Password Policy

TABLE OF CONTENTS

Purpose

All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data as well as to help protect the University's computing resources and infrastructure. This policy establishes a minimum standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this Policy applies to all businesses within Saint Leo University globally.

Audience

The Policy applies to all Saint Leo University personnel, and contractors. The term "personnel" refers to all full-time, part-time, interns, students, temporary employees attending or hired directly by Saint Leo University and on the Saint Leo University payroll. Also, the term “contractor” refers to anyone who is on another University’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.).

Throughout this Policy, “Saint Leo University,” “Saint Leo,” “our,” “we,” and the “University” refer to Saint Leo University. “Personnel”, “contractor”, “you” and “yours” refer to you as an employee/ representative of Saint Leo University.

This Policy applies to Saint Leo University, all wholly owned subsidiaries, subsidiaries in which Saint Leo University has a controlling interest.

Compliance & Enforcement

Compliance with this Policy is mandatory and applies to all Saint Leo University personnel and contractors globally including at any of its subsidiaries or units as well as authorized representatives.

Saint Leo University reserves the right to modify the Policy at its sole discretion.

All Saint Leo University personnel and contractors are responsible for complying with this Policy. A violation of this Policy may result in disciplinary action, up to and including termination. Violators may also be subject to legal action, including civil and/or criminal prosecution. Saint Leo University also reserves the right to take any other action it believes is appropriate based on the severity of the infraction.

This Policy also represents a statement of intent, any behavior or act violating the spirit of this Policy is also subject to disciplinary action in a fashion similar to a policy violation. Saint Leo University personnel and contractors should also note that with specific authorization and approval from senior management, there are some business programs or services which are exempt from portions of this Policy. Saint Leo University Personnel and contractors must contact their manager or supervisor if they do not understand this Policy, are unable to comply with this Policy, or have questions regarding Policy.

Policy Statements

1. General

1.1. Passwords to University accounts and devices must be kept confidential.

1.2. To preserve account integrity, the owner of the account should be the only person with knowledge of the password.

1.3. No user is required to share a University account password with another individual; including but not limited to managers, co-workers, or technical staff.

1.4. Notification of password expiration will be provided to account holders 7 days in advance and every day after until password expiration if you log into the Saint Leo portal.

2. Technical Standards

2.1. Passwords will expire every 90 days

2.2. Passwords to systems containing sensitive information, including electronic Protected Health Information (ePHI) and Personal Identifiable Information (PII) must expire no less often than every 180 days.

2.3. Passwords should be at least 6-12 characters in length.

2.4. Passwords to systems containing sensitive information, including ePHI must be at least 8-12 characters in length.

2.5. Strong passwords should be used. A strong password will include a combination of:

2.5.1. Alphabetic, including both upper and lower case: *A to Z* and *a to z*.

2.5.2. Numeric: *0 to 9*.

2.5.3. Spaces are not permitted

2.5.4. Special Characters such as are valid: !#$^_*.,-

2.6. Passwords to systems containing sensitive information, including ePHI, must require at least two of the three criteria specified immediately above.

2.7. Passwords should not consist solely of personal information or words found in a dictionary (any language). Ideally, this information should not be used. If used, the use of at least two of the three types of strong password characters noted above as part of the password is required.

3. Illegal Activities

3.1. Under no circumstances is a Saint Leo University personnel authorized to engage in any activity that is illegal under local, state, or federal law while using Saint Leo University resources.

4. Communications

4.1. Questions regarding this Policy should be directed to the Saint Leo University Security Team.

4.2. This policy shall be made available to all Saint Leo University personnel and contractors as applicable to their role and function within Saint Leo University.

Legal Conflicts

Saint Leo University policies were drafted to meet or exceed the protections found in existing laws and regulations, and any policy believed to be in conflict with existing laws or regulations must be promptly reported to the Saint Leo University Grand Counsel.

Exceptions

Exceptional circumstances occur from time to time. In these situations, consult Saint Leo University Security Team for guidance.

Comments

N/A

Related Documents

-

References

Mandates

- Payment Card Industry Data Security Standard

Revision History

Revision Level	Date
1.0	2013 February
1.1	2013 February