defined data in motion and at rest

Appendix

N/A