©(ORGANISATION NAME)

BRING YOUR OWN DEVICE

(BYOD) POLICY

Subject: Bring Your Own Device (BYOD) Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 13	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	**Signature**	**Date**
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

Organisation recognizes the benefits that can be attained by allowing users use their own electronic devices for work, whether at home or while travelling. Such devices include laptops, smartphones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. The use of such devices to create and process the Organisation's information and information assets needs to be addressed, particularly in information security, therefore ensuring that technical restrictions are imposed on accessing the Organisation provided services on BYOD.

The Organisation must ensure it remains in control of the data for which it is responsible for, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering users to ensure that they protect their own personal information.

1.1 PURPOSE

The purpose of this policy is to:

- Set guidelines for user conduct, necessary to protect the privacy, security and integrity of the Organisation's information and information assets against the risks that can arise when users use their personally owned devices for business purposes. It aims to mitigate the following potential risks:
    - Loss or theft of mobile devices, leading to unauthorised access to sensitive data stored on them.
    - Exposure of confidential or classified information through public observation of device screens.
    - Introduction of malware or viruses into the Organisation's network via insecure mobile devices.
    - Damage to the Organisation's reputation due to security incidents involving personal mobile devices.

  It is crucial that the controls outlined in this policy are strictly adhered to when using and carrying Bring Your Own Device (BYOD) mobile devices. The decision to use a personal device for business purposes should be a joint agreement between the Organisation and the device owner. Such usage is not mandatory, and employees have the right to decide whether the additional controls imposed by the Organisation on their personal devices are acceptable. If an employee deems the controls unacceptable, they may choose not to use their personal device for business-related activities.

1.2 OBJECTIVES

The objectives of this document include:

- Maintaining confidentiality and integrity of information and information assets.
- Maintaining Data Privacy and protection of all information on personal devices.
- Protection of devices against unauthorised access and disclosure.

1.3 SCOPE

This policy is applicable to every user, personnel that are granted access/privileges on the company's premises, information, and information systems; these include permanent staff, temporary/contract staff, consultants, vendors and other third parties. Breach of this policy may warrant disciplinary measures, up to and including termination of employment/contract.

This Policy applies to, but is not limited to, all Organisation-owned and personal mobile devices and accompanying media that can potentially hold the Organisation's information, for example:

- Laptops.
- Tablets/Notebooks.
- Mobile Phones, Smart Watches.
- Portable audio-visual equipment such as cameras and music players.

1.4 POLICY DETAILS

- The Organisation reserves the right to refuse access to personal devices where it considers that there is a security or other risk to the Organisation.
- Control should be put in place to ensure that no information which has been classified as Confidential, Private, or Internal shall be accessed on any personal device without due authorisation.
- Users are not allowed to download or transfer sensitive business data to their personal devices.
- Should the personal device be lost or stolen, the Incident Management Policy is to be followed and necessary authorities shall be contacted as is deemed necessary.
- The Information Security department should be informed where the use of personal devices is required to join the corporate network to access the Organisation's information and resources. Users are expected to get approval which is inclusive of the duration to make use of the personal device from their manager which will be presented to Information security department to ensure the Organisation's Endpoints Detection and Responses (EDR) and Data Loss Protection (DLP) are installed on all personal devices

to create a better visibility and allow for security monitoring and control edge over their devices.

- Information security team is tasked to inform the IT team and the network management team before installing any software/application used for the Organisation's work before granting the device access to the corporate network because, by default, the company does not trust any alien device to be connected to its network.
- All users are expected to protect personal devices used for work-related purposes from loss, damage, or theft.
- All users are advised to limit the number of emails and other information being synced to the device.
- All users shall remove all Organisation information from the device and return it to the manufacturers' settings before they sell, exchange, or dispose of the device.
- The Organisation will not be responsible for the loss or damage of personal applications or data resulting from the use of Organisation applications.
- Employees' access to Organisation's data is limited based on the user profile, defined by their supervisor, and implemented by IT. Users are only allowed to use their personal devices to access the information authorised for that employee.

All users must take appropriate security measures under the Organisation's acceptable use Policy including but not limited to:

- Ensuring that their personal device is password protected using the features of the device and that a "strong password," as defined in the Password Policy, is required to access the Organisation's network and information.
- Ensuring that their BYOD device locks itself with a password or PIN if the device is idle for one minute.
- Ensuring that their BYOD device shall be locked after three failed login attempts.
- Not sharing their BYOD devices with friends, relatives, etc.
- Not storing or transmitting illicit material or proprietary information belonging to another Organisation.
- Using their BYOD devices to access only authorised information following the Organisation authentication and authorization procedures.
- Maintain the BYOD device by ensuring it is regularly patched and updated.
- Users are expected to enable the disk encryption feature on their personal workstations to mitigate unauthorised data access due to lost or stolen devices.
- Report lost, misplaced or stolen BYOD devices to the IT department within immediately not less than 24 hours.
- Report any security breach immediately to the Information Security Team in accordance with the Information Security Policy.
- Users are expected to exercise the same discretion in using their personal devices as is expected for the use of the Organisation's official devices.

- The Organisation has the right, at any time, to monitor and preserve any communications that use its networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.
- No user may knowingly disable any organisation network software or system identified as a monitoring tool.
- The use of your own device MUST adhere to the Organisation's Acceptable use policy and Information Security Policy.
- It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.
- Upon resignation or termination of employment, users are expected to remove all Organisation's data or information on personal devices. The IT team is also task with this responsibility.

The general principle of this policy is that the degree of control exercised by the Organisation over the BYOD device will be appropriate to the sensitivity of the data held on the device.

Guidance to decide who should have access to what information and on which device is summarised in the table below.

TABLE 1: BYOD GUIDANCE

Information category	Examples	Who may have access via BYOD	Types of BYOD devices	Required controls	Comments
Level 0 - Public	Product catalogues, pricing information, company location addresses and contact numbers	Anyone	Any	None	This information is generally available to the public and accessed via publicly accessible means e.g., a website
Level 1 - Protected	Internal procedures, product details, internal company communications e.g., non-	Employees and other approved stakeholders	Laptops (Windows 8 or later) Tablets (IOS x / Android y or later)	Device password protection Inactive lock	This area is the most likely use of BYOD within the Organisation

	restricted or confidential email		Smartphones (Apple iPhone 5 or later, Blackberry)	Remote wipe Application password protection Periodic audits	
Level 2 - Restricted	HR information, bank details, personal information covered by data protection legislation	Restricted groups of employees	Laptops only (Windows 8 or later)	Full disk encryption VPN Automated patching Anti-virus Firewall Regular audits	This information may be accessible via devices with strict security controls. This may practically preclude the use of a BYOD device depending on the circumstances
Level 3 - Confidential	Company resourcing plans, commercial proposals, unpublished financial information	No-one	None	Not applicable	This information may be accessible via Organisation-provided devices with strict security controls

1.5 AUDIT AND MONITORING

To ensure data is adequately protected, it is important for an Organisation to be able to monitor and audit the level of compliance with this policy. The level of monitoring and audit will be appropriate to the classification of the information held on the device.

The methods and timing of monitoring and audit should be such that the device owner's privacy is not invaded and should be in line with applicable privacy legislation. In general, monitoring of usage outside of business hours should be avoided.

In the event of the device being lost or stolen, the owner must inform the IT service desk as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. As a security precaution, the Organisation reserves the

right to remote wipe the device where possible. This may involve the deletion of non-business data belonging to the device owner.

Upon leaving the Organisation, the device owner must allow the device to be audited and all business-related data and applications removed.

1.6 BYOD TERMS OF USE

As a user of a BYOD mobile device, you agree to comply with the following terms of use.

1.6.1 PHYSICAL PROTECTION

- You must ensure that the device is transported in a protective case and is not exposed to situations in which it may become damaged.
- Do not leave the device unattended or expose it publicly, for example, on the car seat or in a meeting room or hotel lobby.
- Ensure the device is securely stored, and the key is kept in a safe.
- Register your device for any available remote locate and wipe facility and record details of how this will be achieved if required.

1.6.2 ACCESS CONTROLS

- You will not hold classified information on the device unless this has been authorised and appropriate controls (e.g., encryption) is in place.
- Do not keep access tokens, Personal Identification Numbers, or recovery keys other security items on the device except if passworded.
- Ensure that the device screen locks after a short period (preferably after 1 minute) of not being used and requires an access code, PIN or password to unlock it.
- Passwords used should be strong and difficult to guess.
- No unsecured logons (i.e., those that do not require a password) that give access to classified information should be set up on the device.
- You should not attempt to “jailbreak” the device so that the supplier’s security controls are disabled.
- You may be asked to return the device to the IT Service Desk at any time for inspection and audit.

1.6.3 CRYPTOGRAPHIC TECHNIQUES

- Where possible, secure your device so that all the data on it is encrypted and only accessible if the key is known.
- If the encryption is already enabled on the device, do not disable it.

1.6.4 BACKUPS

- Ensure local device files are regularly backed up to the corporate network.
- Do not create unsecured backups of classified information to a personal cloud storage.

1.6.5 VIRUS PROTECTION

- Where applicable, virus protection for your device must be provided and updated on a regular basis.
- Do not disable virus protection on the device.
- You should only purchase and install apps from a reputable source, preferably Google Play for Android devices or App Store for iOS devices.

1.6.6 NETWORK CONNECTION

Avoid connecting (manually or automatically) to unfamiliar or free wireless networks, especially in public locations such as airports.

1.6.7 OVERLOOKING / SHOULDER SURFING

When in public, position the device to prevent unauthorised viewing, photography, or recording of the screen.

2.0 RECOMMENDATIONS

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
● Conduct regular training for employees on BYOD policy, security best practices and the proper use of company approved applications and tools. ● Implement a VPN solution to enable secure remote access to company resources from personal devices. ● Leverage cost-effective cloud-based productivity tools such as Google Workspace or Microsoft 365, which allow	● Adopt cloud-based Mobile Device Management (MDM) solutions such as Microsoft Intune, ManageEngine MDM or On-Premises MDM solutions such as Microsoft Endpoint Manager or VMware Workspace One ● Implement Mobile Threat	● Utilise a cloud-based Enterprise Mobile Management (EMM) solution that includes Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) capabilities. ● Implement Mobile Threat Detection (MTD) solutions to

employees to access and collaborate on documents securely from their personal devices. ● Implement secure file-sharing and collaboration platforms that enable employees to access and share files safely from their personal devices. ● Ensure employees install mobile antivirus on their personal devices to protect against malware and other threats. ● Implement basic IAM solutions to manage user identities, authenticate users, and control access to company resources from personal devices.	Detection (MTD) solutions to detect and mitigate mobile security threats, such as malware, phishing attacks, and network-based attacks. ● Leverage cost-effective cloud-based productivity suites such as Google Workspace or Microsoft 365, which allow employees to access and collaborate on documents securely from their personal devices. ● Implement a secure VPN solution to enable remote access to company resources from personal devices. ● Implement secure file-sharing and collaboration platforms that enable employees to	detect and mitigate mobile security threats, such as malware, phishing attacks, and network-based attacks. ● Utilise a secure VPN solution to enable remote access to company resources from personal devices. ● Leverage cost-effective cloud-based productivity suites like Google Workspace or Microsoft 365, which allow employees to access and collaborate on documents securely from their personal devices. ● Implement secure file-sharing and collaboration platforms that enable employees to access and share files safely from their personal devices. ● Utilise analytics and reporting tools to gain insights into

	access and share files safely from their personal devices. ● Conduct regular training for employees on BYOD policy, security best practices and the proper use of company approved applications and tools.	device usage, app performance, and security incidents. ● Conduct regular security assessment and compliance audits to identify risk, ensure adherence to regulatory requirements and maintain a strong security posture.

If you have any questions about the above policy, please contact the IT Manager or Head of IT.