Weill Cornell Medicine	**Policy Title**	Responsible Use of Information Technology Resources
	Policy Number	500.01
	Department	ITS Security
	Effective Date	October 1, 2007
	Last Reviewed	July 23, 2024
	Last Updated	July 23, 2024
	Approved By	Tom Horton
	Approval Date	July 23, 2024

Policy

All members of the Weill Cornell Medicine community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college, or for college activities by authorized parties regardless of the medium on which the data resides and regardless of the format (e.g., electronic, paper, fax, or other physical form).

Departments are responsible for implementing administrative, operational, physical, and technical controls for access, use, transmission, and disposal of Weill Cornell Medicine data in compliance with all Weill Cornell Medicine policies, standards, procedures, and guidelines.

Weill Cornell Medicine expects community members, including but not limited to faculty, staff, and students, to use all Weill Cornell Medicine information technology resources and data in a manner that is legal, ethical, and consistent with the mission of education, research, and patient care.

Purpose

Information technology resources and data constitute valuable Weill Cornell Medicine assets. The use of these assets is constantly changing and evolving, and it is important that Weill Cornell Medicine articulate a clear statement regarding their appropriate use. This Policy provides both broad and detailed requirements for the responsible use of information technology resources and data. In addition, it requires departments to appoint liaisons who will facilitate communications, training, and awareness programs working with the Information Technologies & Services Department (ITS) and all other college departments.

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

1.01 Acceptable Use

Acceptable use of Weill Cornell Medicine IT resources and data includes, but is not limited to, community members:

1. Respecting system security mechanisms, and not taking measures to circumvent, ignore, or break these mechanisms,
2. Showing consideration for the consumption and utilization of ITS resources,
3. Understanding and complying with policies, standards, procedures, and guidelines concerning the security of the Weill Cornell Medicine information technology and data, and,
4. Assisting in the performance of investigation and remediation steps in a suspected or detected security incident.

1.02 Unacceptable Use

Unacceptable use of IT resources and data includes, but is not limited to, unauthorized access to or unauthorized use of Weill Cornell Medicine ITS resources

1. Use of ITS resources in violation of any other Weill Cornell Medicine policy, applicable law or regulation,
2. Any activity designed to hinder another person's or institution's use of its own information technology resources or data,
3. Downloading, executing, installing, distributing, or using suspicious or malicious software (e.g., key generators, pirated software, spyware, viruses, etc.),
4. Security breaches, intentional or otherwise, including negligent management of data, servers, workstations, other devices or peripherals, or applications resulting in unauthorized use or compromise, and,
5. Password use inconsistent with 11.15 Password Policy

1.03 Departmental Responsibility

In order to facilitate compliance with this and other security policies, each department must appoint a representative who will be responsible for the following:

1. Understanding security policies and assisting in disseminating and evangelizing policies, standards, procedures, and guidelines to the greater Weill Cornell Medicine community,
2. Meeting with appropriate ITS staff (as needed) on a predetermined, regular basis to discuss security and other information technology and data related issues,
3. Providing documented authorization and de-authorization for data and information technology resource access requests to ITS whenever appropriate,
4. Partnering with ITS to perform remediation steps in the event of data loss, theft, compromise, suspected or detected security incidents, etc., and,
5. Partnering with ITS in coordinating all activities related to electronic discovery.

Departments may choose to appoint multiple representatives where appropriate.

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, 500.01 – [Responsible Use of Information Technology Resources], 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
January 31, 2008		Initial draft completed
February 9, 2015	Brian J. Tschinkel	Updated for FY15
July 25, 2022	Brian J. Tschinkel	Updated for FY23
March 3, 2023	Brian J. Tschinkel	Updated policy template and language for branding

June 20, 2024	Tom Horton	Updated policy language and contact information
July 11, 2024	Christine Klucznik	Updated policy template and language