



UT Space Institute Policy: IT1002-SI – Password Standard	
Version: 2	Effective Date: 08/01/2019

Objective

This standard contains requirements and recommendations for all system passwords, including servers, workstations, and network devices, for UTSI. Each user and/or administrator is required to implement the system password definitions listed in this document.

Scope

This standard applies to all users of and information technology (IT) resources owned, operated, or provided by The University of Tennessee Space Institute (UTSI) including its remote centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this standard is based on those guidelines. Specifically, this standard is based on guidelines in NIST SP 800-53 Rev4, *Recommended Security Controls for Federal Information Systems and Organizations*.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

UTSI must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This standard is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.



SPACE INSTITUTE

UT Space Institute Policy: IT1002-SI – Password Standard	
Version: 2	Effective Date: 08/01/2019

Protection

Passwords must never be written down or recorded. No user should ever share or divulge their password to anyone. Each user is accountable and responsible for any action taken with that user's username and password. No university employee or administrator should ever ask a user for their password, and if such an action takes place, the user should not reveal it to anyone, no matter how plausible the reason. Any password that is known to be compromised or suspected to be compromised must be changed immediately.

Minimum Requirements

Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

Passwords must be at least twelve characters in length.

Passwords must contain characters from all of the following four categories (IA-5):

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)

Complexity requirements are enforced when passwords are changed or created. If your password does not meet requirements you will receive a notification to submit a new request.

Expiration

All passwords generated within UTSI for access to Internal Use Only or Proprietary information must be set to expire at a maximum of every 180 days.

Passwords issued for temporary accounts, password resets, and locked out IDs must all be reset to expire immediately so the user will be forced to change their passwords at their first login opportunity (IA-5).

Uniqueness

Where technically feasible, a history of at least ten (5) passwords must be kept within the system for each password generated (IA-5). This uniqueness forces users to create a new password that is unique over a longer time period.



SPACE INSTITUTE

UT Space Institute Policy: IT1002-SI – Password Standard	
Version: 2	Effective Date: 08/01/2019

Inactive Accounts

Accounts not accessed in a year are considered inactive. Active Directory must be checked quarterly for inactive accounts. All inactive accounts found will be disabled. Disabled Active Directory accounts will be deleted at the next quarterly check.

Work and Personal Separation

Users should never use the same passwords between university/work and personal accounts. This creates the risk of unauthorized parties gaining access to university systems.

Recommendation

It is highly recommended that users implement unique passwords for each account (IA-5). It is common practice for threat actors to try compromised credentials in multiple services to gain access to additional accounts. Never reuse credentials that have been compromised.

Account Lockout

An account will be locked out after five (5) bad password or login attempts in fifteen (15) minutes (AC7). The account will remain locked for fifteen (15) minutes once it is locked.

Display and Printing

The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them (IA-6).

Cracking

Users must not attempt to "break", "hack", "crack", or otherwise determine another users' password. This applies to passwords for students, faculty, staff, friends and accounts on systems reached through the Internet.



SPACE INSTITUTE

UT Space Institute Policy: IT1002-SI – Password Standard	
Version: 2	Effective Date: 08/01/2019

Encryption

For security purposes, passwords used for access to proprietary or confidential information will not be sent across the network in 'clear text' format. Passwords used for access to proprietary or confidential information must not be listed in clear text for the purpose of automating a login sequence. All passwords must be stored in an encrypted format by the OS, DBMS, or application.

NOTE: All encryption methods and technology must comply with any international regulations governing this technology.

Retrieval

Computer and communication systems must be designed, tested, and controlled to prevent the retrieval of stored passwords, whether they appear in encrypted or plain text form.

Information System Installation

Default authenticators must be changed upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation (IA-5).

Exceptions

Some systems may not be able to comply with this policy due to restrictions of password length or unsupported characters. For these systems, an exception must be noted and approved by the Security Team.



UT Space Institute Policy: IT1002-SI – Password Standard	
Version: 2	Effective Date: 08/01/2019

Discretionary Controls

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

- Unsuccessful Login Attempts (AC-7): Enforces a limit of consecutive invalid logon attempts by a user during a specified time period.

References

IT0132 – *Identification and Authentication*

NIST SP 800-53 Rev4 *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-63B *Digital Identity Guidelines - Authentication and Lifecycle Management, Appendix A – Strength of Memorized Secrets*

Definitions

Cracking - Refers to using various methods to reveal a password with the intent of accessing a computer, system, or service to which one is not authorized.

Encryption - The process of converting information or data into a special form to prevent unauthorized access. Password - A string of characters that must be supplied by a user in order to gain access to a computer, computer system, or electronic device. Also referred to as a Memorized Secret.

Password Manager - An application used to organize, encrypt, and generate passwords.

Threat Actor - An entity, internal, external, or partner, that is partially or wholly responsible for an incident that impacts, or has the potential to impact, the safety or security of another entity, person, or organization.

Two-Factor Authentication (2FA) - A method of confirming a user's claimed identity by requiring a combination of two different components, which includes something you know (password, PIN), something you have (smart card, token), and something you are (biometrics).