Policy Statement

In accordance with the Weill Cornell Medical College (WCMC) Data Classification Policy, all information systems that create, receive, store, or transmit data classified as 'Confidential' must adhere to the administrative security principles of this document.

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

State and federal regulations, as well as general best practices, shape the security and privacy protections that must be afforded to data classified as "Confidential". This policy addresses regulatory and best practice requirements to ensure proper administrative security of Confidential data.

Principles

Information systems or applications that create, receive, store, or transmit Confidential data (hereafter "Confidential Systems" – see Data Classification policy) must, without exclusion, adhere to the following:

1. Risk Assessment
    a. All Confidential Systems must undergo a documented risk assessment. At minimum, the following must be addressed:
        i. System purpose
        ii. Possible threats
        iii. Possible vulnerabilities
        iv. Remaining residual risks (after mitigation)
    b. Risk assessments should be designed to determine the likelihood of a security compromise and the potential damage such a compromise could cause. Risk assessment tools that address these concerns will be made available to all through the

Information Technologies and Services Department. It is strongly recommended that these tools be used for risk assessment, as they will meet all requirements of this policy.

c. Systems must be rated for risk according to an analysis of the factors above. Systems with significant levels of risk are to be addressed on a priority basis and given the most restrictive and stringent security controls practical.

2. Risk Management

   a. Not all information systems can be governed by the same security controls. In some case, when security controls conflict with equally important considerations of data availability or system usability, it may be necessary to make trade-offs. Managers and administrators of Confidential systems are responsible for:

      i. Identifying and documenting security-control variances between Confidential systems and the policies that apply to those systems.

      ii. Documenting the reasons for such variances.

      iii. Addressing risks presented.

      iv. Identifying compensating controls for the documented risks.

      v. Implementing those compensating controls.

3. Workforce Security Training

   a. WCMC shall provide appropriate training on security regulations and policies to all workforce members. Training must be managed by the WCMC Security Officer or his or her designee and must ensure:

      i. All workforce members receive and understand all appropriate WCMC security policies and procedures.

      ii. New workforce members successfully complete HIPAA Security and Privacy training.

      iii. Workforce members receive additional appropriate training whenever acting as a systems administrator, security administrator, or ITS Liaison.

   b. Training must be reviewed at least biannually and updated when security policies and procedures are substantially changed.

4. Contingency Planning

a. Managers and administrators of Confidential systems are responsible for creating, implementing, and testing, at least biannually, disaster recovers and business continuity plans for those systems. All plans must address and document the following:

i. An analysis of data criticality, which considers importance relative to: the mission of the institution or department, the sensitivity of the data on the system, and the amount of Confidential data on the system.

ii. Data backup policies and procedures.

iii. Recovery procedures used to restore operational capacity or data.

iv. Emergency operating plans, which detail the process for maintaining business operations and protecting Confidential data while operating in an emergency mode.

v. Procedures for testing and revising emergency operating plans. Copies of these plans should be stored in multiple secure locations, including off-site.

5. Review

a. Managers and administrators of Confidential systems are responsible for reviewing these systems at least once every 3 years. Reviews must evaluate risks, identify and test security controls, and update risk management and contingency plans. Reviews must include, at minimum:

i. Any relevant regulatory, compliance, or policy changes.

ii. Changes in the threat or risk environment.

iii. An update of implemented security controls.

iv. An account of data security incidents that occurred since the last review.

v. Implementation plans for new or updated physical, administrative, or technical controls.

6. Record Retention

a. All documentation created for Confidential system as part of policy compliance efforts must be kept for a minimum of 6 years from the creation date or most recent change made.

7. Availability

a. All documentation created for Confidential systems as part of policy compliance efforts must be made available to all parties responsible for implementing the procedures for which the documentation pertains.

8. Security Incident Response Procedures

a. ITS Liaisons and managers and administrators of Confidential systems are responsible for reporting security incidents. Security incidents in this context are defined as one or more of the following:

i. Unauthorized Confidential system access or use.

ii. Unauthorized Confidential data disclosure, modification, or destruction.

iii. Unauthorized interference with normal operations or Confidential systems.

iv. Theft or loss of Confidential systems or data.