

 Information and Communications Technology Division	Standard	
	Effective Date	Date of Last Revision
	August 2, 2005	August 18, 2005
Chapter Name	Chapter Number	
8.0 SECURITY	8.1 S	
Title		
8.1 S Password Standards for Electronic Systems		

1.0 Purpose

The purpose of these password standards is to set the minimum requirements for selecting, changing, expiring, and modifying passwords for electronic systems at Eastern Michigan University.

2.0 Governing Policy/Procedure/Guideline	
Number/Name	Effective Date
8.1 Password Policies for Electronic Systems	April 26, 2005

3.0 Standards

General

- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least once every six (6) months.
- All system-level passwords (e.g., root, admin, administrator, application administration accounts, etc.) must be changed at least every four (4) months.

Supported Systems

The dissemination of the exact criteria for password generation will compromise its effectiveness. Therefore, it has been determined that the standards will not be posted for public review or discussion. Password guidelines are provided to assist in creation of a password that is secure and will meet the mandatory requirements. The Password Standards for Electronic Systems is located on ICT's internal policy site for those staff members who need this information to perform their jobs.

Other Electronic Systems

- User accounts that have system-level privileges granted through group memberships or programs (such as 'sudo') must have unique passwords.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to as many of the "Supported Systems" standards as possible.
- Passphrases should be relatively long and contain both upper / lowercase characters, numeric and punctuation and should conform to as many of the "Supported Systems" standards as possible.

Password Protection Standards

Do not use the same password for Eastern Michigan University accounts as for other non-Eastern Michigan University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for multiple Eastern Michigan University accounts.

Do not share your Eastern Michigan University passwords with anyone for any reason at any time. If someone demands a password, refer them to this document or have them contact the Director IT, Security Administration. ICT technical staff will NEVER ask for your password. In order to assist you, they may be required to establish a new password while they are working on an issue and will then provide you with that password. It will be your responsibility to change the password immediately.

Do not permanently store passwords in any file (written or electronic) including e-mail messages, Palm Pilots or similar devices (unless encrypted according to the Acceptable Encryption Policy).

Establish challenge questions/answers to allow for self-password resetting whenever possible. These should be vague enough to not allow for easy guessing and unique to the individual. These must be entered EXACTLY the same each time they are used.

If an account or password is suspected to have been compromised, report the incident immediately to the Director IT, Security Administration.

Password cracking or guessing may be performed on a periodic or random basis by Network Engineering or its delegates. If a password is guessed or cracked during one of these scans, the user account will be disabled until the password has been reset.

Application Development Standards

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

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should 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.
- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

4.0 Responsibility for Implementation

ICT Director of IT Security Administration and ICT Director IT, Network and Systems.

5.0 Definitions	
<u>Term</u>	<u>Definition</u>
Passphrases	<p>Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."</p> <p>Most often used to secure public/private key authentication for more secure transactions. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.</p>
Challenge Questions / Answers	<p>Challenge questions can be generated by the system (or user) and contain a vague question for the user to supply an answer.</p> <p>Most often used for forgotten password self-service.</p>
Supported Systems	<p>Systems that are controlled by the NSure Identify Management System or those ERP systems which contain password maintenance systems capable of meeting the password requirements.</p>

Other Electronic Systems	Hardware or software systems that do not have the capability to meet the “Supported System” password standards. ERP systems must have written approval for the Director IT, Security Administration to not meet the “Supported System” standards.
--------------------------	---

6.0 Revision History			
<u>Requestor</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Barr	Draft 1 of Password Standards	July 26, 2004	
Barr	Draft 2 of Password Standards	August 2, 2004	
Barr	Draft 2A of Password Standards – minor revision to remove red type. Need to consider Help Desk Password Change standards.	December 9, 2004	
Putney	Draft 3 of Password Standards	July 19, 2005	
Putney	Draft 3a of Password Standards	July 21 st , 2005	
Dorendorf	Removed Secure Information and added content	July 28 st , 2005	August 2, 2005
Laundra	Copyedited/proofed for upload	August 18, 2005	