Chameleon
Security

Bring Your Own Device Policy

Purpose

The purpose of this policy is to establish guidelines and requirements for the use of personally owned devices by employees, contractors, and other affiliates to access the company's information systems, data, and network resources. This policy aims to protect the integrity, confidentiality, and availability of company data while enabling the productivity and flexibility benefits of BYOD.

Scope

This policy applies to all employees, contractors, vendors, and any other affiliates who use personal devices to access the company's information systems and data. It covers all types of personally owned devices including smartphones, tablets, laptops, and any other devices capable of storing or accessing organisational data.

Policy Statement

Chameleon permits the use of personally owned devices to access its information systems and data under specific conditions that ensure the security and integrity of its IT infrastructure. All users must comply with this policy, and any violations may result in disciplinary action, up to and including termination of employment.

Definitions

- **BYOD (Bring Your Own Device):** The practice of employees using their personal devices to access corporate data and applications.
- **Personal Device:** Any electronic device not owned or supplied by the organisation, including but not limited to smartphones, tablets, laptops, and wearable technology.
- **Mobile Device Management (MDM):** Software and services responsible for managing and securing mobile devices used in the enterprise.
- **Virtual Private Network (VPN):** A secure encrypted connection used to access organisational resources remotely.
- **Endpoint Security:** Measures taken to secure endpoint devices like personal computers, smartphones, and tablets from cyber threats.

Device Requirements

- **Approved Devices and Operating Systems:**
    - Only devices and operating systems approved by the organisation's IT department may be used for BYOD.
    - Devices must support encryption and have built-in security features, such as remote wipe and device tracking capabilities.
    - Devices must be kept up to date with the latest security patches and updates.
- **Security Configurations:**
    - All devices must be protected with a strong password or biometric authentication.
    - Enable full-disk encryption to protect sensitive data stored on the device.
    - Disable unnecessary services (e.g., Bluetooth, Wi-Fi) when not in use to minimise attack surfaces.
    - Install and maintain antivirus software to detect and prevent malware infections.
- **User Responsibilities:**

- Users must ensure their devices comply with the organisation's security policies and configurations.
- Report any lost or stolen devices immediately to IT or designated security personnel.
- Do not jailbreak or root devices, as it compromises security controls and exposes the organisation to increased risks.

Access Control

- **Authentication and Authorisation:**
  - Users must authenticate using strong, unique passwords and multi-factor authentication (MFA) for accessing sensitive organisational resources.
  - Access to sensitive data and systems must be based on the principle of least privilege.
  - Regularly review and update access permissions based on changes in job roles and responsibilities.

Data Security

- **Data Encryption and Storage:**
  - All data transmitted between personal devices and organisational networks must be encrypted using secure protocols (e.g., SSL/TLS).
  - Ensure sensitive data stored on personal devices is encrypted using approved encryption algorithms and methodologies.
  - Use secure cloud storage solutions approved by the organisation for backing up organisational data.
- **Data Segregation and Usage:**
  - Keep personal and organisational data separate on BYOD devices to prevent unauthorised access and data leakage.
  - Prohibit the storage of sensitive organisational data on personal cloud services or unauthorised third-party applications.

Monitoring and Management

- **Device Monitoring and Audit:**
    - Implement continuous monitoring and auditing of BYOD devices accessing organisational networks.
    - Use Mobile Device Management (MDM) solutions to enforce security policies, monitor device health, and detect unauthorised access attempts.
    - Regularly review audit logs and security incident reports to identify and mitigate potential security threats.
- **Incident Response and Reporting:**
    - Establish procedures for reporting security incidents involving BYOD devices promptly.
    - Define steps for containing and remediating security breaches or policy violations.
    - Conduct post-incident reviews to identify lessons learned and improve incident response capabilities.

Compliance and Legal Considerations

- **Regulatory Compliance:**
    - Ensure BYOD practices comply with relevant Australian laws and regulations, including the Privacy Act 1988 and the Australian Privacy Principles (APPs).
    - Comply with the Notifiable Data Breaches scheme, requiring organisations to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) in the event of eligible data breaches.
    - Conduct regular audits and assessments to verify compliance with legal requirements and organisational policies.
- **User Agreements and Policies:**
    - Require all users to sign a BYOD agreement acknowledging their responsibilities and agreeing to comply with the company's security policies.

- Provide ongoing training and awareness programs to educate users about their obligations and the risks associated with BYOD.

Policy Review and Maintenance

- **Regular Review Cycle:**
  - Conduct periodic reviews and updates of this policy to reflect changes in technology, security threats, and regulatory requirements.
  - Engage stakeholders from IT, legal, and compliance departments in the review process to ensure alignment with organisational goals and objectives.
  - Communicate updates and changes to all users and provide training on new policy requirements as necessary.

Enforcement

- **Compliance Monitoring and Enforcement:**
  - Monitor and enforce compliance with this policy through regular audits, assessments, and security reviews.
  - Implement sanctions and disciplinary actions for policy violations, including temporary or permanent revocation of BYOD privileges.
  - Ensure consistent application of enforcement measures across all levels of the organisation.