

Bring Your Own Device (BYOD) Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides general guidance for BYOD arrangements. Security requirements should be tailored to your organisation's risk profile and data sensitivity. Consider seeking IT security advice for implementation.

1. Purpose

This policy establishes guidelines for employees who use personal devices to access [Company Name] systems, data and networks. It aims to balance the flexibility of personal device use with the need to protect company information and maintain security standards.

2. Scope

This policy applies to:

- All employees who use personal devices for work purposes
- Smartphones, tablets, laptops and other personal computing devices
- Access to company email, applications, networks and data
- Remote and on-site work using personal devices

3. Policy Statement

[Company Name] permits employees to use personal devices for work purposes subject to compliance with this policy. Participation in BYOD is voluntary, but employees who choose to use personal devices must agree to the security and usage requirements outlined here.

4. Eligibility

4.1 Employee Eligibility

- BYOD is available to [all employees / specified roles]
- Employees must have a legitimate work need
- Manager approval may be required
- Employees must agree to policy requirements

4.2 Device Requirements

Personal devices must meet minimum requirements:

- Operating system: Current or previous major version
- Automatic security updates enabled
- Screen lock with passcode/biometric enabled
- Encryption capabilities
- No jailbroken or rooted devices

5. Security Requirements

5.1 Device Security

Employees using personal devices must:

- Enable device encryption
- Set a strong passcode (minimum 6 digits or complex password)
- Enable automatic screen lock (maximum 5 minutes)
- Keep operating system and apps updated
- Install and maintain antivirus software (where applicable)

5.2 Access Security

- Use company-approved authentication methods
- Enable multi-factor authentication where available
- Never share login credentials
- Log out of company systems when not in use
- Use VPN when required for remote access

5.3 Network Security

- Avoid using public Wi-Fi for sensitive work
- Use secure, encrypted connections
- Be cautious of unfamiliar networks
- Use VPN when connecting from untrusted networks

6. Acceptable Use

6.1 Permitted Activities

- Accessing company email
- Using approved business applications
- Accessing company intranet and documents
- Business communications
- Calendar and scheduling

6.2 Prohibited Activities

- Storing highly sensitive data locally without encryption
- Using unauthorised cloud storage for company data
- Sharing the device with family or others for work access
- Disabling security features
- Installing software that compromises security

7. Data Protection

7.1 Company Data

- Company data remains the property of [Company Name]
- Do not store sensitive data on personal devices unnecessarily
- Use company-approved apps for document storage
- Do not transfer company data to personal accounts
- Delete company data when no longer needed

7.2 Personal Data

- [Company Name] respects employee privacy on personal devices
- Company monitoring is limited to company data and apps only
- Personal content is not accessed during normal operations
- Clear separation between work and personal data is encouraged

8. Mobile Device Management (MDM)

8.1 MDM Requirements

Employees may be required to:

- Install company MDM software on personal devices
- Allow remote management of work-related apps and data
- Accept security policy enforcement

8.2 MDM Capabilities

MDM software may:

- Enforce password policies
- Enable remote wipe of company data only
- Monitor compliance with security requirements
- Push company apps and updates
- Restrict certain device features when accessing company data

9. Support and Costs

9.1 IT Support

- [Company Name] provides support for company apps and access
- Personal device hardware and software support is the employee's responsibility
- IT may assist with company-related configuration

9.2 Costs

- Employees are responsible for device purchase and maintenance
- Employees are responsible for data plans and internet access
- [Company Name] may contribute towards costs at its discretion
- Any reimbursement will be agreed in writing

10. Lost or Stolen Devices

If a personal device used for work is lost or stolen:

- Report to [IT/Manager] immediately
- Attempt to locate the device using find my device features
- Change passwords for all company accounts
- Remote wipe may be initiated for company data
- Cooperate with any security investigation

11. Termination of Employment

When employment ends:

- All company data must be removed from personal devices
- Access to company systems will be revoked
- MDM software and company apps must be removed
- Remote wipe of company data may be performed
- Employee retains ownership of personal device and data

12. Compliance and Breaches

12.1 Compliance

- Employees must comply with all policy requirements
- Regular security checks may be conducted
- Non-compliant devices may have access revoked

12.2 Policy Breaches

Breaches of this policy may result in:

- Removal of BYOD privileges

- Disciplinary action
- Revocation of system access
- In serious cases, termination of employment

13. Responsibilities

13.1 Employees

- Maintain device security as required
- Report security incidents promptly
- Keep personal and work data separate where possible
- Comply with all policy requirements

13.2 IT Department

- Provide approved apps and access methods
- Support company-related access issues
- Monitor compliance and security
- Respond to security incidents

14. Review

This policy will be reviewed:

- At least annually
- When security threats or technology change
- When business requirements change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s BYOD Policy. I understand the security requirements and agree to comply with this policy when using personal devices for work purposes.

Employee Name: _____

Signature: _____

Date: _____