árido software	Bring Your Own Device Policy	Code: PO-02
		Version: 0
		Date: 11-02-2026

Bring Your Own Device (BYOD) Policy

Version: 0.0
Last reviewed: 11/02/2025
Approval status: To be approved in management review

1. Objective

The objective of this Bring Your Own Device (BYOD) Policy is to enable employees to use personally owned devices for work purposes in a way that protects the confidentiality, integrity, and availability of the Organization's information and systems. This policy establishes the minimum security, compliance, and operational requirements for connecting and using personal devices to access Organization data, applications, and networks, and defines the conditions under which BYOD access may be limited, revoked, or subject to approved exceptions based on device or platform constraints.

2. Scope

This BYOD Policy applies to all employees who use personally owned devices to access, store, process, or transmit Organization information, or to connect to Organization networks, systems, applications, or cloud services, whether on-site or remotely.

3. Policy Statement

The Organization grants its employees the privilege of purchasing and using devices of their choosing at work for their convenience. The Organization reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

4. Acceptable Use

- The Organization defines acceptable business use as activities that directly or indirectly support the business of the Organization.
- The Organization defines acceptable personal use on working time as reasonable and limited personal communication or recreation, such as reading or game playing.
- The Organization does not define acceptable personal use on non-working time, such as break time, lunch time, and off-the-clock time because that is your personal time.

Comentado [GC1]: aclarar que llos usuarios se van a comprometer a enviar capturas anualmente como evidencia que windows defender esta funcionando en su dispositivo.
crear una carpeta en sharepoint para guardar las evidencias

Comentado [GC1R2]: evidencias del acknowledment/aceptacion de esta misma politca
podemos hacer un forms con el link
o por mail

Comentado [GC1R3]: nuevos ingresantes deberan leer la politica como proceso de onboarding

Comentado [GC1R4]: agregar link a la carpeta de evidencias en este documento.

tarea anual (sistema interno de tickets/tareas) para IT manager, para que revise las evidencias y asi mantener el seguimiento

Comentado [GC1R5]: cualquier cambio de device debe ser informado a la compañia

Though, to the extent you are accessing social media sites, you are required to follow the Organization's Social Media Policy.

5. Rules

- Employees are not allowed to access certain websites during work hours/while connected to the corporate network at the discretion of the Organization. Such websites include, but are not limited to the following non-exclusive list of websites:
  - Pornographic websites or other similar websites that contain illicit materials or materials of a sexual nature;
  - Online gaming websites;
  - Sites typically known to contain malware links;
  - Certain social media networking sites;
  - Others.
- Devices' camera and/or video capabilities are not disabled while on-site.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to another Organization;
  - Harass others;
  - Engage in outside business activities;
  - Engage in any activity that would violate the Organization's policies;
  - Others.
- Employees may use their mobile device to access the following Organization-owned resources: email, calendars, contacts, documents, etc.
- Employees are requiered to submit screenshots annually as evidence that their devices are up to date with the latest updates.
- Employees must notify the company or any change of device used for work purposes.

Comentado [GC2]: review

6. Devices and Support

- Smartphones including iPhone, Android and Windows phones are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

7. Reimbursement

- The Organization will not reimburse the employee for a percentage of the cost of the device (include the amount of the Organization's contribution), or the Organization will contribute X amount of money toward the cost of the device.
- The Organization will not reimburse the employee for the following charges: roaming, plan overages, etc.

Comentado [GU3]: Ver si aplican

Comentado [GC3R2]: No aplica - no hay reintegros

8. Security

- All devices used for the Organization's business or on behalf of Organization must be registered with and authorized by [PERSON/POSITION] in the [DEPARTMENT NAME] Department, inclusive of owner information.
- The employee must install applicable security software upon Organization's request and consent to Organization's efforts to manage the device and secure its data.
- The device must comply with Organization's device configuration requirements.
- Password protect the device through the use of strong passwords consistent with Organization's current password policies and procedures.
- The device must lock itself with a password or PIN if it is idle for [10] minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the Organization's list of approved apps. [TODO]
- Smartphones and tablets that are not on the Organization's list of supported devices are not allowed to connect to the network. [TODO]
- Employees' access to Organization data is limited based on user profiles defined by IT and automatically enforced as stablished in PO-03
- Employees shall not back up or otherwise store the Organization's content locally or to cloud-based storage or services without Organization's consent. Any such backups or other stored copies of Organization content inadvertently created must be deleted immediately. To the extent you create backups or otherwise store Organization content with Organization's consent, you must provide Organization with access to your local or cloud-based storage to access and review any such backups or other stored copies of Organization content when requested or required for Organization's legitimate business purposes, including in the event of any security incident or investigation.

Comentado [GU4]: Hacer mencion a la politica de contraseñas

Comentado [GU5]: Política de control de acceso

Comentado [GC5R2]: PO-03 Access Control Policy.docx

9. Disclaimers

- It is the employee's responsibility to take precautions, such as backing up email, contacts and code commits/push to remote repositories.

- Lost or stolen devices must be reported to the Organization within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Organization's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Organization and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The Organization reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

árido software	Bring Your Own Device Policy	Code: PO-02
		Version: 0
		Date: 11-02-2026

[OPCIONAL]

BRING YOUR OWN DEVICE (BYOD) POLICY ACKNOWLEDGMENT

Employee Name: _____
Employee Position: _____
Date of Receipt of Bring Your Own Device (BYOD) Policy: _____

I acknowledge and agree that:

1. I have received a copy of the Organization Bring Your Own Device (BYOD) Policy;
2. I have read the Bring Your Own Device (BYOD) Policy in its entirety and fully understand the provisions contained therein; and
3. I agree to abide by the provisions contained in the Bring Your Own Device (BYOD) Policy.

Employee's Signature

Employee's Name (Printed)

Date