

 Password Addendum	NETWORK SECURITY		
	Doc. Version:	1.0.0	Page 1 of 2
	Revised by:	John Baxter	Date: 8/29/04
	Effective Date:	10/12/2004	
	Approval:	W. R. Rice, Chancellor & C. Fitch, CIO	

1.0 Responsibility

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk.

As a result, all UTHSC faculty, students, employees are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

2.0 Purpose

The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

3.0 Scope

This policy applies to all UTHSC users who have or are responsible for a computer account, or any form of access that supports or requires a password, PIN, pass-phrase, etc., on any system that resides at any UTHSC facility, has access to the UTHSC network, or stores any non-public UTHSC information.

4.0 Policy

4.1. General

1. Passwords should be changed every 6 months.
2. System-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) shall be changed quarterly and be different from the user's other passwords.
3. Old passwords shall not be re-used for the next 12 months.
4. Passwords shall conform to the guidelines outlined below.

4.2. Strong Password Construction Guidelines

1. Passwords must contain (8) or more characters including three of the following: upper and lower case letters, numerals, or special characters..
2. Passwords must not be:
 - words from dictionaries, in English or any other language
 - publicly known slang, jargon or common use words
 - names of family, pets, friends, co-workers, fantasy characters, etc.
 - computer terms and names, commands, sites, companies, hardware, software
 - geographical words such as "UTHSC", "sanjose", "sanfran" or any derivation
 - birthdays and other personal information such as addresses and phone numbers

	NETWORK SECURITY		
	Doc. Version:	1.0.0	Page 2 of 2
	Revised by:	John Baxter	Date: 8/29/04
	Effective Date:	10/12/2004	
Password Addendum	Approval:	W. R. Rice, Chancellor & C. Fitch, CIO	

- word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc
- any of the above spelled backwards
- any of the above preceded or followed by a digit (e.g., secret1, 1secret)

4.3. Password **Protection Guidelines**

1. Passwords must be treated as confidential information. No employee should give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members. Don't reveal a password over the phone to anyone or on a questionnaire, security forms, or the like.
2. If someone demands your password, refer them to this policy or have them contact the IT Department.
3. Passwords must not be transmitted electronically over the unprotected Internet, such as via e-mail. Passwords may, however, be used to gain remote access to company resources via the company's Virtual Private Network or SSL-protected Web site.
4. Users must not keep an **unsecured** written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled safe area or in an encrypted file if in electronic form.
5. Do not use the "Remember Password" feature of any application or web site.
6. Passwords used to gain access to company systems must not be used as passwords to access non-company accounts or information.
7. If possible, don't use the same password to access multiple company systems.
8. If an employee either knows or suspects that his/her password has been compromised, it shall be reported to the department manager and the password changed immediately.

5.0 **Enforcement**

Reference **Enforcement** section of Acceptable Use document.

6.0 **Additional Information**

Any inquiries relating to this Password Addendum should be directed to the Security Director.