Weill Cornell Medical College

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 integrity 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 protect data integrity.

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. Disabling unnecessary services
    a. All Confidential Systems must disable services that are not required to achieve the business purpose or function of the system. Examples of unnecessary services could include, but are not limited to, FTP, Telnet, SMTP, Web services, etc.
2. Monitoring Log-in Attempts
    a. All access to Confidential Systems must be logged. Logs must be audited on a predetermined, periodic basis. Documented procedures must be in place for the regular review of the audited activity. Discrepancies or access violations found through audits must be documented and, when appropriate, reported as per the WCMC incident reporting process (see Incident Reporting Policy).
3. Protection from malicious software

a. All Confidential Systems must be tagged with an ITS tag, which ensures ITS-offered protections from malicious software are available. These protections include, but are not limited to, antivirus software, personal firewall software, and automated installation of security patches. For non-networked Confidential Systems, users should make reasonable efforts to keep systems updated with the latest security patches and antivirus software and definitions. Antivirus software is available to all users through the Information Technologies and Services Department.

b. Confidential Systems (including laptops and PDA's) should be used for appropriate WCMC functions. While non-essential computer activities such as playing music are not generally prohibited, users should be cognizant that, when misused, this type of practice can result in disruption of the larger WCMC computing environment. Users are expected to treat electronic resources with care and seek advice from their direct supervisors or ITS Liaisons if they are unsure as to the appropriateness of particular computing functions.

4. Patch Management

    a. Managers and administrators of Confidential Systems have the responsibility of determining whether and/or which patches (e.g. operating system, application, or other patches) to deploy. In cases where the ITS department recommends deployment of a patch, managers and administrators of Confidential Systems must deploy that patch in a timely manner or otherwise implement documented compensating controls.

5. Intrusion Detection and Vulnerability Scanning

    a. Networks that support processing, storage, or transmission of Confidential data must be monitored for intrusion and compromise by contemporary intrusion detection and/or prevention technologies. Intrusions must be investigated, logged and reported as per the WCMC incident reporting policy.

    b. Vulnerability scanning of Confidential Systems must occur on a predetermined, regular basis, no less than annually. Vulnerability scans must be reviewed by trained personnel and, when appropriate, reported as per the WCMC incident reporting policy.

6. Server Security

    a. Server administrative functions on Confidential Systems may be performed only by personnel with documented authorization.

7. Workstation Security

a. Anyone authorized to use a WCMC workstation is expected to protect the integrity of that workstation and the data it contains.

b. Users are expected to make reasonable efforts (e.g. by one more of the following: locking, logging out, using privacy screens, using logons with limited access, etc.) to restrict the viewable access to workstations that are connected to (or are considered to be) Confidential Systems when they are going to be out of viewable range of those workstations. After a predetermined amount of inactivity, workstations that have access to (or are considered to be) Confidential Systems should automatically lock or log off. Electronic access from workstations to Confidential Systems should be automatically terminated after a predetermined period of activity.

c. Workstations, printers, fax machines, etc, classified as "Confidential" should not be located in public sections of walkways, hallways, waiting areas, etc. To the extent reasonable, efforts should be made to limit the viewing of data on these workstations to workforce members with legitimate business need to do so.

8. Laptops

    a. All reasonable efforts should be made to avoid storing Confidential data on laptops. Laptops devices that store Confidential data must employ:

        i. Unique individual power-on passwords

        ii. Password protected screen savers (when technically possible)

        iii. Encryption of Confidential data (when technically possible)

9. Mobile Devices

    a. All reasonable efforts should be made to avoid storing Confidential data on mobile devices, including PDA's, Blackberries, Flash Drives, etc. Mobile devices that must store Confidential data must employ encryption of Confidential data (when technically possible).

10. Data Security

    a. Managers and administrators of Confidential Systems must document and adhere to a process to regularly assess data storage systems and requirements in order to:

        i. Reduce the risk of compromise of Confidential data confidentiality and/or integrity.

ii. Implement and/or review controls designed to protect Confidential data from improper alteration or destruction.

iii. Ensure that Confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.

iv. Ensure that back-end databases containing large amounts (over 1 gigabyte) of Confidential data are isolated from other application or system services (e.g. application middleware, Web and e-mail servers, thin-client servers, etc.) and where not practical, protected by equivalent compensating controls.

v. Backup tapes containing Confidential data must be encrypted using contemporary encryption standards.

11. Transmission Security

a. Managers, administrators, or other applicable users of Confidential Systems are responsible for protecting Confidential data (including file transfers) while in transit, both within the WCMC networks, and on public networks such as the Internet. Managers and administrators of Confidential Systems and data must adhere to the following:

i. Any transmission of Confidential data over public networks must be encrypted.

ii. Integrity controls that ensure data has not been tampered with by unauthorized users must be in place for all Confidential data that traverses the WCMC networks.

iii. Sender authentication controls that verify the sender of Confidential data is who that sender claims to be must be in place for all Confidential data that traverses the WCMC networks.

iv. Recipient authentication controls that verify the recipient of Confidential data is who that recipient claims to be must be in place for all Confidential data that traverses the WCMC networks.

v. System logs of all transmissions of Confidential data over public networks must be stored for a documented, predetermined amount of time. These logs must be available for audit.

12. Email Transmission Security

a. Many of the controls above are addressed by the appropriate use of security technologies (e.g. IPSec-compliant virtual private networks (VPN's), SMTP over SSL, etc) and practices. Users must be particularly careful when transmitting email containing Confidential data, as e-mail is inherently insecure. Additional standards for the use of email in communicating Confidential data are:

    i. The inclusion of Confidential data in email must be kept to the minimum necessary needed to meet the intended purpose of the message and must be directed only to people with legitimate authorization.

    ii. Sending messages to an unintended recipient is particularly easy to do with email, and senders should verify the send-to email address before sending messages containing Confidential data.

    iii. To protect the confidentiality of Confidential data, senders should use encrypted email services wherever such services are available and practical.

    iv. Instead of sending or receiving email attachments containing unencrypted Confidential data, users should use a secure file transfer service, such as https://transfer.med.cornell.edu.

    v. Instant messaging and other similar technologies (e.g. text paging, text messaging) have many of the same security problems as email and are generally even more difficult to secure. Unless the communicating parties are certain that communications are protected effectively against unauthorized use or disclosure (such as through the WCMC encrypted instant messaging service, talk.med.cornell.edu), Confidential data may not be sent through instant messaging or other similar technologies.