	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Responsible Use of Information Technology Resources
	Policy Number	ITS-500.01
	Department/Office	ITS Security
	Effective Date	October 1, 2007
	Last Reviewed	July 11, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	March 24, 2026

Purpose

Information Technology Resources and data constitute valuable Weill Cornell Medicine (WCM) assets. The use of these assets is constantly changing and evolving, and it is important that WCM articulate a clear statement regarding their appropriate use. This policy provides requirements for the responsible use of Information Technology Resources and data.

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 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 WCM data in compliance with all WCM policies, standards, procedures, and guidelines.

WCM expects Workforce Members to use all WCM Information Technology Resources and data in a manner that is legal, ethical, and consistent with the mission of education, research, and patient care.

Definitions

Information Technology (IT) Resources are the computing systems, networks, software, data, and related services owned, managed, or provided by WCM to support clinical, research, educational, and administrative activities. This includes institutional devices, applications, accounts, and infrastructure used to access, process, store, or transmit institutional information.

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

1.01 Acceptable Use

Acceptable use of WCM IT resources and data includes, but is not limited to, Workforce 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 WCM 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, accessing or using WCM ITS resources without proper authorization, and/or any of the following:

1. Use of ITS resources in violation of any WCM policy, NYP policy, or applicable law, regulation, or license;
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 unlicensed, 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 WCM Policy ITS-500.15 - *Password Policy*.

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-500.01 – 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

References

- WCM Policy ITS-500.15 - Password Policy
- Cornell University Policy 4.6 – Standards of Ethical Conduct

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on March 19, 2026; and WCM-Executive Policy Review Group (WCM-EPRG) on March 24, 2026.

Version History

Date	Author	Revisions
01/31/2008		Initial draft completed
02/09/2015	Brian J. Tschinkel	Updated for FY15
07/25/2022	Brian J. Tschinkel	Updated for FY23
03/03/2023	Brian J. Tschinkel	Updated policy template and language for branding
06/20/2024	Tom Horton	Updated policy language and contact information
07/11/2024	Christine Klucznik	Updated policy template and language
03/24/2026	Office of the CISO	Updated policy template and language, removed the departmental responsibility section.

Appendix

N/A