SAGRADO
Universidad del Sagrado Corazón

Policy on Identification and Authentication Systems

Effective: 2019.January.01

I. Purpose

This Policy states the requirements for identifying and authenticating users of Universidad del Sagrado Corazón (Sagrado/University) computer systems and networks and describes centrally-supported identification and authentication facilities.

II. Applicability

This Policy is applicable to all University students, faculty and staff, and all others using the University's information technology resources ("users").

III. Identification and Authentication

All users of Sagrado computer systems and networks must develop and implement access control policies to ensure the security and integrity of both University data and data belonging to individuals.

It is Sagrado's policy that all University business for which computer-based forms and actions have been released will be done using those computer-based systems; paper forms are no longer accepted. This Policy applies to all aspects of qualifying transactions including initiation, routing, processing by Academic Departments, Administrative Offices, and offices that provide Student Services, and transmissions. Secure identification of the participants in all such transactions is crucial to the successful conduct of University business.

A. Identification: General

Authentication is the secure identification of system users. The University is responsible for determining which authentication method to use.

1. Linked Identifiers

Sagrado maintains a set of linked records identifying all employees, students, and others who use the University's Information Technology Resources.

2. Management of Identifiers

a. *Uniqueness*. Each identifier ("Sagrado User ID") is unique; that is, each identifier is associated with a single person.

b. *One Identifier per Individual.* An individual may have no more than one Sagrado User ID number and one personal email, except when expressly authorized by the President for valid reasons.

c. *Non-Reassignment.* Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.

B. Identification: Sagrado User ID

1. Sagrado Network Identifiers

The Sagrado User ID consists of alphabetic characters and digits and is assigned by the University.

2. Eligibility for Sagrado User ID

- Authorized, registered students, as defined by the Registrar
- Full-time faculty and part-time faculty
- Administrative staff
- Temporary and casual faculty and staff
- Student Services staff
- "University sponsored guest", subject to the following conditions:
    - The ID is to be used by a specific, named individual requiring access to University computing resources in support of legitimate University work.
    - The ID is sponsored by a faculty member, a manager as defined by Human Resources, or an individual who has been expressly granted the privilege to sponsor.
    - The sponsor accepts responsibility for ensuring that the sponsored ID is used in support of work consistent with the University's mission and in a manner consistent with the University's policies.

3. Establishing a Sagrado User ID

Sagrado User IDs are established and maintained via online procedures. Note that employees and students must have a University ID number in order to obtain a Sagrado User ID.

C. Identification: University ID

An eight-digit University identification number is automatically assigned to regular, continuing employees by the Automatic Data Processing system and to students by the Jenzabar system.

D. Authentication

1. Authentication Methods

Authentication methods involve presenting both a public identifier (such as the Sagrado User ID) and private authentication information, such as a Personal Identification Number (PIN), password, or information derived from a cryptographic key.

2. Eligibility for Authentication Entry

A User must be associated with an entry in the authentication service to be able to use the systems and services.

a. *Sagrado User ID*. Eligibility for an entry in the authentication service begins when the individual accepts the offer of student registration or employment. Eligibility ends when a person's active association with the University ends; i.e., when an employee is no longer employed or a student is no longer registered.

b. *University Sponsored Sagrado User* ID. The University may grant a Sagrado User ID for a specific period of time. The sponsor determines the length of sponsorship; sponsorship must be renewed to keep the ID valid. There is no grace period: the entry becomes invalid immediately at the end of the sponsorship period.

c. *Reactivation*. An entry may be reactivated if the individual subsequently rejoins the University, either via regular association or sponsorship.

d. *Suspension*. The use of an authentication entry may be revoked if it is used in a manner inconsistent with Sagrado policies or if an individual is subject to other administrative action that denies them University privileges.

IV. User Responsibilities

1. Official Actions

Use of the authentication service to identify oneself to an on-line system constitutes an official identification of the user to the University, in the same way that presenting an ID Card does. Users can be held responsible for all actions taken during authenticated sessions.

2. Integrity

Regardless of the authentication method used, Users must use only the authentication information that they have been authorized to use and must never identify themselves falsely as another person or entity.

3. Confidentiality

Regardless of the authentication method used, users must keep their authentication information confidential and must not share or make it available for use by unauthorized persons.

4. Reporting Problems

Anyone suspecting that their authentication information has been compromised must immediately contact the Chief Information Officer at 787.728.1515, ext. 3571, or by electronic mail at luis.gotelli@sagrado.edu.

5. Security Precautions

Users are strongly encouraged to change their password regularly (at least once every three months), to limit possible abuse of passwords that may have been compromised without the user's knowledge. Passwords should be chosen so that they are not easily guessable, for example, not be based on the user's name or birth date.

V. Violations to this Policy

Universidad del Sagrado Corazón reserves the right to interpret this Policy in its administration, implementation and application. Any violation of this Policy by a student, faculty or staff or any other person may result in a disciplinary action that may include expulsion from the University (students) or termination of the employment relationship (faculty and administrative staff), or other appropriate legal actions.

If there is ambiguity in any provision of this Policy, the University reserves the discretion to interpret it according to the purpose for which it was established, the impact on the operations of the University, and good faith, unless any law provides otherwise.

Gilberto J. Marxuach Torrós
President