Policy	Password Guidelines
Impact	Data, Technology, and IT Resources
Responsible Office	IT Services
Created	January 8, 2012
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

PASSWORD GUIDELINES

PURPOSE

Shepherd University is dedicated to ensuring the privacy and proper handling of user passwords on all affiliated Shepherd University information assets and IT resources.

GUIDELINES

Access to Shepherd University information assets and IT resources are governed by role-based permissions of all users as it pertains to network access, wireless access, e-mail access, and affiliated applications that leverage the campus single-sign-on capabilities (SSO).

Shepherd University mandates all faculty, staff and affiliates to change their primary, network/email password twice a year, with a minimum of 180 days between each change. Students are encouraged, but not mandated, to regularly change their passwords. Users may elect to change their passwords more frequently.

Passwords may be used only by the authorized user. Passwords and user accounts may not be shared with others. User account owners are responsible for all actions performed from their account. Passwords should never be written down or stored electronically in plain text.

All passwords must adhere to the following standards:

1. Must be at least eight (8) characters in length.
2. Must include at least one (1) lower-case letter.
3. Must include at least one (1) upper-case letter.
4. Must include at least one (1) numeral.
5. Must include at least one (1) special character (e.g. $,#,!,@).
    a. Please note passwords may not begin with a special character.
6. Must be changed at least every 180 days.
7. Should not be an older or reused password.

Shepherd University IT Services will never ask users to disclose their passwords for any reason.

HOW TO CHANGE PASSWORDS IN RAIL

RAIL is a user self-service portal that enables users to make necessary changes to their accounts and perform other self-service functionality (e.g. pay tuition). Users may access RAIL by visiting the Shepherd University website and clicking on RAIL in the Quick Link section. To access RAIL, users will need their 9-digit Shepherd University ID number (SUID) and PIN. The SUID number is also reflected on the back of users Rambler Card. The PIN is not the same as the user password. The PIN would have been setup initially by the user. If users fail to recall their PIN, they may need to contact the Office of the Registrar to have it reset at 304.876.5463 or 800.344.5231.

Once in RAIL, users need to:

1. Go to Personal Information.
2. Select Password Management.
3. Click on Change Password
    a. Please note the password must follow the above-mentioned guidelines
4. Log out of RAIL.
    a. Please note, users need to wait a minimum of five (5) minutes before logging back into any Shepherd University network, information asset, or IT resource, to account for the new password to update within all systems.

PRIVACY, OPERATIONS, and MONITORING

Shepherd University is dedicated to ensuring the privacy and proper handling of passwords of its students, faculty, staff, and affiliates.

Shepherd University seeks to maintain its IT environment and manage all information assets including data, computing devices, systems technology, telephony, and IT resources in a manner that respects individual privacy and promotes user trust. However, the use of Shepherd University IT resources is not completely private, and users should have no expectation of privacy in connection with the use of any information asset or IT resource.

Shepherd University has the legal right to access, preserve, and review all information stored on or transmitted through any information asset or IT resource, including the inspection of e-mail messages, logging of activities, monitoring usage patterns, and data audits/integrity checks. IT Services may, with or without notice to users, take any other action it deems necessary to preserve, secure, and protect systems, information assets, or IT resources for the betterment of Shepherd University. Without limiting its right to take action, Shepherd University may, at its sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy, including the contents and records of individual communications, to appropriate Shepherd University personnel and/or law enforcement agencies.

SCOPE of AFFECTED PARTIES

These guidelines apply specifically to faculty, staff, and affiliated users; however, students may elect to adhere to this guideline at their discretion.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Understand and comply with the guidance provided here, as well as applicable compliance programs and affiliated awareness trainings.
- Promptly report any suspected violation or breach of confidentiality, along with any security events, and/or incident to itworkorder@shepherd.edu.

CIO/CISO - INFORMATION PRIVACY OFFICER

- Oversee and administer this guideline.
- Facilitate the review of requests for a security policy exception.
- Develop awareness and necessary training materials as it pertains to this policy.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in this policy.

RELATED TOOLS

RELATED POLICIES & GUIDELINES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- E-Mail Policy
- Information Security & Privacy Policy
- Work from Home / Remote Access Guidelines