Bring Your Own Device (BYOD) Policy

Version 3.0
April 3, 2025

CONFIDENTIAL
This document contains proprietary information of XYZ Corporation
Unauthorized distribution is strictly prohibited
Class Project Submission - Not for actual implementation

XYZ Corporation
Information Security Department

Prepared by: Group 2

Document Control

Document Title	Bring Your Own Device (BYOD) Policy
Version	3.0
Document ID	SEC-POL-005-BYOD
Classification	INTERNAL - CONFIDENTIAL
Effective Date	April 3, 2025
Document Owner	Information Security Department
Project Team	Student Project Group
Distribution	Class submission only - For educational purposes

Project Team Members

Student 1	Bryan Lim
Student 2	Jacob Garcia
Student 3	Casey Sharp
Student 4	Raquel Lugo
Student 5	Grzegorz Rudnicki

Related Documents

Document ID	Document Title
SEC-POL-001	Information Security Policy
SEC-POL-002	Acceptable Use Policy
SEC-POL-003	Data Classification and Handling Policy
SEC-POL-004	Password and Authentication Policy
SEC-POL-008	Incident Response Policy
SEC-STD-012	Mobile Device Security Standard
HR-POL-015	Employee Confidentiality Agreement

Contents

1 Executive Summary

BYOD Program Overview

XYZ Corporation recognizes the value of allowing employees to use their personal devices for work purposes. This BYOD (Bring Your Own Device) Policy establishes a comprehensive framework that balances employee flexibility with organizational security requirements. The policy outlines specific technical, procedural, and behavioral requirements to protect company data while respecting employee privacy and device ownership.

This BYOD Policy (Version 3.0) reflects XYZ Corporation's commitment to:

- Enabling a flexible, mobile workforce through secure use of personal devices
- Implementing reasonable and enforceable security controls focused on company data protection
- Clearly separating personal and company data with appropriate technical controls
- Respecting employee privacy rights regarding their personal devices
- Ensuring compliance with applicable laws and regulations
- Providing clear guidance on responsibilities, support, and compliance verification

Legal Note: This policy has been reviewed by Legal Counsel to ensure it is enforceable while respecting applicable laws, including but not limited to data protection regulations, privacy laws, and employment legislation. Each section contains specific, measurable requirements that facilitate compliance verification and enforcement.

2 Introduction and Overview

2.1 Purpose

Purpose Statement

This policy establishes the framework and guidelines for employees using personally-owned devices to access, store, and process company information for work purposes. XYZ Corporation ("the Company") supports the BYOD (Bring Your Own Device) approach to enhance productivity and flexibility while maintaining appropriate security controls to protect company data, systems, and compliance posture. This policy balances security requirements with realistic implementation and enforcement mechanisms.

The purpose of this policy is to:

1. Define the parameters for secure usage of personally-owned devices for company business
2. Establish clear boundaries between personal and company data
3. Outline specific security requirements that must be met by participating devices
4. Specify the rights and responsibilities of both the Company and employees
5. Provide a framework for incident handling and support
6. Ensure the protection of company data in accordance with regulatory requirements
7. Support business operations through flexible work arrangements

2.2 Primary Objectives

The primary objectives of this BYOD policy are to:

- Enable workforce mobility and flexibility by allowing employees to work from various locations using personal devices
- Enhance productivity by allowing employees to use familiar devices and reduce time required to learn new systems
- Reduce hardware procurement and maintenance costs by leveraging employee-owned equipment where appropriate
- Protect company data with reasonable, enforceable security controls focused on data rather than device management
- Ensure compliance with relevant regulatory requirements including data protection laws
- Clearly define responsibilities for both the Company and employees regarding device management and data protection
- Establish practical procedures for security incident response relating to personal devices
- Balance security needs with IT administrative workload through self-service and automation
- Provide appropriate support for employees using personal devices for work purposes
- Maintain separation between personal and work data to protect employee privacy

2.3 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at the Company who voluntarily choose to use their personal devices to conduct company business, access company data, or connect to company networks. It covers personal smartphones, tablets, laptops, and desktops used to access company resources.

Participation in the BYOD program is voluntary. Employees who do not wish to use personal devices for work may request company-issued equipment through the standard procurement process.

2.3.1 In Scope

This policy covers:

- Personally-owned smartphones, tablets, laptops, and desktop computers
- Access to company email, calendars, contacts, and applications
- Access to company networks, systems, and data repositories
- Storage of company data on personal devices
- Security requirements for personal devices
- Incident reporting and response procedures
- Process for enrolling and removing devices from the program

2.3.2 Out of Scope

This policy does not cover:

- Company-owned devices, which are covered under the Corporate Device Policy (SEC-POL-006)
- Personal devices that do not access company resources
- Wearable technology devices (covered by separate policy SEC-POL-012)
- IoT devices, home networking equipment, or smart home devices
- Personal applications and data unrelated to company business
- Hardware or software support unrelated to company applications

2.4 Scope Limitations

This policy has the following limitations:

- It does not apply to company-owned devices, which are covered under the Corporate Device Policy
- It focuses primarily on protecting company data rather than controlling the entire personal device
- It acknowledges the personal ownership of devices and the limitations this places on enforcement
- It limits administrative overhead to ensure realistic implementation
- It recognizes that complete technical verification of all requirements may not be feasible
- It balances technical controls with administrative controls and user education
- It acknowledges that some controls may be circumvented by determined users

2.5 Legal Framework

This policy operates within the context of the following legal frameworks:

- Employment laws regarding reasonable employer requirements
- Data protection regulations including requirements for data security
- Privacy laws governing employer access to personal information
- Consumer protection laws related to personal device ownership
- Intellectual property laws regarding company data and resources
- Industry-specific regulations applicable to the Company's business

Legal Note: This policy has been drafted to respect both the Company's right to protect its data and the employee's right to privacy on a personally-owned device. Technical measures implemented under this policy will be limited to company data and applications, with clear separation from personal content. This balance makes the policy legally defensible while protecting company interests.

2.6 Audience

This policy applies to and must be understood by the following stakeholders:

1. **Employees:** Staff members who choose to use personal devices for work
    - Responsible for following security requirements
    - Must understand boundaries between personal and company data
    - Need to know enrollment and support procedures
2. **Contractors and Temporary Workers:** Non-permanent workforce members requiring access to company resources through personal devices
    - Subject to the same requirements as employees
    - May have additional restrictions based on contract terms
    - Must understand BYOD requirements are separate from employment status
3. **IT Department:** Staff responsible for implementing and supporting BYOD
    - Must understand technical implementation requirements
    - Responsible for supporting company applications on personal devices
    - Need to maintain separation between personal and company data
4. **Information Security Team:** Personnel responsible for security compliance
    - Responsible for developing and updating technical controls
    - Monitors compliance and security incidents
    - Provides security guidance related to BYOD
5. **Department Managers:** Leadership responsible for ensuring team compliance
    - Ensure team members understand and follow the policy
    - Manage exceptions and special requests
    - Support enforcement when necessary

2.7 Definitions

Term	Definition
BYOD	Bring Your Own Device, referring to the practice of employees using personally-owned devices to access company data and systems. This includes smartphones, tablets, laptops, and desktop computers.
Personal Device	Any employee-owned computing equipment including smartphones, tablets, laptops, and desktops used to access company resources. This specifically refers to hardware owned and maintained by the employee, not the Company.
Company Data	Information created, stored, or processed on behalf of the Company including customer information, financial data, proprietary information, and business communications. This includes all data classified under the Data Classification Policy regardless of storage location.
MDM	Mobile Device Management software that enables secure access to company resources on mobile devices through configuration profiles, not full device control. MDM enables organizations to secure, monitor, and manage personal devices from a central location.
MAM	Mobile Application Management, focusing on securing enterprise applications rather than the entire device. MAM allows for application-level policies and security controls without affecting the rest of the device.
Containerization	Technology creating a separate, encrypted area on a device that isolates business data from personal data. Containerization creates logical separation that prevents data leakage between work and personal spaces.
Encryption	The process of encoding information so that only authorized parties can access it. For the purposes of this policy, encryption refers to industry-standard algorithms that render data unintelligible without the correct decryption key.
Multi-Factor Authentication (MFA)	A security mechanism requiring two or more verification factors to gain access to resources. Factors include something you know (password), something you have (token/device), and something you are (biometric).
Data Leakage	The unauthorized transfer of company data from within an organization to external recipients through various digital or physical means. This includes inadvertent sharing, malicious actions, and technical vulnerabilities.
Security Incident	Any actual or suspected event that could lead to loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or similar occurrence where persons other than authorized users potentially have access to company data.

Term	Definition
Acceptable Use	The permitted actions and behavior when using company resources, as defined in the Acceptable Use Policy. Acceptable use includes both permitted and prohibited activities.
Remote Wipe	The ability to remotely delete data from a device. For BYOD, this refers to selective wiping of company data and applications rather than full device wiping.
Data Classification	The process of categorizing data based on its sensitivity and the impact of its disclosure, as defined in the Data Classification and Handling Policy. Classifications typically include Public, Internal, Confidential, and Restricted.
Self-Attestation	A process where employees formally declare compliance with specific requirements through digital or written confirmation. Self-attestation is used where technical verification is impractical.
Risk-Based Approach	A methodology that allocates security resources and controls according to the level of risk, focusing stronger controls on higher-risk scenarios and accepting lower controls for lower-risk situations.

2.8 Compliance and Enforcement

Realistic Enforcement Approach

This policy uses a balanced approach to enforcement that focuses on protecting company data while acknowledging the practical limitations of managing personal devices. Technical controls are applied primarily to company applications and data rather than the entire device. Verification combines automated technical checks, self-attestation, and risk-based manual verification.

Enforcement Type	Implementation Methods
Technical Enforcement	• Containerization of company data and applications to enforce separation • Access controls for company resources based on device compliance status • Automated compliance verification during connection attempts to company resources • Application-level security rather than full device control • Certificate-based authentication for company resources • Conditional access policies that verify security status before allowing resource access
Administrative Enforcement	• Clear policy acknowledgment process with electronic signature • Periodic automated compliance reports to management • Risk-based approach to manual verification focusing on high-risk users • Enforcement focused on company resource access rather than device configuration • Regular self-attestation regarding continued compliance • Documented exceptions process with appropriate approvals
Security Training	• Initial BYOD security training before enrollment • Annual online refresher course with verification quiz • Regular security awareness communications specific to mobile security • On-demand training resources in the BYOD portal

Compliance Reminder: This approach to compliance enforcement recognizes the practical limitations of managing personal devices while focusing controls on protecting company data. The combination of technical, administrative, and educational measures creates multiple layers of protection.

2.9 Non-Compliance Consequences

Failure to comply with this policy may result in the following consequences:

Violation Level	Examples	Consequence
Minor Violation	• Delayed security updates (under 30 days) • Temporary disabling of required security features • Brief connection to high-risk networks	• Automated notification with remediation instructions • Temporary restriction of specific resource access until remediated • Additional targeted security awareness training
Significant Violation	• Extended failure to install security updates (over 30 days) • Disabled device encryption or authentication • Storing sensitive data outside approved containers	• Temporary suspension of BYOD privileges • Required meeting with IT Security • Notification to department manager • Mandatory remedial security training
Critical Violation	• Jailbreaking or rooting device • Installing unauthorized MDM profiles • Deliberate data exfiltration • Sharing device with unauthorized users	• Immediate revocation of BYOD privileges • Required use of company-owned equipment • Security incident investigation • Review of all company data accessed

Warning: The above consequences apply specifically to violations of the BYOD policy. Additional consequences may apply under other company policies if the viola-

tion also constitutes a breach of those policies, particularly regarding data protection, confidentiality, or acceptable use.

3 Eligible Devices and Enrollment

3.1 Supported Devices

3.1.1 Device Eligibility Criteria

For a personal device to be eligible for the BYOD program, it must meet all of the following criteria:

1. Run one of the supported operating systems at or above the minimum version
2. Have sufficient storage space for required company applications (minimum 1GB available)
3. Have sufficient processing capability to run required applications effectively
4. Support hardware encryption capabilities
5. Be capable of receiving regular security updates
6. Not be jailbroken, rooted, or otherwise have security features compromised
7. Be able to implement a screen lock with authentication
8. Support installation of required company applications

3.1.2 Smartphones and Tablets

The following smartphones and tablets are eligible for the BYOD program:

Platform	Minimum Version	Notes
Apple iOS	iOS 14.0 or later	Standard support with full MDM capability
Apple iPadOS	iPadOS 14.0 or later	Standard support with full MDM capability
Android	Android 10.0 or later	Samsung devices with Knox security platform recommended for enhanced security features
Android Enterprise	Android 10.0 or later	Enhanced security with work profile separation

Ineligible Mobile Devices

The following types of mobile devices are not eligible for the BYOD program:

- Devices that cannot receive regular security updates
- Devices from manufacturers that have ceased support
- Devices running custom or modified operating systems
- Devices with removed or bypassed security features
- Devices that cannot support required security applications

3.1.3 Laptops and Workstations

The following laptop and desktop computers are eligible for the BYOD program:

Platform	Minimum Version	Notes
Windows	Windows 10 (20H2) or later	Professional, Enterprise, or Education editions required for BitLocker support and advanced security features
macOS	macOS 11.0 (Big Sur) or later	All models supporting the minimum OS version are eligible
Chrome OS	Version 94 or later	Must support Android applications and Linux containers

Ineligible Computer Devices

The following types of computers are not eligible for the BYOD program:

- Computers running Home editions of Windows
- Computers that cannot encrypt their storage drives
- Computers shared with other household members that cannot support separate user profiles
- Computers running Linux operating systems (except in special cases with CISO approval)
- Computers that cannot receive regular security updates

Verification Method: Device eligibility is automatically verified during enrollment through the MDM registration portal, which detects device type and OS version. For items that cannot be automatically detected, users must self-attest compliance during the enrollment process.

3.2 Enrollment Process

Enrollment Requirements

Enrollment in the BYOD program requires explicit acknowledgment of this policy, completion of BYOD security training, and successful configuration of the device according to security requirements. Enrollment constitutes acceptance of all policy terms.

3.2.1 Pre-Enrollment Requirements

Before enrolling a device, employees must:

1. Complete the required BYOD security awareness training (available in the Learning Management System)
2. Review this BYOD policy in its entirety
3. Ensure their device meets eligibility requirements
4. Back up any personal data on the device (recommended but not required)
5. Obtain manager approval for BYOD participation (if required by department)

3.2.2 Enrollment Steps

To enroll a personal device for work use:

1. Access the BYOD portal at https://byod.company.com using your company credentials
2. Review and electronically accept this BYOD policy via the company portal
3. Complete the self-service enrollment form, which includes:
   - Device details (make, model, operating system)
   - Serial number or IMEI (for mobile devices)
   - Self-attestation of compliance with security requirements
   - Acknowledgment of company rights regarding company data
4. Download and install the required MDM profile (for mobile devices) or MDM client (for computers)
5. Install the required company applications from the appropriate app stores or company portal
6. Follow the provided instructions to configure security settings
7. Register the device with company authentication systems

8. Verify enrollment by accessing a company resource and confirming successful access

Note: Enrollment is a self-service process with automated verification. IT support is available for employees who encounter difficulties. Enrollment must be completed within 7 days of starting the process, or it will expire and need to be restarted.

3.2.3 Required Applications

As part of the enrollment process, the following applications must be installed:

Application	Purpose	Devices
Company Email Client	Secure access to company email with data containment	All devices
MDM Agent	Device verification and security policy enforcement	All devices
Authenticator App	Multi-factor authentication for company resources	All devices
Mobile Content Management	Secure document viewing and editing	All devices
VPN Client	Secure network connection when required	Laptops, optional for mobile
Antivirus/Security	Malware protection and security monitoring	Laptops and desktops only

3.2.4 Enrollment Verification

Upon completion of enrollment:

1. The system will verify device compliance with security requirements
2. A confirmation email will be sent to the employee's company email address
3. The device will be added to the BYOD inventory system
4. The employee's manager will be notified of successful enrollment
5. Access to company resources will be enabled for the enrolled device

3.3 Security Requirements

3.3.1 Authentication Requirements

Authentication Security

Proper authentication is the first line of defense against unauthorized access to company data. All devices must implement strong authentication measures for both device access and company resource access.

Device Authentication

Devices must be protected with one of the following:

- PIN code (minimum 6 digits)
- Password (minimum 8 characters, including uppercase, lowercase, and numeric or special characters)
- Biometric authentication (fingerprint, facial recognition) with fallback to PIN or password

Additional Authentication Controls

The following additional authentication controls are required:

1. Device must automatically lock after inactivity (maximum 15 minutes)
2. Maximum of 10 failed authentication attempts before requiring administrator reset or implementing a time delay
3. Screen timeout must be set to 5 minutes or less
4. Previous unlock patterns (if used) cannot be reused
5. Biometric authentication, if used, must be limited to the device owner only

Company Resource Authentication

Company resources require multi-factor authentication via:

- Company-approved authenticator app
- Push notifications to registered device
- Hardware security keys (optional but recommended)
- SMS one-time codes (allowed but not recommended)

Verification: Authentication requirements are verified through:

1. Self-attestation during enrollment
2. MDM verification for mobile devices (when applicable)
3. Access requirements for company resources
4. Spot checks during technical support interactions

3.3.2 Security Software Requirements

Device Security Protection

Keeping devices secure requires both system-level protections and application-level security measures. All devices must maintain current security protections to minimize the risk of compromise.

Operating System Security

All devices must have:

- Current operating system with security updates applied within 30 days of release
- Automatic updates enabled where possible
- All available security features activated
- Built-in firewalls enabled (where applicable)
- System integrity protection features enabled

Malware Protection

- Laptops and desktops must have active antivirus protection from one of the approved solutions in Appendix A
- Antivirus software must be configured for automatic updates and real-time scanning
- Full system scans must be configured to run at least weekly
- Mobile devices should use only applications from official app stores

Device Integrity

- Devices must not be jailbroken, rooted, or have security features disabled
- Devices must not run beta or developer preview operating systems
- Devices must not have unauthorized MDM profiles installed
- Devices must not have debugging modes enabled

Enforcement Method: Security requirements are enforced through:

1. Self-attestation during enrollment and annual recertification
2. Automated vulnerability scanning when connecting to company resources
3. Conditional access policies that verify security status before resource access
4. Random security posture assessments
5. Access denial for non-compliant devices

3.3.3 Company Container Requirements

Data Separation

Company data must be logically separated from personal data to prevent leakage and enable selective management of company information without affecting personal content.

Container Technology

- Company data must be accessed through approved applications that provide data separation
- Company email must use the approved email application with containerization
- Company documents must be accessed through managed applications that prevent data leakage
- Container must encrypt all stored company data using AES-256 or equivalent encryption
- Container must require separate authentication after device unlock

Data Transfer Controls

- Copy/paste operations between company container and personal apps must be restricted
- Screenshots while using company apps may be disabled for highly sensitive applications
- File sharing from company container to personal apps must be controlled
- Printing from company container must be logged and may be restricted
- Downloads from company resources must remain within the managed container

Container Configuration

- Container must be configured to allow remote wiping of company data only
- Container must implement separate timeout controls from device settings
- Container must enforce document encryption when storing company files
- Container must prevent backup of company data to personal backup systems
- Container access must be automatically revoked if device is non-compliant

Enforcement Method: Container requirements are enforced through:

1. Mobile Application Management (MAM) controls
2. Application policies that prevent export to unmanaged applications
3. Authentication requirements for accessing company containers
4. Technical restrictions on data movement between containers
5. Monitoring of container access and usage

3.4 Acceptable Use Guidelines

3.4.1 Approved Business Activities

Permitted Uses

Personal devices enrolled in the BYOD program may be used for business activities that are consistent with the Company's Acceptable Use Policy. The following provides specific guidance for BYOD scenarios.

Employees may use personal devices for:

- Email and calendar access through approved applications
- Document viewing and editing in approved applications
- Business communication through approved channels (email, messaging, conferencing)
- Accessing company web applications and intranet resources
- Customer relationship management (CRM) using approved applications
- Business process applications through secure channels
- Time and expense reporting through company systems
- Secure access to business intelligence and reporting systems
- Project management and collaboration tools
- Corporate learning and training platforms

3.4.2 Prohibited Activities

Employees may not use personal devices for:

- Storing company data in unapproved applications or personal cloud storage
- Forwarding company email to personal email accounts
- Installing unapproved applications that access company data
- Sharing the device with family members or others while logged into company resources
- Taking screenshots of sensitive company information
- Connecting to company networks through unauthorized VPNs or proxies
- Backing up company data to personal backup systems

- Using unapproved collaboration or file sharing services for company data
- Recording or photographing confidential company meetings or materials
- Allowing automated tools or bots to access company resources

3.4.3 Data Protection Requirements

When using personal devices for business:

- Store company data only in approved applications or cloud storage
- Do not use personal email or cloud storage for company data
- Do not share your device with others when accessing company resources
- Maintain a clear separation between personal and company data
- Report lost or stolen devices promptly according to the incident response procedure
- Ensure device security patches are applied within 30 days of release
- Log out of company applications when not in use for extended periods
- Be cautious about using company applications on public Wi-Fi networks
- Do not leave the device unattended when logged into company resources
- Consider using a VPN when accessing company resources from public networks

3.4.4 Personal Use Boundaries

Separation of Personal and Business Use

While the Company respects that BYOD devices are personally owned, certain guidelines must be followed to maintain appropriate boundaries between personal and business use.

- Personal use of the device should not interfere with business activities
- Personal applications should not pose security risks to company data
- Device should not be used for personal activities while actively connected to secure company networks
- High-risk personal activities (visiting untrusted websites, sideloading applications) may compromise device security and should be avoided
- Personal use is not monitored but may affect device eligibility if it compromises security

Enforcement Method: Data protection requirements are enforced through:

1. Container technologies that isolate company data
2. Application-level controls that prevent data sharing with unauthorized apps
3. User education and acknowledgment
4. Periodic security awareness reminders
5. Technical controls that prevent unauthorized data movement

For complete details on acceptable use guidelines, refer to the Corporate Acceptable Use Policy (SEC-POL-002).

Legal Note: The acceptable use guidelines represent reasonable requirements for protecting company data while respecting that the device is personally owned. These guidelines focus on company data protection rather than controlling personal use.

3.5 Company Access and Privacy Protection

3.5.1 Company Access Scope

Limited Access Guarantee

The Company implements technical measures to limit its access to only company data and applications on BYOD devices. These limitations protect both employee privacy and company data.

The Company may access:

- Company data and applications on your device
- Basic device information (make, model, OS version, device name)
- Security compliance status for company applications
- Device identifiers (IMEI, serial number) for inventory purposes
- List of installed company applications
- Device encryption status
- Authentication status and settings for company applications
- Company container health and configuration

The Company explicitly cannot access:

- Personal files, photos, messages, or emails
- Personal application data or usage
- Browsing history or personal web activity
- Location data (except during active use of company applications, if required)
- Passwords or personal authentication data
- Call logs or SMS messages (unless using a company-provided business line)
- Personal contacts or personal calendar
- Camera or microphone without explicit user action
- Social media or personal accounts

3.5.2 Remote Management Capabilities

The Company maintains the ability to:

- Remove company applications and data remotely
- Reset passwords for company applications
- Block access to company resources if security requirements are not met
- Apply security policies to company applications
- View the last connection time to company resources
- Force authentication to company resources
- Push updates to company applications
- Remove company configuration profiles

The Company does not have the ability to:

- Wipe the entire personal device
- Access or delete personal data
- Track device location when not actively using company applications
- Access the device camera or microphone
- View or modify personal settings
- Install or remove personal applications
- Access device without user knowledge
- Monitor device usage outside of company applications
- Remotely control or view the device screen

Note: Technical controls prevent the Company from accessing personal data, providing protection for both the employee's privacy and the Company's security needs. These limitations are enforced through containerization and application-level management.

3.5.3 Privacy Protection Measures

Employee Privacy Rights

The Company recognizes and respects the privacy rights of employees regarding their personal devices. The following measures ensure this protection.

1. **Technical Controls:**
    - Container-based approach isolates company data
    - Mobile Application Management focuses on applications, not whole device
    - Limited device attributes collection
    - No personal data backups to company systems
    - No monitoring of personal activity
2. **Administrative Controls:**
    - Clear documentation of data collected
    - Regular privacy impact assessments
    - Restricted IT admin access to BYOD management console
    - Logging of all administrator actions
    - Regular audit of access logs
3. **Transparency Measures:**
    - Detailed privacy notice for BYOD participants
    - Clear consent process during enrollment
    - Right to unenroll at any time
    - Notification when policy changes affect privacy
    - Process to request collected data review

Legal Note: The privacy protection measures implemented in this policy comply with applicable data protection laws and respect employee privacy rights while maintaining necessary security controls for company data protection.

3.6 Support and Resources

3.6.1 IT Support Scope

Support Boundaries

The Company provides support for company applications and access on BYOD devices but cannot provide comprehensive support for the personal device itself.

IT will support:

- Enrollment in the BYOD program
- Installation and configuration of company applications
- Access to company resources and networks
- Troubleshooting company application issues
- Configuration of company email and productivity tools
- Resolving connection issues to company resources
- Security requirements related to company data access
- Password resets for company applications
- Container management and configuration
- VPN configuration for company access

IT will not support:

- Hardware issues with personal devices
- Operating system problems not related to company applications
- Personal applications or data
- Home network or internet connectivity issues
- Performance issues not related to company applications
- Device upgrades or migrations
- Personal email or cloud storage configuration
- Non-company application installation or troubleshooting
- Personal account configuration
- Carrier or service provider issues

3.6.2 Available Resources

Resources available to BYOD participants:

- Self-service BYOD portal: https://byod.company.com
- Knowledge base articles for common issues
- Technical support for company applications: support@company.com
- BYOD help desk: x1234 (business hours only)
- Emergency security support: x5555 (24/7 for security incidents only)
- Step-by-step enrollment guides for each supported platform
- Video tutorials for common procedures
- Monthly BYOD user webinars
- Peer support community forum
- Regular security update notifications

3.6.3 Support Process

1. **Self-Service:** Check knowledge base and troubleshooting guides on BYOD portal
2. **Tier 1 Support:** Contact help desk via email, phone, or portal for basic issues
3. **Tier 2 Support:** Escalation to specialized support for complex issues
4. **Security Incidents:** Immediate escalation to security team for potential breaches
5. **Specialized Support:** Scheduled assistance for complex configuration issues

3.7 Incident Response

3.7.1 Lost or Stolen Devices

Immediate Reporting Requirement

Lost or stolen devices with access to company resources must be reported immediately to minimize the risk of data exposure.

If your personal device is lost or stolen:

1. Report to IT Security immediately via:
   - Email: security@company.com
   - Phone: x5555 (24/7 emergency line)
   - BYOD Portal: https://byod.company.com/report
   - In-person to any IT Security team member
2. Provide the following information:
   - Device make, model, and identifier
   - Date and time of loss
   - Circumstances of loss or theft
   - Whether the device was locked and encrypted
   - Types of company data accessed on the device
   - Whether any recovery attempts have been made
3. IT Security will:
   - Reset company account passwords
   - Remotely remove company data if possible
   - Revoke device access to company resources
   - Issue a temporary access token for continued work if needed
   - Document the incident in the security management system
   - Conduct risk assessment for potential data exposure
4. User responsibilities:
   - File a police report if theft is suspected
   - Use device locator services if available
   - Notify cellular carrier if applicable
   - Change passwords for any personal accounts accessed from the device
   - Monitor accounts for unusual activity

Warning: Failure to promptly report a lost or stolen device may result in more severe consequences if company data is compromised. The focus of incident response is on protecting data, not punishing accidental loss.

3.7.2 Security Incidents

For other security concerns or suspected incidents:

1. Stop using company applications on the device immediately
2. Disconnect from company networks if connected
3. Report the incident to IT Security using the contact methods above
4. Preserve evidence where possible (do not power off the device or delete logs)
5. Document observations including:
    - Unusual behavior observed
    - Applications or resources affected
    - Any error messages received
    - Recent changes or installations
    - Timestamp of observations
6. Follow instructions provided by the security team
7. Be available for investigative follow-up
8. Do not attempt to fix security issues yourself
9. Do not discuss the incident outside the response team

3.7.3 Compromise Recovery Process

If a device is determined to be compromised:

1. Device will be immediately disconnected from company resources
2. Security team will assess the extent of potential data exposure
3. Company container will be remotely wiped if possible
4. Device must be reset to factory settings before re-enrollment
5. Security training refresher may be required
6. Enhanced monitoring may be implemented for the device
7. Incident will be documented according to incident management procedures
8. Legal and compliance teams will be notified if regulated data was exposed

3.8 Program Exit

3.8.1 Voluntary Withdrawal

Right to Withdraw

Participation in the BYOD program is voluntary, and employees may withdraw at any time following the appropriate procedure to ensure company data is properly removed.

To withdraw from the BYOD program:

1. Submit withdrawal request via BYOD portal or to IT Support
2. Schedule a data removal session if required for complex cases
3. Remove company applications from your device following provided instructions
4. Delete any locally saved company data
5. Return any company-issued accessories or peripheral equipment
6. Verify removal of company container and applications
7. Receive confirmation of successful program exit
8. Alternative work equipment will be provided if needed

3.8.2 Employment Termination

Upon leaving the Company:

1. Company applications and data access will be automatically disabled on the effective termination date
2. You must delete all company applications and data prior to your last day
3. Company email and resource access will be terminated
4. IT may verify data removal during exit interview
5. Instructions for secure deletion will be provided in exit materials
6. Access tokens and certificates will be automatically revoked
7. You may be required to sign a declaration confirming all company data has been removed
8. Failure to remove company data may have legal consequences

Legal Note: Upon termination of employment, employees have a continuing legal obligation to protect company confidential information, including any that may have been accessed through personal devices. Retention of company data after employment ends may violate confidentiality agreements and data protection laws.

4 Risk Management and Compliance

4.1 Risk Assessment

Balanced Risk Approach

The Company recognizes that BYOD introduces specific security risks but implements controls proportionate to these risks while maintaining usability.

4.1.1 Identified Risks

The BYOD program introduces the following key risks, which are addressed through policy controls:

Risk	Impact	Mitigation Measures
Data Leakage	Unauthorized disclosure of company information	Containerization, data loss prevention controls, application restrictions
Device Compromise	Malware infection leading to data theft	Security requirements, anti-malware, OS updates, application controls
Unauthorized Access	Inappropriate access to company resources	Multi-factor authentication, device locks, access controls
Compliance Violations	Regulatory penalties for mishandled data	Data classification, special controls for regulated data, compliance verification
Mixed Data	Difficulty separating personal and company data	Container separation, clear data ownership, selective wipe capability
Lost/Stolen Devices	Physical loss leading to data compromise	Device encryption, remote wipe capability, incident response plan

4.2 Regulatory Compliance

Compliance Framework

This policy is designed to ensure compliance with regulatory requirements while enabling BYOD flexibility. Special controls apply to regulated data.

4.2.1 Regulated Data Handling

For regulated data categories, additional requirements apply:

Data Category	Special Requirements
Protected Health Information (PHI)	• Access limited to authorized roles • Enhanced encryption requirements • Specialized container configuration • Additional authentication controls • Detailed access logging
Payment Card Information (PCI)	• Prohibited from storage on BYOD devices • Accessible only through secure web interfaces • Special training requirements • Enhanced monitoring of access
Personally Identifiable Information (PII)	• Restricted download capabilities • Enhanced access controls • Special handling procedures • Data loss prevention controls
Confidential Business Information	• Limited offline access • Additional authentication for sensitive documents • Restricted sharing capabilities

5 Appendices

5.1 Appendix A: Approved Security Solutions

5.1.1 Approved Antivirus/Endpoint Protection Solutions

The following security solutions are approved for use on BYOD devices:

Solution	Supported Platforms	Minimum Version
Microsoft Defender	Windows	Windows 10 built-in
Symantec Endpoint Protection	Windows, macOS	14.3 or later
McAfee Total Protection	Windows, macOS	16.0 or later
Sophos Intercept X	Windows, macOS	10.8 or later
Trend Micro Maximum Security	Windows, macOS	17.0 or later

5.1.2 Approved Mobile Device Management Solutions

The Company uses the following MDM solutions for BYOD management:

Solution	Purpose
Microsoft Intune	Primary MDM/MAM solution for all platforms
VMware Workspace ONE	Secondary solution for specialized use cases

5.2 Appendix B: Data Classification Mapping

The following table maps data classifications to BYOD handling requirements:

Classification	Handling Requirements	Allowed on BYOD?
Public	Standard container protection	Yes
Internal	Standard container protection, limited sharing	Yes
Confidential	Enhanced container protection, restricted offline access	Yes with controls
Restricted	Enhanced protection, enhanced authentication, limited availability	Limited roles only

6 Acknowledgment and Signature

Binding Agreement

This acknowledgment represents a formal agreement between the employee and the Company regarding BYOD participation. Please read carefully before signing.

By signing below, I acknowledge that I have read and understand the XYZ Corporation Bring Your Own Device (BYOD) Policy. I voluntarily choose to participate in the BYOD program and agree to comply with all policy requirements.

I understand that:

- The Company will only access company data and applications on my device
- I am responsible for securing my device as specified in this policy
- Failure to comply may result in loss of BYOD privileges
- I can withdraw from the program at any time
- This policy may be updated, and I will be notified of significant changes
- I am responsible for maintaining device security and applying updates
- I will promptly report security incidents or lost/stolen devices
- I will remove all company data when leaving the organization

Name (Print):	
Employee ID:	
Department:	
Job Title:	

Device Type:	
Device Make/Model:	
Device Operating System:	

Employee Signature:	
Date:	

Manager Name:		
Manager Signature:		
Date:		

IT Security Approval:		
Date:		