**Cybersecurity Templates**

**Bring Your Own Device (BYOD)**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Bring Your Own Device (BYOD)** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[Bring Your Device (BYOD) Policy 3](#_Toc206715798)

[1. Introduction 3](#_Toc206715799)

[2. Audience 3](#_Toc206715800)

[3. Scope 3](#_Toc206715801)

[4. BYOD Controls 3](#_Toc206715802)

[4.1 Access & Authentication 3](#_Toc206715803)

[4.2 Device Security 3](#_Toc206715804)

[4.3 Data Handling 3](#_Toc206715805)

[4.4 Acceptable Use 3](#_Toc206715806)

[4.5 Reporting & Incidents 4](#_Toc206715807)

[5. Governance 4](#_Toc206715808)

[6. Appendices 4](#_Toc206715809)

[Appendix A – User Acknowledgement 4](#_Toc206715810)

[Appendix B – Minimum Device Requirements (Checklist) 4](#_Toc206715811)

[Appendix C – Incident Reporting Contacts 4](#_Toc206715812)

# Bring Your Device (BYOD) Policy

# 1. Introduction

[Organisation] recognises that employees may use personal devices (laptops, tablets, mobile phones) for work. While this can improve flexibility and productivity, it also introduces risks. The purpose of this policy is to provide clear rules for the secure use of personal devices at work.

# 2. Audience

This policy applies to all [Organisation] employees, contractors, volunteers, and third-party users who access [Organisation] systems or data using personal devices.

# 3. Scope

This policy covers all personally owned devices that connect to [Organisation] networks, systems, applications, or process organisational information. It applies whether used on-site, off-site, or remotely.

# 4. BYOD Controls

## 4.1 Access & Authentication

* Users must use strong passwords and Multi-Factor Authentication (MFA).
* Devices must lock automatically after a maximum of 5 minutes of inactivity.
* Privileged access to critical systems is not permitted from BYOD.

## 4.2 Device Security

* Devices must run supported operating systems with the latest security patches.
* Full-disk encryption must be enabled.
* Personal devices must not be jailbroken or rooted.
* Anti-malware/endpoint protection must be enabled where supported.

## 4.3 Data Handling

* Work data must only be accessed through approved apps within a secure container.
* Copying or transferring work data to personal storage (whether cloud-based or local) is strictly prohibited.
* Backup of work data must only be done using [Organisation]-approved services.

## 4.4 Acceptable Use

* BYOD is for business purposes only.
* Users must avoid risky behaviours such as torrenting, using unapproved app stores, or forwarding business data via SMS.
* Public Wi-Fi should only be used in conjunction with an [Organisation]-approved VPN.

## 4.5 Reporting & Incidents

* Lost, stolen, or compromised devices must be reported immediately.
* [Organisation] reserves the right to remotely wipe business data from a personal device if it is lost, stolen, or upon termination.

# 5. Governance

* The CISO or authorised manager must approve exceptions to this policy.
* Non-compliance may lead to the removal of BYOD access, disciplinary action, or contract termination.
* This policy will be reviewed annually.

# 6. Appendices

## Appendix A – User Acknowledgement

I have read and understood the [Organisation] BYOD Policy. I agree to comply with its requirements. I understand that violations may result in loss of BYOD privileges and disciplinary action.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Device (Make/Model/OS): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix B – Minimum Device Requirements (Checklist)

* Encryption enabled (Yes/No)
* OS version up to date (Yes/No)
* Anti-malware active (Yes/No)
* Screen lock enabled (Yes/No)
* VPN installed (Yes/No)

## Appendix C – Incident Reporting Contacts

Service Desk: [Insert contact]

Security Hotline: [Insert contact]