Policy

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

Departments are responsible for implementing operational, physical, and technical controls for access, use, transmission, and disposal of WCMC data in compliance with all WCMC privacy and security policies, procedures, and guidelines.

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

Entities Affected By This Policy

The Weill Cornell Medical College and Graduate School of Medical Sciences

- **Responsible Executives:** WCMC Chief Information Officer
- **Responsible Department:** Information Technologies and Services
- **Dates:** *Issued:* Interim, October 1st, 2007. *Final Issuance:* January 31st, 2008
- **Contact:** Information Technologies and Services

Reason for Policy

Information technology resources and data constitute valuable WCMC assets. The use of these assets is constantly changing and evolving, and it is important that WCMC articulate a clear statement regarding the appropriate use of college information technologies and data. This policy provides both broad and detailed guidelines for the responsible use of information technologies resources and data. In addition, it requires departments appoint ITS Liaisons, which will be used to facilitate communications, training, and awareness programs between the Information Technologies and Services Department and all other college departments.

Principles

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

1. Respecting system security mechanisms, and not taking measures designed to circumvent, ignore, or break these mechanisms
2. Showing consideration for the consumption and utilization of IT resources
3. Understanding and complying with policies, procedures, and guidelines concerning the security of the WCMC information technology and data
4. Assisting in the performance of remediation steps in the event of a detected vulnerability or compromise

Unacceptable use of IT resources and data includes, but is not limited to:

1. Unauthorized access to or unauthorized use of WCMC IT resources
2. Use of resources in violation of any applicable law or regulation
3. Any activity designed to hinder another person's or institution's use of its own information technology and data
4. Installation, distribution or intentional use of malicious software (spyware, viruses, etc.)
5. Security breaches, intentional or otherwise, including negligent management of a server or workstation resulting in its unauthorized use or compromise
6. Sharing of a password

In order to facilitate compliance with this and other security policies, each department must appoint an **Information Technologies and Services (ITS) Liaison**. ITS Liaisons will be responsible for:

1. Understanding security policies and assisting in disseminating and evangelizing policies, procedures, and guidelines to the greater WCMC community
2. Meeting with appropriate ITS staff members 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. Assisting in performing remediation steps in the event of data loss, theft, compromise, detected vulnerability, etc.
5. Assisting in coordinating all activities related to E-Discovery (see definitions)

Departments may choose to appoint multiple liaisons when appropriate. Liaison appointments must be approved by the ITS Security Officer or his or her designee.