Policy Title	Data Loss Prevention
Policy Number	500.09
Department	ITS Security
Effective Date	April 7, 2011
Last Reviewed	July 23, 2024
Approved By	Tom Horton
Approval Date	July 23, 2024

Policy

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

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

Purpose

Weill Cornell Medicine 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

Applies to all members of the Weill Cornell Medicine community who utilize Weill Cornell Medicine information technology resources. This includes Weill Cornell Medicine-Qatar and those responsible for managing and safeguarding Weill Cornell Medicine data.

Procedure

The data loss prevention 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 data in motion (e.g., emails, instant messages, web or file transfers, etc.)
- Search for and analyze data at rest (e.g., data residing on a file server, database, or cloud storage solution) and data at the endpoint (e.g., files on a laptop, desktop, or on a flash drive).

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

Weill Cornell Medicine handles a large amount of High Risk data on a daily basis. Technologies that enable Weill Cornell Medicine 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 is being used in conjunction with other security tools to protect high risk data and reduce the risk of it being compromised. This helps protect both Weill Cornell Medicine data as well as the Weill Cornell Medicine 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, 500.05 – Security and Privacy Incident Response Plan, to the Chief Information Security Officer, using one of the methods below:

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

Policy Approval

Version History

Date	Author	Revisions
April 7, 2011		Initial draft completed
May 13, 2023	Brian J. Tschinkel	Updated policy template and language
July 3, 2024	Tom Horton	Updated contact information and fixed a typo
July 12, 2024	Christine Klucznik	Updated policy template and language