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.

UTM 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.
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.

For all new accounts, your UTSI username will be the first letter of your first name and up to seven characters of your last name. Your username will be determined from the information you gave above. Whenever we receive your request a temporary password will be sent to the new user that must be changed upon setting up your account.

Passwords must be at least eight characters long and must contain upper and lowercase letters and numerals.

Please provide the name of your supervisor/advisor. In case your username already exists in our directory, or we need to contact you, please provide us a means to do so.

Passwords must meet the following minimum requirements:

Not contain the user’s account name or parts of the user’s full name that exceed two consecutive characters.
Be at least eight characters in length.
Contain characters from all 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, !, $, #, %)

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.