


BOSTON UNIVERSITY

		Title:	Password Policy
		Policy ID:	BU 000-005C
		HIPAA Section:	164.308(a)(5)(ii)(D)
		Version:	1.0
		Effective Date:	April 20, 2005
Policy Custodian:	Information Services & Technology		
Authorized By:	Vice President for Information Services & Technology		

1. Purpose – To establish a standard for creating, changing, and safeguarding passwords.

2. Password Policy – Boston University considers the most important safeguards with respect to passwords to be (i) complexity, (ii) each user-level account has no more than one assigned user responsible for that account, and (iii) secrecy. To maintain secrecy, passwords should never be written down or disclosed to others.

2.1. All administrator-level passwords (e.g., root, enable, system administration, application administration accounts, etc.) must be changed at least once per 90 days.

2.1.1. The Information Security group of Information Services & Technology (IS&T) will maintain a list of users with knowledge of these administrative passwords.

2.1.2. When (i) a user with knowledge of administrative passwords terminates employment with Boston University or a Covered Entity (CE), or (ii) a user's need for administrator-level access expires, the related password(s) must be changed.

2.2. All user-level passwords will be changed at least every 180 days.

2.3. Password cracking or guessing may be performed on a periodic or random basis by the Information Security group, HIPAA Security Officer, or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change the password.

3. Password Construction – Users should be aware of how to select strong passwords.

3.1. Strong passwords have the following characteristics:

- ☐ contain both upper and lower case characters (e.g., a-z, A-Z)
- ☐ have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:"';<>?,./)
- ☐ are 10 or more alphanumeric characters long with a minimum of 15 alphanumeric characters for local MS Windows accounts

BOSTON UNIVERSITY

- ☐ are not a word in any language, slang, dialect, jargon, etc.
- ☐ are not based on personal information, names of family members, etc.

3.2. Weak passwords have the following characteristics:

- ☐ contain fewer than ten characters
- ☐ are words found in a dictionary (English or foreign)
- ☐ examples include:
 - the names of family members, pets, friends, co-workers, fantasy characters, etc.
 - computer terms and names, commands, sites, companies, hardware, software
 - the words "Boston University", "boston", or any derivation of the various CE names

4. Password Protection Standards

4.1. Passwords must never be written down or stored on-line.

4.2. Do not use the same password for Boston University accounts as for other non-Boston University access (e.g., personal ISP account, option trading, benefits, etc.).

4.3. Do not share passwords with anyone, including IS&T employees, administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Boston University information.

4.3.1. If someone demands a password, refer them to this document or have them call someone in the Information Security group.

4.4. Do not use the "Remember Password" feature of applications (i.e., email, Internet Explorer).

4.5. If an account or password is suspected to have been compromised, report the incident to the Information Security group and change the passwords.

5. Application Development Standards

5.1. Application developers must ensure their programs contain the following security precautions. Applications should:

- ☐ support authentication of individual users
- ☐ not store passwords in clear text or in any easily reversible form.
- ☐ provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

BOSTON UNIVERSITY

6. Remote Access

6.1. Remote access to the servers containing ePHI must be done through the Boston University VPN.

BOSTON UNIVERSITY

Modification Control Sheet

Rev	Date	Author	Description of Modification
0.0	20100429	David Hutchings, IS&T Information Security	Changed all references to "University Information Systems" and "Information Systems and Technology" to "Information Services & Technology".