DT-73-2024-PE

SAGRADO
Universidad del Sagrado Corazón

Bring Your Own Device Policy

(BYOD)

Effective: 2024.10.01

I. Purpose

This policy is to establish Universidad del Sagrado Corazón's standard for the use of personal electronic devices for working activities, which include but are not limited to connecting personal mobile devices to the University's network, apps, and others electronic media, either on premises or remotely; it is also designed to ensure compliance with standards for devices and networks, preventing information from being transmitted over insecure networks where it could potentially be accessed by untrusted parties or being insecurely stored on any personal device.

II. Regulatory Context

Federal and state laws, regulations, and other institutional policies related to electronic information privacy, including but not limited to, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Gramm- Leach-Bliley Act.

III. Scope

This policy applies to authorized personnel who use personal devices to access the University's electronically stored information or information systems. Such access is considered a privilege to the employee. Therefore, employment at the University does not automatically grant permission to use these devices to gain access to institutional networks, electronically stored information, and information systems.

IV. Definitions

1. **Authorized User** – any user with the required permissions to access an information system.

2. **Bring Your Own Device ("BYOD")** - It refers to a policy that allows employees to use their personal devices for work and can access company network, apps, and resources.

3. **Electronically Stored Information ("ESI")** - any documents or information that are stored in electronic form. Common examples of ESI include word processing documents, spreadsheets, digital photographs, videos, emails and their attachments, text and instant messages, communications conducted in ephemeral messaging applications or in workplace collaboration tools Information stored in databases.

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

5. **Mobile Device** – refers to any electronic device that could connect to a wired or wireless network. Examples of those devices will be defined in the procedures created for such effects.

6. **Members 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, support services staff, stakeholders, third-party, suppliers and vendors).

7. **Personal Identifiable Information** – information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information allowing the physical or online contact of a specific individual is the same as personally identifiable information. This information can be kept in either paper, electronic or other media.

V. General Policy

The University adheres to all legal requirements related to the privacy and integrity of its information systems and electronically stored information. The Integrated Information Technology Office (ITI for its Spanish acronym) is the unit in charge of the development of procedures to enforce this policy. As such, it will be responsible for the following subject matters: Risk Assessment, Development of BYOD (Bring Your Own Device) procedures.

It is the responsibility of all members of the University Community who uses a personal mobile device to access institutional resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any personal mobile device that is used to conduct University's business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

VI. Interpretation of this Policy

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

If there is any ambiguity in any provision of this Policy, 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.

VII. Reporting Violations

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

Gilberto J. Marxuach Torrós
President