Information for New Users

SMUMN Password Requirements

General Information

Password management is done through the SMUMN Portal. To ensure passwords do not get out of sync (Portals, Canvas, Active Directory, and Google Workspace), Saint Mary's has ONLY implemented the password change settings via the Portal, which is the main way users access the system. This protocol ensures that when users change their passwords, it gets updated in all other places as well.

The Portal and Active Directory accounts are set to lockout after 10 attempts and unlocks after 10 minutes.

Active Directory accounts that are not in the portal (ex: contractor/vendors) do not have access to the portal so their passwords are set to expire annually.

Saint Mary's University uses the National Institute of Standards and Technology (NIST) for best practice guidelines.

Policy Statements

1. Passwords must be 15 characters in length. Special characters, numbers and upper/lower case characters are not required.

2. Passwords will expire every 365 days.

3. When changing a password, the user must not change it to the most recent password.

4. Passwords are to be used and stored in a secure manner. Passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.

5. Passwords are to be individually owned and kept confidential, and are not to be shared under any circumstances.

Investigations and Consequences

Alleged violations of this policy by students of the College will be investigated by the vice president for student affairs or their designee. The assistant vice president for IT or their designee will assist in investigations, as appropriate. The use of technology may be suspended during an investigation if staff believe that inappropriate use has occurred. Inappropriate use will be handled using the disciplinary judicial process outlined in the College Student Handbook.

Alleged violations of this policy by students attending in the Schools of Graduate and Professional Programs will be investigated by the dean of the academic area/school in which the student is studying. The assistant vice president for IT or their designee will assist in investigations, as appropriate. The use of technology may be suspended during an investigation if staff believe that inappropriate use has occurred. Inappropriate use will be handled using the Grievance Procedure in the most recent Schools of Graduate and Professional Programs Catalog and Student Handbook.

Alleged violations of this policy by employees will be investigated by the employee's supervisor in coordination with the assistant vice president for human resources or their designee. The assistant vice president for IT or their designee will assist in investigations, as appropriate. The use of technology may be suspended during an investigation if staff believe that the inappropriate use has occurred. Violation of this policy by employees will be handled according to established procedures in the Saint Mary's Employee Handbook, under the Work Rules and Conduct Standards and the Corrective Action sections. The university supports the theory of corrective action and retains

Information for New Users

discretion to take action that is appropriate to the particular circumstances. Violations of rules or policies may result in corrective measures that, depending upon the circumstances and at the discretion of the university, may include verbal or written warnings, suspension (with or without pay), or immediate discharge. These corrective measures do not constitute an exclusive list of possible actions and may be repeated, skipped or taken out of order.

Sanctions for non-compliance may include legal action according to applicable laws and contractual agreements.

For questions regarding your password please contact the IT HelpDesk at 507-457-7800.

Unique solution ID: #1496
Author: n/a
Last update: 2024-08-02 18:25