

TITLE: EPHI3. GENERAL INFORMATION SECURITY POLICY

POLICY:

CUMC follows good password, software, network (including Internet) and other security practices, and provides security awareness training to the workforce members to exercise appropriate precautions against potentially risky behavior. This policy is an addition to ***CU Desktop and Laptop Security policy***.

PURPOSE:

CUMC specifies this policy to follow reasonable information security practices for EPHI security, and to instruct all workforce members on such practices.

APPLICABILITY:

CUMC faculty, staff, students, owners, custodians, and users of EPHI systems

PROCEDURE:

1. EPHI systems are required to be protected by authentication systems that employ user identifiers (UserIDs) and secret passwords unique to each user. Password management procedures include:
 - A. Do not share passwords.
 - B. Require and force regular password changes every 45-180 days, including immediate password change for the initial password if necessary.
 - C. Prevent reuse of passwords that were used recently (the recommended number of previously used passwords for prevention is 3-6).
 - D. Require and force the use of individual passwords to maintain accountability.
 - E. Permit workforce members to select and change their own passwords.
 - F. Require passwords that meet good password criteria:
 - i. Do not use dictionary words or commonly known proper nouns.
 - ii. Use passwords that are at least six characters long.
 - iii. Include capital letters and numbers.Consult Information Security Office for *Information security guidance list: Good password guidance* for a comprehensive and recent guide.
 - G. Require passwords not to be displayed in clear text when inputting into information systems.
 - H. Require passwords to be given to workforce members in a reasonably secure manner.
 - I. Force changing of default vendor passwords immediately following installation of hardware and software.
 - J. Train workforce members on good password practices.

2. EPHI systems are required to follow reasonable practices for guarding against, detecting and reporting malicious software that pose a risk to information. Malicious software includes viruses, worms, Trojan horses, spyware, and other malicious software.

Responsibilities of workforce members include:

- A. Not bypass or disable protection mechanisms unless properly authorized to do so.
- B. Report suspected or confirmed malicious software.
- C. Exercise caution when accessing web pages and email attachments from unknown sources.

Responsibility of owners and custodians of workstations, servers and systems include:

- A. Install anti-virus (and other protective) software and ensure regular updates of the same.
- B. Implement regular security patch procedures for all underlying software including operating system, databases, web and other servers and services, etc.
- C. Configure systems to guard against accidental or opportunistic misuse of the system. This includes shutting down unnecessary services, ensuring requirement of good passwords for all accounts in all underlying software, and protections of files and databases.
- D. Implement anti-spam and anti-virus software for email and other mass communication systems.
- E. Implement ability to possibly recognize a malicious attack and to recover from a malicious attack with adequate backup and disaster recovery strategies.
- F. Document security measures conducted towards these requirements. Consult Information Security Office for *Application security documents list: ports, services, files protection* and *Application security documents list: security metrics*.

3. Workforce members are required to logoff from EPHI applications after completing their access at any location that may potentially have multiple users. Owners and custodians should implement procedures in information systems to terminate established sessions after no more than 15 minutes of inactivity through an automatic logoff mechanism or an equivalent alternative mechanism. An exception to this requirement may be made in those cases where the immediate area surrounding a system is physically secured.
4. Workforce members receive EPHI security information, awareness reminders, training, and updates via:

- A. EPHI system sign-on messages (see **Information security: audit and evaluation policy** (#EPHI4))
- B. Pop-up messages, and dialog boxes, as appropriate within applications
- C. Screen savers
- D. Management bulletins through email and mail, as well as communication with staff in seminars and other venues
- E. Training

POLICY MAINTENANCE:

Information Security Office

REFERENCES:

All information security policies

CU Administrative policies in Computing & Technology

Health Insurance Portability and Accounting Act of 1996, 45 CFR

164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D),
164.312(a)(2)(iii)

REVIEW/REVISION DATE:

November 2007