

WeServ
Bring Your Own Device Policy
WS-ISMS-PO-011

This document is classified as **Fujitsu-Restricted** Only.

Objective

- This policy aims to define a set of guidelines in allowing employees to use their smartphones, and other mobile devices solely for work-related activities except for personal laptops or desktops, while maintaining the security and integrity of the organization's data and technological infrastructure.
- This policy is also implemented with high regard to the protection of the employee, company and customers information and shall apply to work performed on any personal device on the company's behalf during and outside working hours, within and off WeServ's premises.

Intended Readers

- All WeServ Employees

Policy

ACCEPTABLE USE OF DEVICE(S)

1	WeServ defines acceptable business use as activities that directly support the objectives of the organization. The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
2	Employees' access to company data shall be limited based on user profiles defined by IT and automatically enforced. Employees are blocked from accessing non-work-related websites during work hours/while connected to the corporate network at the discretion of the company.
3	The employee shall always use his/her device(s) in an ethical manner and adhere to the company's acceptable use policy.
4	<p>In furtherance, employees who intends to use a personal device, shall adhere to the following guidelines:</p> <ul style="list-style-type: none"> • All personal devices used shall be registered with the local IT department and authorized/approved by the employee's Direct Manager, RBU Head and Head of Information Security or Security Lead. If there is project related information or access to customer information with the use of personal mobile device(s), approval of customer will be also required. • All approved and registered personal mobile devices shall be managed by Microsoft Intune, a Microsoft Endpoint Manager. • It shall be the employee's responsibility to take additional precautions, such as backing up email, contacts, etc. to prevent loss of personal data. • Employees shall use their mobile device only to access company-owned resources: email, calendars, contacts, documents, etc. • Employees shall not use their mobile device for any illegal activity (e.g., storage or transmission of illicit materials, storage or transmission of proprietary information belonging to other companies, harassment, engaging in outside business activities). • Passwords shall be required to unlock personal mobile devices. Minimum password length shall be eight (8), combination of alpha, numeric and special characters. • Employees may opt to follow the standard naming convention recommended by

This document is classified as **Fujitsu-Restricted** Only.

	<p>IT for the device. If standard naming convention is not followed, it is recommended that employee will change the name of the device to reflect his name when attending virtual meetings.</p> <ul style="list-style-type: none"> Employees are prohibited to allow use of the device, such as use of Outlook, One Drive, Teams, and other Microsoft 365 applications where the company or work account is logged-in by anyone not authorized by WeServ, including the employee's family, and friends outside of work and other non-work-related activities. Work products or sensitive business content shall not be saved in the personal device, and as such, should be deleted if inadvertently downloaded to the personal device. Employees are prohibited to back up their personal device to cloud-based storage or services without prior consent. Such cloud-based storage shall be accessed and reviewed in the event of a security incident investigation. In the event that personal mobile devices need to be brought to Repair Shop or Repair Technician, any of the following security measures should be considered by employee: <ul style="list-style-type: none"> Perform hard reset or factory reset configuration before endorsing or leaving the phone to technician for repair that will take more than one (1) hour Passcode or password or any screen lock protection (PIN, Pattern, Biometrics, etc.) should not be shared or disclosed to technician. Request IT to perform remote retire via Microsoft Intune before endorsing the device for repair
--	---

DEVICES AND SUPPORT

1	Smartphones & Tablets shall be allowed, provided that the devices shall be presented to IT for assessment, configuration, and installation of standard applications, software, and security tools, such as Microsoft Intune before they can be provided access to the network.
2	Jailbroken (Apple) or Rooted (Android) devices shall not be allowed. The device's original operating system shall be retained and kept current with security patches and updates.
3	Local I.T. will only provide support for any access issues to Fujitsu network using their personal mobile device. Connectivity issues, operating system or hardware-related issues are beyond the scope of local I.T. but employee should inform local IT if there is any need for repair by other Third Party.
4	To prevent any financial ambiguity, WeServ shall not shoulder the cost of the repair of the device, nor the cost of the device itself, nor cover the cost of the data plan coverage used for the device. The employee shall be personally liable for all costs associated with the personal mobile device.

TECHNICAL REQUIREMENTS


1	<p>The following minimum compliance and configuration policies should be met prior to approving or allowing the use of personal mobile device.</p> <p>Users are advised to update and patch the smart device on regular basis as advised by OEM with stable version and or recommended in this policy document</p>
----------	--

This document is classified as **Fujitsu-Restricted** Only.

1.1	Platform	iOS	Android
	Minimum OS Version	15.0 or Higher	10.0 or Higher
	Rooted Devices	Blocked	Blocked
	Jail Broke devices	Blocked	Blocked
	Require a password to unlock mobile devices	Required	Required
	Required password type	Alpha Numeric	Alpha Numeric
	Minimum password length	8	8
2	Other technical requirements may be referred to the following global policies and may be subject to change without prior notice:		
	a) InTune Device Compliance Policy		
	b) InTune Device Configuration Policy		

SECURITY

1	Personal devices that will be used shall be installed with Mobile Device Management software (i.e., Microsoft Intune) to manage the device and secure its data.
2	<p>Intune managed Android/iOS devices to be used in accessing email and collaboration services shall be allowed access to Office 365 and Mobile Microsoft Office 365.</p> <ul style="list-style-type: none"> Intune managed Android/iOS devices to access corporate and business delivery information shall NOT be allowed access to ZinZai, FJ Global, One ERP, Local Data Center Applications. <ul style="list-style-type: none"> ZinZai, FJ Global, One ERP, Local Data Center Applications shall be only allowed access through company issued laptops or desktops. Any use of personal laptops or desktops to access the above-mentioned applications shall only be thru the approved Virtual Desktop Infrastructure (VDI) set-up which is not part of this policy Access to business delivery applications shall be based on Client Specific Guidelines or Local Service Request (LSR)
3	<p>Microsoft Authenticator shall be enabled on all approved Corporate & Personal devices.</p> <ul style="list-style-type: none"> Microsoft Authenticator (For employees consenting the application be installed and enabled on their personal device)
4	Employees shall comply with approved device configuration and password protection requirements. Configuration requirements shall include mandatory settings for device encryption, the installation of corporate applications, password length and complexity, automatic device lock, minimum Operating System version and others.
5	Employees shall not alter the security settings, device and storage encryption, password protection, password complexity and length of the device without prior consent.
6	As a security requirement, the device shall be set to lock after five (5) failed login attempts. PIN shall be required to unlock devices that have been idle for five (5) minutes.


	<h1>Bring Your Own Device Policy</h1>		
Document No.: WS-ISMS-PO-011	Effective Date: November 24, 2022	Version: 1.00	Page 5 of 6

This document is classified as **Fujitsu-Restricted** Only.

7	Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
8	The employee's device shall or may be remotely wiped if the personal device is lost or stolen.
9	When the employee has been terminated or resigned from the company, InfoSec will perform remote wipe or retire from Intune to remove access to company information. The said device will also be removed or deleted by InfoSec from Intune.
10	In the event of any security incident and investigation, employees shall promptly provide IT with relevant logs and/or allow access to their personal mobile device in his presence. The employee shall also allow collection of evidence(s) such as but not limited to screenshots, copy of emails, pictures, documents, and other pertinent information that may be necessary for investigation
11	<p>In the event that the personal mobile device of employee needs to be disposed or sold to other party, any of the following security measures shall be performed:</p> <ul style="list-style-type: none"> • Logged out company provided Microsoft account from personal mobile device and perform hard reset or factory reset configuration. • Inform and request from InfoSec to perform complete remote wipe to the device <p>In addition, any SD card attached to the device shall be formatted and removed from the personal mobile device.</p>
12	Any employee found to install Outlook or Teams and setup Intune Company Portal in their personal device without approval from Management and InfoSec is considered as unauthorized access and personal device will be immediately removed from Intune without prior notice to employee. Such action of the employee may also require separate investigation from InfoSec, CCO and HR for any disciplinary action that may be imposed for violating the Company Code of Conduct.

RESPONSIBILITIES

1	To ensure that this policy is established, effectively monitored, and continuously improved, the following responsibilities are tasked to the Local IT and Information Security Group											
2	<table><tr><th>Local I.T.</th><th>Information Security Group</th></tr><tr><td>Verifies the compliance of the device connected</td><td>Regularly tests and verifies that remote wipe functionality is maintained</td></tr><tr><td>Monitors only approved and authorized devices that are part of Intune container</td><td>Generates monthly/quarterly report to be in compliance with EARC</td></tr><tr><td>Wherever possible, update the smart devices with antivirus solution (Defender of Android)</td><td></td></tr><tr><td>Ensures that the JML process checklist should include all the required controls to onboard/offboard smart devices</td><td></td></tr></table>		Local I.T.	Information Security Group	Verifies the compliance of the device connected	Regularly tests and verifies that remote wipe functionality is maintained	Monitors only approved and authorized devices that are part of Intune container	Generates monthly/quarterly report to be in compliance with EARC	Wherever possible, update the smart devices with antivirus solution (Defender of Android)		Ensures that the JML process checklist should include all the required controls to onboard/offboard smart devices	
Local I.T.	Information Security Group											
Verifies the compliance of the device connected	Regularly tests and verifies that remote wipe functionality is maintained											
Monitors only approved and authorized devices that are part of Intune container	Generates monthly/quarterly report to be in compliance with EARC											
Wherever possible, update the smart devices with antivirus solution (Defender of Android)												
Ensures that the JML process checklist should include all the required controls to onboard/offboard smart devices												

	<h1>Bring Your Own Device Policy</h1>		
Document No.: WS-ISMS-PO-011	Effective Date: November 24, 2022	Version: 1.00	Page 6 of 6

This document is classified as **Fujitsu-Restricted** Only.

RISKS, LIABILITIES & DISCLAIMERS

1	Employees shall agree to the terms and conditions set forth in this policy to be able to connect their personal devices to the company network. WeServ reserves the right to revoke this privilege if users do not abide by the policies outlined herein and shall disconnect devices or disable services without notification.
2	WeServ reserves the right to monitor, intercept, access, record, review, and erase, without further notice, all content created on, transmitted to, received, or printed from, stored, or recorded on the personal device(s) using authorized application(s).
3	WeServ may also store copies of such content for a period after they are created and may delete such without notice. In addition, the company may obtain and disclose contents of the personal device(s), including personal content, for litigation or investigations of any reported security incident(s).
4	Employees shall assume full liability for risks that may render the device unusable. This may include, but is not limited to, the partial to complete loss of company, customer and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors.
5	WeServ shall not be responsible for any losses or damages to the device, its software, and/or its functionality, resulting from its use for the company's business purposes.
6	<p>Nonconformance to this policy is subject to the corresponding disciplinary actions set forth in the Code of Conduct.</p> <p>Every user is accountable for any action that can be traced to Smart devices. Every user has a responsibility to keep Personal devices secure and is responsible for the consequences of not keeping it so.</p>

Definition of Terms

Terms	Description
Mobile Device	A piece of portable electronic equipment (smartphone, tablet), small enough to hold and operate in the hand, which can connect to the internet. Handheld computer devices will typically have an LCD or OLED flat screen interface, providing a touchscreen interface with digital buttons and keyboard or physical buttons along with a physical keyboard.

Change History

Version No.	Issue Date	Modified By	Description of Changes	Reviewed/ Approved By	Change Ref. No.
0.01	09-01-2022	K. Jimenea	Initial Draft		
1.00	11-23-2022		Official Release	I. Lerma; S. Cariño; V. Ramiro; A. Gregorio	56