Password

Best Practice

This document describes guidelines for selecting strong passwords and protecting them from unauthorized disclosure.

Draft Date: September 25, 2008

OBJECTIVE

This document outlines the best practices for the creation, maintenance, and protection of passwords for University of Tennessee Information Technology (IT) resources. Strong passwords are an integral part of ensuring authorized access to user accounts and IT resources. A poorly chosen password can result in the compromise of the confidentiality, integrity, and availability of the University of Tennessee IT resources. Therefore, all users are responsible for taking the appropriate steps, as outlined below, in the construction, maintenance, and protection of their passwords.

SCOPE

Individuals Covered

This policy applies to all students, faculty, staff, and others--referred to as "users" throughout this policy--who access, use, or handle the university's IT resources. "Users" include but are not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities or individuals who are granted access.

Resources Covered

This policy applies to all university IT resources, whether individually controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or provided by the university or otherwise connected to university IT resources. This includes but is not limited to networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, whether used for administration, research, teaching, or other purposes. This policy also applies to all personally owned devices used to store, process, or transmit university information or that are otherwise connected to university IT resources.

COMPLIANCE

At minimum, individual university units (e.g. campuses or institutes, departments, colleges, and divisions) must follow these principles and rules while connected to university IT resources. Each unit is responsible for security on its systems and may apply more stringent security standards than those detailed here, provided these do not conflict with or lower standards or requirements established by the IT security strategy, policies, or best practices.

Any non-compliance with the university's IT security strategy, policies, or best practices must be reported to the position of authority (POA) or their designee for IT at the respective campus/institute or the Information Security Office (ISO). The contact information for both entities, the ISO and the POA, can be found at http://security.tennessee.edu/. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. The ISO will work with Human Resources and Student Judicial Affairs to develop and implement appropriate sanctions for non-compliance. Issues that cannot be resolved by the ISO will be directed to the Vice President for Information Technology. Critical non-compliance issues will be directed to the Audit Committee of the Board of Trustees.

INFORMATION AND SYSTEM CLASSIFICATION

University faculty, staff, and students often have a business need to collect, transmit, store, or process information. Protecting the confidentiality, integrity, and availability of this information is the responsibility of the entire university. The *Information Classification Policy (IT0115)* and *System Classification Policy (IT0116)* formalize this responsibility and define a framework for categorizing information and computer systems according to the perceived risk to the university.

University policies mentioned in this document can be found from the *University of Tennessee Policy Search Page* at http://www.tennessee.edu/policy/. Best practice documents are referenced from the *Information Security Office* home page at http://security.tennessee.edu/.

GENERAL PRACTICES

The following general practices are detailed below and provide the foundation for sound password management principles:

- Passwords should meet or exceed complexity requirements based on the risk.
- Passwords should be changed frequently based on risk.
- Passwords should be protected from exposure.

PASSWORD COMPLEXITY

Strong passwords are required for all accounts issued by The University of Tennessee. All passwords, including initial passwords, must be constructed, implemented, and maintained according to the following guidelines:

- Strong passwords contain a minimum length of (8) characters and are composed of at least three of the following characteristics (using all four is encouraged):
- At least one numeric character (0-9)
- At least one lower case character (a-z)
- At least one upper case character (A-Z)

- At least one non-alphanumeric character* (~, !, @, #, $, %, ^, &, *, (,), -, =, +, ?, [,], {, })

**Be aware that some university systems may not support non-alphanumeric characters or only support a specific subset.*

STRONG PASSWORDS

When constructing a password, remembering these guidelines can increase its strength:

- **Do not** use words in any language, slang, dialect, jargon, etc.
- **Do not** use personal information such as names (relatives, pets, etc.), or dates such as birthdays or anniversaries.
- **Do not** use words, phrases, or acronyms associated with the university (e.g., "vols", "mocs", "uthsc", "skyhawks")
- **Do not** use computer terms, commands, sites, or software applications (e.g., "banner", "iris", "andi", "coeus")
- **Do not** use word or number patterns (e.g., "aaabbb", "qwerty", "zyxwvuts", "123321", "abc123", etc.)
- **Do not** increment previous passwords by prepending/appending additional characters ("oldpassword1", "1oldpassword", etc.)

Strong Passwords can be easily created using Mnemonics. This process provides the ability to create a password that cannot be easily guessed but remain simple enough for a person to remember.

For example, "one fish two fish red fish blue fish" becomes "()F2f|2Fbf" (this and other examples should not be used as they are very common examples used for instruction). Books and movies provide great passwords, as do phrases such as "I-40 was slow as molasses this morning", which becomes "I40W$aMtM". Further examples include:

- Msi5Yon! — My Son is 5 years old now!
- Ihli(f5yN — I have lived in California for 5 years now
- Fa$t4Ward — Fast Forward
- BB#s4034 — Basketball numbers 40 and 34

PASSWORD CHANGE FREQUENCY

Regularly changing passwords is a sound security principle that adds to the overall security of university IT resources and systems. Depending on the classification of information particular passwords should be set to expire at regular intervals. Passwords for newly activated accounts must be changed on first use.

The following table indicates the required frequency of password changes based on the classification of information:

Public	Proprietary	Confidential	Highly Confidential
180 days	90 days	60 days	Contact the ISO

PROTECTION OF PASSWORDS

All passwords must comply with the following:

- Default passwords must be changed to conform to this best practice prior to deployment of all software applications, systems, and other IT devices on the university network.
- System administrators must validate the identity of the user prior to performing a password reset on the user's account.
- System administrators must issue passwords via a secure communication channel. E-mail is not considered a secure communication channel.
- Users must never share or reveal passwords with or to anyone (e.g., supervisor, a spouse, child, or secretary). Shared accounts are thus prohibited.
- Passwords must not be displayed, stored, or transmitted in plain text (e.g., authentication requests, unencrypted protocols, batch files, automatic log-in scripts, software macros, terminal function keys, devices without access control).
- Passwords must not be stored in any location where unauthorized individuals might discover or obtain them.
- If a user suspects their account has been compromised, the password on that account or system and all other accounts or systems using that same password must be changed immediately.

Other "**Do not's**" include:

- **Do not** reveal a password to ANYONE
- **Do not** reveal a password in an email message
- **Do not** talk about a password in front of others
- **Do not** hint at the format of a password (e.g., "my family name")
- **Do not** reveal a password on questionnaires or security forms
- **Do not** share a password with family members
- **Do not** reveal a password to co-workers while on vacation
- **Do not** write down your password and store it in plain view or in any other insecure location
- **Do not** store passwords in a file on ANY computer system without encrypting the file

As a general rule, there are no **legitimate** reasons that a password should be revealed by any method to any person. The only notable exception to this rule is a situation where a user is being assisted **in person** by a **known** and **trusted** university IT support person. After assistance has been rendered, the user should **immediately** change the shared password. Social engineering attacks generally rely on a user's trust of IT support personnel to obtain passwords.

The Information Security Office, or its designee, will perform various password auditing, cracking, or guessing efforts on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change that password. If the same password is used to access other systems, it is recommended that the user change the password on all systems where it is used. All other unauthorized attempts to "break", "hack", "crack", or otherwise determine a user's password are prohibited.

OTHER PASSWORD RELATED SECURITY BEST PRACTICES:

- ***Account Lockout:*** all accounts should be set to "lock out" a user after a maximum of 5 incorrect password or failed login attempts
- ***Lockout Threshold:*** the minimum "lock out" time should be set to five (5) minutes
- ***Password History:*** systems should be configured to require a password that is different from the last ten (10) passwords