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 authentication and authorization 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 authentication and authorization to 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. Access

    a. Managers and administrators of Confidential systems are responsible for ensuring access to those systems is based on work function and is controlled using the minimum necessary standard. Documented procedures for ensuring appropriate access to Confidential Systems must include:

        i. Authorization methods (e.g. using a CWID), including manner and type of authorized administrative access

        ii. Authentication methods (e.g. requiring passwords), including manner and type of authentication

        iii. Methods for evaluating access to Confidential systems based on the need to fulfill an appropriate business purpose

iv. Documentation of each workforce member's and vendor's access rights to Confidential systems

v. Acknowledgement forms, signed by the appropriate supervisors, which document that they have knowingly and willingly authorized access rights to Confidential systems to appropriate workforce members and vendors

vi. Acknowledgement forms, signed by the appropriate workforce members and vendors, which document that all appropriate parties are aware of their authorized access rights to Confidential systems

vii. A formal process for annually reviewing and revising workforce member and vendor access to Confidential systems

viii. A formal process for the timely termination of workforce member and vendor access to Confidential systems whenever appropriate (e.g. immediately upon end of employment).

ix. A formal process for the timely change of workforce member and vendor access to Confidential systems whenever appropriate (e.g. after a change in role or position).

x. A formal process for regularly assessing effectiveness of access controls to Confidential systems

xi. A formal process for providing, and subsequently removing, electronic access to Confidential systems to appropriate workforce members and vendors during an emergency

2. Unique User Identification

a. All electronic access to Confidential systems must be the result of using a unique identifier, such as a username and password. Users are only granted one unique WCMC CWID and password. Using another user's account (CWID) to access Confidential systems is prohibited. Violators will be subject to disciplinary action (see the WCMC Sanctions Policy).

b. Managers and administrators of Confidential systems are responsible for ensuring that access technologies and methodologies for those systems incorporate the following:

i. Usage of "strong" (difficult to guess) passwords that contain, at minimum, a combination of capital and lower-case letters, and numbers

ii. Usage of "unique" (not shared among multiple users) user ID's (e.g. CWID's) with appropriate authentication mechanism (passwords, tokens, biometrics, etc)

iii. Forced periodic password changes of, at minimum, every 180 days

iv. Enforced prohibition of password reuse

v. Enforced prohibition of sharing or disclosing of password

c. Gaining access to Confidential systems or data by using credentials other than one's own makes it impossible to properly log and audit access. Therefore, it is not acceptable for any user to use another user's authorization credentials (e.g. CWID and password) to gain access to any Confidential IT resources. It is additionally not acceptable for any user to act on behalf of another user when accessing IT resources unless this practice has been documented and approved by a supervisor of that system.

d. In some circumstances, such as in research labs, is it acceptable *to* use a 'shared' account for *login only* to computer workstations. In cases where shared accounts are preferred or required, managers and administrators of confidential systems must ensure that shared accounts are used only to login (authenticate) to those systems, and not for authenticating to applications accessible from the system. It is never acceptable to use a shared account to access applications, databases, or other systems that store Confidential data. Accounts used in this shared manner must never be normal user accounts (e.g. CWID's), but should instead be accounts created solely for the purpose of logging into limited numbers of computer workstations.

3. Audit Controls

a. All access to Confidential systems and data must be electronically logged. Logged data must be audited on a predetermined basis; at least annually. Documentation of audits must be kept for at least 2 years. Discrepancies or access violations found through audits should be reviewed and remediated.

b. Audit logging should be deployed in layers: at the network, application, back-end database, and system levels, and incorporate the following:

i. Access logs – systems or security administrators must have procedures in place to log and review administrative and user access to IT resources.

ii. Activity logs – systems or security administrators should log and review user activity, such as data insertions, revisions, changes, or deletions

iii. Systems monitoring – systems or security administrators should monitor IT resources for anomalies such as changes in performance, network traffic, and intrusion detection.