ITS POLICIES AND GUIDELINES
CATEGORY: Security, Privacy, Information Access & Management
STATUS: Approved

POLICY TITLE: **Password Management Policy**

POLICY PURPOSE:
This policy establishes conditions for use of, and requirements for appropriate security for Truman accounts and passwords. These requirements are necessary to protect University IT systems and data and to ensure that all users are aware of their responsibilities in effective password management.

APPLIES TO:
- All members of the Truman State University community
- Anyone granted access to Truman State University data, systems or networks

---

Contents:

POLICY STATEMENT:
The University shall develop, implement, and regularly review a formal, documented process for appropriately creating, modifying and safeguarding passwords used to validate a user's identity and establish access to the University's information systems and data.

The University's password management processes will include the following requirements:
- System-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed at least every 90 days. System level passwords on stand-alone or unshared systems may not need to be changed with the same frequency. For example, local user accounts who have administrative privileges on their workstations.
- User-level passwords for important systems/user roles (e.g. IT staff, key finance users) must be changed at least every 90 days. Certain areas or job functions may require more frequent password changes and therefore fall into this category.
- All general user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 180 days. The recommended change interval is every 90 days.
- User accounts may not have system-level privileges with the exception of those users that have administrative privileges on their own workstations.
- Users that can justify system-level privileges must request a separate admin account giving them specific system-level permissions for their applicable areas. Exceptions must be approved in writing by ITS.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of network resources. As such, users (including contractors and vendors with access to Truman systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Individual responsibilities include:
- Create a strong password; see General Password Requirements.
- Do not use the same password for Truman accounts as for other non-Truman access (e.g. personal ISP account, option trading, benefits, etc.).

- Where possible, do not use the same password for different Truman accounts (i.e., do not use the general user-level password for system-level or user-level accounts on important systems).
- It is the individual's responsibility to safeguard the password. Do not share Truman passwords with anyone. All passwords are to be treated as sensitive, confidential Truman information and should not be written down or stored on a computer system where they might be easily acquired by others. (Passwords stored on a computer system should always be encrypted.)
- Account owners are held responsible for all activities associated with their accounts.
- Passwords should not be inserted into non-encrypted email messages or other forms of non-encrypted electronic communication.

General Password Requirements
Passwords for network accounts must meet the following minimum requirements:

- Maximum age of 180 days
- Not contain all or part of the user's account name
- Be at least eight characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, ! $, #, %)
- Be different than the previous fifteen passwords

Other system accounts may have password requirements that vary from the minimum requirements stated above. Whereever possible, minimum password requirements should meet industry best practices.

Password Expiration
Truman requires that all general user-level passwords be changed at least every 180 days and all user-level passwords for important systems/user roles much be changed at least every 90 days. ITS strongly encourages all individuals to change their password before it expires, in order to avoid disruption of access to University services. Passwords can be changed at https://secure.truman.edu/password/.

Thirty days before the password expires, ITS will send an e-mail notification informing the individual of the impending password expiration date. This email notification will be sent again fifteen days before the password expires, a week before the password expires and then daily until the password is changed.

In addition to the University's password expiration requirements, a password should be changed immediately if an account owner believes that it has been compromised (for example, if there is a possibility that another person may have viewed or acquired the password.)

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:
Any exceptions to this policy must be approved in writing by ITS.

CONSEQUENCES:
By failing to abide by this policy or policy procedures, individuals may be subject to sanctions, up to and including the loss of computer or network privileges, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

CONTACTS:
Responsible Executive: Provost and Vice President for Academic Affairs
Responsible Office: Information Technology Services

Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	Truman State University President
APPROVED ON:	2016/12/01
EFFECTIVE ON:	2016/12/01
REVIEW/CHANGE HISTORY:	2010/06/03, 2011/02/03, 2013/11/12
REVIEW CYCLE:	Annual

DEFINITIONS:

General user-level passwords are for day to day use of the University information technology resources. These accounts will not have system level privileges with the exception of users that have administrative privileges on their own workstations.

ITS – Information Technology Services

System-level passwords are used for managing and administering the University's information technology shared resources and include any account that holds more privileges then a regular user account. This would also include any account whose sole purpose is the administration, upkeep and maintenance of its associated system and any account that has the ability to change the configuration of a shared system.

User-level passwords for important systems include individuals whom, as a core responsibility of their role or position, have access to sensitive data, functionality, and systems. These areas could include, but are not limited to, University financial information, employee or student records and information technology resources. Certain areas or job functions may require more frequent password changes and therefore fall into this category.

RELATED DOCUMENTS:

KEYWORDS: