DT-30-2023-RE

SAGRADO
Universidad del Sagrado Corazón

Password Management Procedure

Effective: 2023.06.01

I. Purpose

This Procedure describes the cybersecurity processes for protecting passwords and credentials at Universidad del Sagrado Corazón ("University" OR "Sagrado") according to the Password Management Policy.

II. Definitions

1. Information System – Any system that belongs to the University and that can be accessed through a computer or similar devices.

2. Member of the University Community - includes any person or legal entity who has an interest in the University's Mission, institutional activities and/or operations (e.g., trustees, faculty, administrative staff, student support services staff, students, stakeholders, third-party, suppliers and vendors).

3. Password - a secret word or phrase that must be used to gain access to an Information System.

III. Roles and Responsibilities

1. Board of Trustees
   - Approves Capital and Operational Budget for Information Technology.
   - Via the audit committee oversees risk management practices and security risks identified by the CIO.
2. Executive Leadership
   - Manages Expenditures for Information Technology
   - Communication Path to Staff and Faculty
3. Chief Information Officer (CIO)
   - Communicates information security risks to executive leadership.
   - Reports information security risks annually to university leadership and gains approval to bring risks to acceptable levels.
   - Establishes an information security framework and awareness program.

4. User
   - Responsible for complying with this Procedure.

IV. Proceedings

At a minimum, the Integrate Information Technology Office (ITI for its Spanish acronym) will enforce the use of strong passwords to authenticate user identities. This specifically includes the use of strong passwords when logging into confidential systems.

1. Password rotation schedules will be used. Passwords may not be reused for at least 12 password change periods and changed passwords cannot use the same phrase with simple changes like "Password1" to "Password2."
2. All roles will require users to change passwords at least every 90 days. Any exceptions to this requirement must be documented and approved by the CIO.
3. All systems and applications will ensure that user sessions expire after 15 minutes of inactivity and require re-submission of the user's password to re-activate the session. Exceptions must be approved by the CIO.
4. The University's information resources will never display, transmit, or store a password in clear text that can be viewed by a third party.
5. First-time passwords (e.g., passwords assigned by ITI administrators upon account creation or during password resets) must be set to a unique value per user and changed immediately after first use.
6. All passwords will be encrypted during transmission and storage on all system components.
7. Password procedures and policies will be distributed to all users who have access to the University's information.

In the event of a password compromise or suspected compromise, an user must immediately change all passwords on the University's issued accounts. It is recommended to change passwords on personal accounts as well.

A. General Password Construction Guidelines

1. Passwords must use alpha and numeric characters, must be at least 8 characters in length, no longer than 32 characters in length, and require the use of three out of four of the following:
    - Capital letters
    - Lower case letters
    - Numbers
    - Special characters
2. Passwords may use all special characters but there is no special requirement to use them.
3. The following passwords are not allowed:

- Passwords with more than 2 sequential and repetitive characters (e.g. 12345 or aaaaaa).
- Context-specific passwords (e.g. the name of the site, etc.).
- Commonly used passwords (e.g. p@ssw0rd, etc.).

B. Weak passwords have the following characteristics.

1. The password is a word found in a dictionary (English or foreign)
2. The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words University, Universidad, Sagrado or any derivation thereof.
    - Birthdays and other personal information such as addresses and phone numbers.
3. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
4. Any of the above spelled backwards.
5. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

C. Password Protection Standards

1. Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Sagrado's information.
2. Passwords should never be written down or stored online without encryption.
3. Do not reveal a password in email, chat, or other electronic communication.
4. Do not speak about a password in front of others.
5. Do not reveal a password on questionnaires or security forms.
6. If someone demands a password, refer them to this document and direct them to ITI.
7. If an account or password compromise is suspected, report the incident to ITI.

V. Interpretation of this Procedure

This Procedure is approved by the Chief of Information Officer with the advice and counsel of the office of the General Legal Counsel. Questions about the scope and interpretation of this Procedure should be directed to the office of Information Technology at 787.728.1515, ext. 8044.

If there is any ambiguity in any provision of this Procedure, the University reserves the discretion to interpret it in accordance with the purpose for which it was established, the impact to the University's operations and good faith, unless otherwise provided by law.

VI. Reporting Violations

Violations to this Procedure should be directed to the office of the office of Compliance, Internal Audit and Institutional Integrity at cumplimiento@sagrado.edu. Any violations to this Procedure will be addressed in accordance with the Sagrado's policies and procedures.

Raúl Rosado
Chief Information Oficer