Bring Your Own Device (BYOD) POLICY

www.invenio-solutions.com

DOCUMENT CONTROL

DOCUMENT NAME	Bring Your Own Device Policy
ABSTRACT	This document details the Policy and Guidelines on using various BYOD and establishes the steps that both users and the IT department should follow to initialize, support, and remove devices from company access by Invenio employees.
DOCUMENT REFERENCE	HRD026

AUTHORISATION

Process Owner	Reviewed By	Authorized By
Name: Kaushal Jora/ Gagan Ahuja	Name: Rajendra Gupta	Name: Naveen Agarwal
Signature:	Signature:	Signature:

SECURITY CLASSIFICATION: Company Confidential

DISTRIBUTION LIST

Master IT Department
Copies Electronic only

VERSION HISTORY

VERSION	DATE	PREPARED BY	CHANGES & REASONS FOR CHANGE
Draft 0.1	23-Feb-22	Kaushal Jora, Gagan Ahuja, Vivek Srivastava	First draft
Draft 0.2	29-April-22	Kaushal Jora, Vivek Srivastava	Second draft
Issue 1.0	5-July-22	Kaushal Jora, Gagan Ahuja, Vivek Srivastava, Rajendra Gupta	First published version baselined

Table of Contents

1 PURPOSE AND OBJECTIVE

At Invenio employee is provided a company laptop to carry out official work.

Additionally, personally owned devices such as smartphones shall be allowed to connect to Invenio environment to facilitate easier communication. However, connecting BYOD to Invenio network entails several information securities risks.

This policy document addresses these information security risks in the following ways:

- Defines limits of access to be provided to BYOD.
- Defines restrictions to prevent connecting unsupported devices or devices that are not updated with the permitted Operating System (OS) and software.
- Defines control to prevent downloads of company information.

2 SCOPE AND COVERAGE

This policy covers personally owned devices such as smartphones

3 INTENDED AUDIENCE

- All Invenio employees, Full time, or part-time employees
- Contract workers, consultants, temporary workers
- IT Support team
- other personnel granted access to organizational systems, networks, software, and/or data

4 ABBREVIATIONS, ACRONYMS AND DEFINITIONS

Abbreviations	Description
BYOD	Bring Your Own Device

5 REFERENCES

1. **MICROSOFT ENTERPRISE + MOBILITY SECURITY (EMS):** Is a mobility management and security platform that helps protect and secure our organization and empower our employees.
2. **MICROSOFT INTUNE:** Microsoft Intune lets you manage your devices from the cloud or while connected to an existing System Center Configuration Manager infrastructure. Microsoft Intune lets you manage devices in a flexible way that's best for you which is not intrusive i.e., it will not monitor/manage any kind of your personal data in your device. So, personal data privacy is not breached after installing this application. Please refer below image for the data managed by this application:

3. **INVENIO MOBILE DEVICE POLICY** (addressing ISO 27001:2013 clause A.06.02.1 Mobile Device Policy).
4. **CYBER ESSENTIAL CHECKLIST** clause A4.1.1, A6.4.2 as follows:

Requirement number	Requirement	Guidance	Invenio Implementation
A2.6	*Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system versions for all devices. All devices that are connecting to cloud services must be included.*	*All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. This applies to both corporate and personal owned devices (BYOD). You do not need to provide serial numbers, mac addresses or other technical information.* *A scope that does not include end user devices is not acceptable."*	*We extract list of BYOD's connected to Invenio network to find if there are any devices that are:* *1) not supported by the vendor* *2) obsolete OS* *3) lacking current security updates* *Devices having the above gaps are logged and tracked to closure.* *We have Microsoft EMS + Intune (EMS-Enterprise Mobility and Security) to extract this report to fulfil this requirement.* ***Refer to Annexure A, B, C & D**.*
A4.1.1	*When corporate or user-owned devices (BYOD) are not connected to the organisation's internal network, how are the firewall controls applied?*	*You should also have firewalls in place for home-based workers, if those users are not using a corporate virtual private network (VPN) connected to your office network, they will need to rely on the software firewall included in the operating system of the device in use.*	*1. We have denied users access to official data on their user-owned devices (BYOD) using Microsoft EMS + Intune (EMS-Enterprise Mobility and Security). All user-ids are assigned with EMS + Intune licenses.* *2. Company provided laptops have Trend Micro Worry-free endpoint firewall agent is installed. This firewall is used when working from home. Also, windows Firewall is there to protect from vulnerabilities. Also, we have DLP (Data Loss Prevention) and URL filtering using TrendMicro for all users who work from home.* ***Refer to Annexure A, B, C & D**.*

A6.4.2	*Where auto updates are not being used, how do you ensure all high-risk or critical security updates of all operating systems and firmware are applied within 14 days of release?*	*It is not always possible to apply auto updates. Please indicate how any updates are applied when auto updates are not configured.*	*We monitor the status of updates using the Microsoft EMS + Intune (EMS-Enterprise Mobility + Security) tool for EUD (End user devices), and mobile devices including BYOD.* *For EUD (End user devices): we train all the users during IT induction and regularly to update the software once they receive the notifications for any applications related update or contact IT Team to help in updating the same within 14 days. Firewalls and Network devices: We get notification from vendors when new updates are released. Also, we check manually on weekly basis if there are any new updates. These are installed manually immediately and within 14 days of release. For servers: We manually check updates once in two days.* *For BYOD: We manually checks for status of updates of all BYOD devices on weekly basis by extracting report from Intune.* ***Refer to Annexure A, B, C & D**.*

6 PROCESS DESCRIPTION

Invenio IT Infrastructure consists of the following technologies:

- Microsoft's Enterprise Mobility + Security
- Microsoft Intune
- Antivirus (Sophos or TrendMicro)

The above technologies ensure limited and secure access on personal devices. There are no restrictions on using BYOD except Invenio resources. These Invenio applications (MS Outlook, MS Teams, MS Office) on personal devices can be used to carry out business communications even when an employee is not working on company provided laptop. The setup of every employee's BYOD requires registering it in the above environment who wants to access MS Outlook, MS teams, MS Office on their personal devices.

.

On personal devices, Intune helps make sure our Invenio's data stays protected and can isolate organization data from personal data, so personal information is isolated from organizational IT awareness. Data accessed using organization credentials are given additional security protection.

For example, a user signs into a device with their organization credentials. Their organization identity allows access to data that's denied to their personal identity. As the organization data is used, app protection policies control how the data is saved and shared. When users sign in with their personal identity, those same protections aren't applied. In this way, IT has control of organization data, while end users maintain control and privacy over their personal data.

As per "What info can your company see when you enroll your device? | Microsoft Docs", the organization cannot see your personal information when you enroll a device with Microsoft Intune. When you enroll a device, you give permission to Invenio to view limited information about your device, such as device model and serial number. Your organization uses this information to help protect the corporate data on the device

The process steps are given below:

6.1 Request to Connect BYOD to Invenio Network

6.1.1 **Smart phones/Tablets:** An employee requiring his personally owned device such as smart phone to connect to Invenio IT infrastructure environment shall send an email request to the IT Helpdesk along with details and configuration of the device.

6.1.2 **Personal PCs:** As a standard practice, personal laptops or desktops will not be allowed to connect to Invenio network. Only in exceptional cases, such as it is not possible to deliver Invenio laptops due to unavoidable reasons like remote locations or any pandemic-related situations, personal laptops shall be allowed. This will require approval from the CTO.

6.2 Verification of BYOD by IT

6.2.1 IT shall verify that the BYOD device is supported by the vendor and has up to date OS.

6.2.2 After verification, IT shall register the device in Microsoft Intune and send out a confirmation email back to the requester. Unless the BYOD device is configured in Intune, it cannot be connected to the Invenio IT environment.

6.3 Connecting BYOD to Invenio Network

6.3.1 After receiving the confirmation email, the employee will have to install Intune App on his device and configure the user id and password to connect to the Invenio IT infrastructure. (See Intune Installation for MacBook, Android Device, Windows Devices and IOS devices under Annexure A, B, C & D).

6.3.2 It is individual responsibility to ensure timely update of the devices with all critical and security patches as and when they are released.

6.4 Periodic Review of BYOD Devices and Reporting

6.4.1 The IT department shall periodically review to check if there are any unsupported devices or devices that do not have current security updates. When noncompliance is found, they will log

as an incident and send out notification (information/reminder/warning) to the owner of the device.

7 RESPONSIBILITIES:

As explained above.

8 OUTPUTS

1. BYOD user list (Refer to Cyber Essentials requirement A2.6 as mentioned in section 4 References above). BYOD user list can be exported from EMS portal by IT admins in .xlsx

BYOD defaulter list (Obsolete BYOD or not up to date security updates) (Refer to Cyber Essentials requirement A6.4.2 as mentioned in section 4 References above). BYOD Defaulters list can be exported from EMS portal by IT admins in .xlsx

BYOD User list and defaulters list.xlsx

9 DISCLAIMER

Invenio has the absolute right to Alter or Abolish the Policy.

The Invenio management has the right to review, modify and rescind this policy at any given point in time.

10 ANNEXURE

10.1 ANNEXURE A: Intune enrollment- Android Device

10.2 ANNEXURE B: Intune enrollment- IOS Device

10.3 ANNEXURE C: Intune enrollment- MacBook Device

10.4 ANNEXURE D: Intune enrollment- Windows Device