



Bring Your Own Device Procedure (BYOD)

Effective: 2024.10.01

I. Purpose

This procedure is based upon the Policy of BYOD (the “Policy”) and provides a detailed framework for the secure use of personal devices by authorized users to access Universidad del Sagrado Corazón’s network and resources, specifically through Microsoft 365, Google Suite, and Forti VPN with FortiToken. The goal is to ensure compliance with security protocols and the safeguarding of institutional data when accessed from personal devices.

II. Regulatory Context

This procedure adheres to federal and state regulations regarding electronic information privacy, such as FERPA, HIPAA, FCRA, and the Gramm-Leach-Bliley Act, as each are defined in the Policy. Additionally, it complies with institutional policies governing data protection and network security. The use of personal devices to access Microsoft 365, Google Suite, and Forti VPN must meet these regulatory standards to ensure that sensitive information is not compromised.

III. Scope

This procedure applies to authorized personnel who use personal mobile devices to access the University’s electronically stored information or information systems. Such access is a privilege, not a right. 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 individual approved by the University to use a personal device for accessing institutional resources.
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)** – Documents, spreadsheets, emails, and other data stored in digital form within the University’s systems.
4. **Information System** – University-owned systems and electronic media licenses accessed through personal devices, such as but not limited to, Microsoft 365, Google Suite, and Forti VPN.
5. **Mobile or Personal Device** – Any personal device (e.g., smartphones, tablets, laptops) used to connect to the University’s wired or wireless networks.
6. **FortiToken** – A security token used for multi-factor authentication (MFA) to access University systems.

V. General Procedures

1. Device Registration
 - a. Authorized users must register their personal devices with the ITI office.
 - b. Device details such as operating system, security features (encryption, antivirus), and compliance with University policies will be documented.
 - c. Access to University Resources
2. Microsoft 365:
 - a. Access Microsoft 365 apps via web portals or mobile apps.
 - b. MFA using FortiToken is required for all access points.
 - c. Synchronization of sensitive data to unencrypted personal devices is prohibited.
3. Google Suite:
 - a. Access to Google Suite apps (Gmail, Drive, Docs) is allowed with FortiToken-based MFA.
 - b. ITI will enforce data loss prevention policies, especially when accessing sensitive data.
4. Forti VPN:
 - a. Personal devices must use Forti VPN to access University resources remotely.
 - b. FortiToken MFA will be required to authenticate VPN sessions.
 - c. Devices without up-to-date security patches will be denied access.
5. Device Security Requirements. Devices must be secured by:
 - a. Passwords, PINs, or biometric authentication.
 - b. Full-device encryption to protect institutional data.
 - c. Installation of Mobile Device Management (MDM) for remote management and data wipe in case of device loss or theft.
 - d. Regular system and security updates.
6. Prohibited Activities
 - a. The use of public Wi-Fi without connecting through Forti VPN is prohibited.
 - b. Storing University data on personal cloud services (e.g., Google Drive, Dropbox) is strictly forbidden.
 - c. Unauthorized users must not access University systems through an authorized user’s personal device.


7. Monitoring and Compliance
 - a. The ITI office will regularly monitor personal device access to ensure compliance with this procedure.
 - b. Violations (e.g., unregistered devices, disabling MFA) will result in the immediate suspension of access.
8. Support and Training
 - a. ITI will provide training on securely using Microsoft 365, Google Suite, and Forti VPN securely with FortiToken MFA.
 - b. Users will receive regular security updates and compliance reminders.

VI. Interpretation of this Procedure

This Procedure is implemented by the Integrated Information Technology (ITI) office under the direction of the University President. Questions about the interpretation or application of this procedure should be addressed to ITI at 787.728.1515 ext. 8044.

VII. Reporting Violations

Violations to this procedure 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