Bring Your Own Device (BYOD) Policy Template

Document Control Information

- **Document Title:** Bring Your Own Device (BYOD) Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Bring Your Own Device (BYOD) Policy establishes [ORGANIZATION NAME]'s requirements for the secure use of personally-owned devices to access, store, or process organizational information in accordance with ISO 27001:2022 requirements. It provides a framework for balancing the flexibility and productivity benefits of BYOD with the need to protect organizational information assets.

1.2 Scope

This policy applies to: - All employees, contractors, consultants, and third parties who use personally-owned devices to access organizational information - All types of personally-owned devices including smartphones, tablets, laptops, and desktop computers - All organizational information accessed, stored, or processed on personally-owned devices - All networks and systems accessed using personally-owned devices - All locations from which personally-owned devices are used for work purposes

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Enabling the productive use of personally-owned devices for work purposes - Protecting organizational information accessed, stored, or processed on personally-owned devices - Implementing appropriate security controls for BYOD - Respecting the privacy of device owners - Providing clear guidance on BYOD responsibilities - Ensuring compliance with legal and regulatory requirements - Regularly reviewing and improving BYOD security controls

2. BYOD Program

2.1 Eligibility

- BYOD participation shall be based on business need and role requirements
- Eligibility shall be determined by:
  - Job function
  - Access requirements
  - Security considerations
  - Management approval
- Eligibility shall be documented
- Eligibility shall be regularly reviewed
- Eligibility changes shall be promptly implemented
- Eligibility shall be revoked when no longer appropriate

2.2 Enrollment Process

- BYOD enrollment shall follow a defined process
- The process shall include:
  - Eligibility verification
  - User agreement acceptance
  - Device assessment
  - Security configuration
  - Management solution enrollment
  - User training
- Enrollment shall be documented
- Enrollment shall be approved by appropriate authority
- Enrollment shall be completed before access is granted
- Enrollment process shall be regularly reviewed

2.3 User Agreement

- BYOD users shall accept a user agreement
- The agreement shall include:
  - User responsibilities
  - Organizational rights
  - Privacy considerations
  - Support limitations
  - Security requirements
  - Compliance expectations
  - Termination procedures
- Agreement acceptance shall be documented
- Agreement shall be reviewed annually

- Agreement shall be updated when requirements change
- Agreement shall be legally reviewed

3. Device Requirements

3.1 Supported Devices

- Only approved device types shall be permitted
- Approval shall be based on:
  - Operating system
  - Model
  - Age
  - Security capabilities
  - Management compatibility
- Supported devices shall be documented
- Support shall be regularly reviewed
- Unsupported devices shall be blocked
- Exceptions shall be documented and approved

3.2 Operating System Requirements

- Devices shall run approved operating systems
- Requirements shall include:
  - Current version
  - Security updates
  - Support status
  - Configuration capabilities
- Operating system requirements shall be documented
- Compliance shall be verified
- Non-compliant devices shall be remediated or blocked
- Requirements shall be regularly updated

3.3 Security Software

- Devices shall have required security software
- Software may include:
  - Mobile device management agent
  - Endpoint protection
  - VPN client
  - Secure email client
  - Secure browser
- Software requirements shall be documented
- Software shall be properly configured

- Software shall be regularly updated
- Software effectiveness shall be monitored

3.4 Jailbreaking/Rooting

- Jailbroken or rooted devices shall not be permitted
- Detection mechanisms shall be implemented
- Detection shall be performed:
    - During enrollment
    - Periodically thereafter
    - Upon suspicious activity
- Detected devices shall be blocked from access
- Users shall be notified of violations
- Repeated violations shall be addressed
- Detection effectiveness shall be regularly assessed

4. Security Controls

4.1 Device Authentication

- Devices shall require authentication
- Authentication shall include:
    - PIN, password, or passphrase
    - Biometric where available
    - Minimum complexity requirements
    - Maximum retry limits
    - Inactivity timeout
- Authentication requirements shall be documented
- Authentication compliance shall be verified
- Authentication failures shall be monitored
- Authentication requirements shall be regularly reviewed

4.2 Encryption

- Devices shall use encryption
- Encryption shall include:
    - Full device encryption
    - Application data encryption
    - Communication encryption
    - Backup encryption
- Encryption requirements shall be documented
- Encryption compliance shall be verified
- Encryption effectiveness shall be regularly assessed

- Encryption requirements shall be regularly reviewed

4.3 Application Controls

- Application usage shall be controlled
- Controls may include:
  - Prohibited application lists
  - Required application lists
  - Application vetting
  - Application permissions management
- Application controls shall be documented
- Application compliance shall be monitored
- Application control violations shall be addressed
- Application controls shall be regularly reviewed

4.4 Network Controls

- Network connections shall be secured
- Controls shall include:
  - VPN requirements
  - Wi-Fi security requirements
  - Bluetooth restrictions
  - Tethering restrictions
  - Public network guidance
- Network controls shall be documented
- Network compliance shall be monitored
- Network control violations shall be addressed
- Network controls shall be regularly reviewed

5. Data Protection

5.1 Data Storage

- Organizational data storage shall be controlled
- Controls shall include:
  - Storage location restrictions
  - Containerization
  - Encryption requirements
  - Backup restrictions
  - Sharing restrictions
- Storage controls shall be documented
- Storage compliance shall be monitored
- Storage violations shall be addressed

- Storage controls shall be regularly reviewed

5.2 Data Transfer

- Data transfer shall be controlled
- Controls shall include:
  - Transfer method restrictions
  - Encryption requirements
  - Destination restrictions
  - Volume limitations
  - Monitoring and logging
- Transfer controls shall be documented
- Transfer compliance shall be monitored
- Transfer violations shall be addressed
- Transfer controls shall be regularly reviewed

5.3 Data Segregation

- Organizational data shall be segregated from personal data
- Segregation methods may include:
  - Containerization
  - Separate profiles
  - Dedicated applications
  - Storage partitioning
- Segregation requirements shall be documented
- Segregation compliance shall be verified
- Segregation effectiveness shall be regularly assessed
- Segregation requirements shall be regularly reviewed

5.4 Data Backup

- Organizational data backup shall be controlled
- Controls shall include:
  - Backup method requirements
  - Backup location restrictions
  - Encryption requirements
  - Retention limitations
  - Recovery testing
- Backup controls shall be documented
- Backup compliance shall be monitored
- Backup effectiveness shall be regularly assessed
- Backup controls shall be regularly reviewed

6. Device Management

6.1 Mobile Device Management

- BYOD devices shall be enrolled in mobile device management (MDM)
- MDM shall provide:
  - Policy enforcement
  - Configuration management
  - Compliance monitoring
  - Remote wipe capability
  - Application management
  - Security monitoring
- MDM requirements shall be documented
- MDM effectiveness shall be regularly assessed
- MDM capabilities shall be regularly reviewed
- MDM exceptions shall be documented and approved

6.2 Configuration Management

- Device configurations shall be managed
- Management shall include:
  - Security settings
  - Network settings
  - Application settings
  - Feature restrictions
  - Update management
- Configuration requirements shall be documented
- Configuration compliance shall be monitored
- Configuration changes shall follow change management
- Configuration effectiveness shall be regularly assessed

6.3 Patch Management

- Devices shall be kept updated
- Update requirements shall include:
  - Operating system updates
  - Security patches
  - Application updates
  - Firmware updates
- Update timeframes shall be defined
- Update compliance shall be monitored
- Update failures shall be addressed
- Update requirements shall be regularly reviewed

6.4 Remote Wipe

- Remote wipe capability shall be implemented
- Capability shall include:
  - Selective organizational data wipe
  - Full device wipe when necessary
  - Automatic triggering conditions
  - Authorization requirements
  - Documentation procedures
- Remote wipe shall be used when:
  - Device is lost or stolen
  - User is terminated
  - Security is compromised
  - Compliance is violated
- Remote wipe procedures shall be documented
- Remote wipe effectiveness shall be regularly tested
- Remote wipe shall respect privacy considerations

7. Access Control

7.1 Authentication Requirements

- BYOD access shall require strong authentication
- Authentication shall include:
  - Organizational account credentials
  - Multi-factor authentication where appropriate
  - Session timeouts
  - Re-authentication requirements
- Authentication requirements shall be documented
- Authentication compliance shall be monitored
- Authentication failures shall be investigated
- Authentication requirements shall be regularly reviewed

7.2 Access Restrictions

- BYOD access shall be restricted based on:
  - User role
  - Device compliance
  - Location
  - Network
  - Time
  - Risk factors
- Access restrictions shall be documented

- Access compliance shall be monitored
- Access violations shall be addressed
- Access restrictions shall be regularly reviewed

7.3 Virtual Private Network

- VPN shall be used for remote access
- VPN requirements shall include:
  - Strong encryption
  - Strong authentication
  - Split tunneling controls
  - Session management
  - Logging and monitoring
- VPN usage shall be enforced where appropriate
- VPN compliance shall be monitored
- VPN effectiveness shall be regularly assessed
- VPN requirements shall be regularly reviewed

7.4 Application Access

- Application access shall be controlled
- Controls shall include:
  - Authentication requirements
  - Authorization controls
  - Data access limitations
  - Offline access restrictions
  - Session management
- Application access shall be based on need
- Application access shall be regularly reviewed
- Application access shall be promptly revoked when no longer needed
- Application access controls shall be regularly assessed

8. Monitoring and Compliance

8.1 Device Monitoring

- BYOD devices shall be monitored for security and compliance
- Monitoring shall include:
  - Security status
  - Configuration compliance
  - Application inventory
  - Patch status
  - Policy violations

- Monitoring shall respect privacy boundaries
- Monitoring scope shall be documented and communicated
- Monitoring findings shall be addressed
- Monitoring effectiveness shall be regularly assessed

8.2 Compliance Verification

- BYOD compliance shall be regularly verified
- Verification shall include:
  - Automated compliance checks
  - Periodic manual reviews
  - User self-assessments
  - Random audits
- Verification shall be documented
- Non-compliance shall be addressed
- Verification effectiveness shall be regularly assessed
- Verification shall be regularly reviewed

8.3 Non-Compliance Handling

- Non-compliant devices shall be managed
- Management shall include:
  - Notification to users
  - Remediation guidance
  - Grace periods where appropriate
  - Access restrictions
  - Escalation procedures
- Non-compliance procedures shall be documented
- Non-compliance shall be tracked
- Repeated non-compliance shall be addressed
- Non-compliance handling shall be regularly reviewed

8.4 Usage Monitoring

- BYOD usage shall be monitored
- Monitoring shall include:
  - Access patterns
  - Data transfers
  - Resource utilization
  - Security events
- Monitoring shall respect privacy boundaries
- Monitoring scope shall be documented and communicated
- Monitoring findings shall be addressed

- Monitoring effectiveness shall be regularly assessed

9. Security Incidents

9.1 Incident Types

BYOD security incidents may include: - Device loss or theft - Malware infection - Unauthorized access - Data leakage - Policy violations - Suspicious activities - Compromised credentials - Jailbreaking/rooting

9.2 Incident Reporting

- BYOD security incidents shall be promptly reported
- Reporting procedures shall be documented and communicated
- Reporting shall include:
  - Incident description
  - Device information
  - Data potentially affected
  - Actions taken
- Reporting shall be to designated contacts
- Reporting shall be timely
- Reporting effectiveness shall be regularly assessed
- Reporting shall be included in user training

9.3 Incident Response

- BYOD incidents shall be managed according to the Incident Management Policy
- Response shall include:
  - Incident assessment
  - Containment actions
  - Investigation
  - Recovery steps
  - Documentation
- Response procedures shall be documented
- Response shall be timely and appropriate
- Response effectiveness shall be regularly assessed
- Response lessons learned shall be incorporated into controls

9.4 Lost or Stolen Devices

- Lost or stolen devices shall be handled promptly
- Handling shall include:
  - Immediate reporting

    - Remote location attempts where possible
    - Remote wipe execution
    - Access revocation
    - Risk assessment
    - Documentation
- Procedures shall be documented and communicated
- Response shall be timely
- Response effectiveness shall be regularly assessed
- Response procedures shall be regularly reviewed

10. Privacy Considerations

10.1 Personal Data

- Personal data on BYOD devices shall be respected
- Privacy protections shall include:
    - Clear boundaries between personal and organizational data
    - Limitations on monitoring of personal activities
    - Transparency about organizational access
    - Minimization of impact on personal use
- Privacy protections shall be documented and communicated
- Privacy concerns shall be addressed
- Privacy impact shall be regularly assessed
- Privacy protections shall comply with legal requirements

10.2 User Consent

- BYOD users shall provide informed consent
- Consent shall cover:
    - Organizational access to device
    - Monitoring activities
    - Data management rights
    - Remote wipe implications
    - Support limitations
- Consent shall be documented
- Consent shall be refreshed when requirements change significantly
- Consent shall be legally reviewed
- Consent shall be obtained before access is granted

10.3 Personal Use

- Personal use of BYOD devices shall be permitted

- Personal use shall:
    - Not interfere with work duties
    - Not compromise security
    - Not violate acceptable use requirements
    - Not create legal liability
- Personal use guidelines shall be documented and communicated
- Personal use impact shall be regularly assessed
- Personal use issues shall be addressed
- Personal use guidelines shall be regularly reviewed

10.4 Device Wiping

- Device wiping shall respect personal data
- Wiping shall:
    - Target organizational data when possible
    - Provide notice when possible
    - Follow documented procedures
    - Be properly authorized
- Wiping procedures shall be documented and communicated
- Wiping impact shall be regularly assessed
- Wiping issues shall be addressed
- Wiping procedures shall be regularly reviewed

11. Support and Maintenance

11.1 Support Scope

- BYOD support scope shall be defined
- Scope shall include:
    - Supported devices and operating systems
    - Supported applications
    - Configuration assistance
    - Security issue resolution
    - Access problem troubleshooting
- Support limitations shall be documented and communicated
- Support effectiveness shall be regularly assessed
- Support scope shall be regularly reviewed
- Support exceptions shall be documented

11.2 User Responsibilities

- BYOD users shall have defined responsibilities

- Responsibilities shall include:
  - Device maintenance
  - Security update installation
  - Security control compliance
  - Incident reporting
  - Acceptable use compliance
- Responsibilities shall be documented and communicated
- Responsibility compliance shall be monitored
- Responsibility violations shall be addressed
- Responsibilities shall be regularly reviewed

11.3 Technical Support

- Technical support shall be provided for BYOD
- Support shall include:
  - Access issues
  - Application problems
  - Security configurations
  - Policy compliance
- Support procedures shall be documented
- Support effectiveness shall be regularly assessed
- Support issues shall be tracked and analyzed
- Support capabilities shall be regularly reviewed

11.4 Device Replacement

- Device replacement procedures shall be established
- Procedures shall include:
  - Data migration
  - Access transfer
  - Old device decommissioning
  - New device enrollment
- Replacement procedures shall be documented
- Replacement effectiveness shall be regularly assessed
- Replacement issues shall be addressed
- Replacement procedures shall be regularly reviewed

12. Termination Procedures

12.1 Employment Termination

- BYOD access shall be terminated when employment ends

- Termination shall include:
  - Access revocation
  - Data removal
  - Application removal
  - Account deactivation
  - MDM unenrollment
- Termination procedures shall be documented
- Termination shall be timely
- Termination effectiveness shall be verified
- Termination procedures shall be regularly reviewed

12.2 Role Change

- BYOD access shall be adjusted when roles change
- Adjustment shall include:
  - Access review
  - Permission updates
  - Data access changes
  - Application access changes
- Adjustment procedures shall be documented
- Adjustment shall be timely
- Adjustment effectiveness shall be verified
- Adjustment procedures shall be regularly reviewed

12.3 Voluntary Withdrawal

- Users may voluntarily withdraw from BYOD
- Withdrawal shall include:
  - Data removal
  - Application removal
  - Account reconfiguration
  - MDM unenrollment
- Withdrawal procedures shall be documented
- Withdrawal shall be timely
- Withdrawal effectiveness shall be verified
- Withdrawal procedures shall be regularly reviewed

12.4 Program Termination

- BYOD program termination procedures shall be established
- Procedures shall include:
  - Notification timeline
  - Alternative access methods

    - Data migration
    - Device decommissioning
- Termination procedures shall be documented
    - Termination shall be managed
    - Termination impact shall be assessed
    - Termination procedures shall be regularly reviewed

13. Training and Awareness

13.1 User Training

- BYOD users shall receive security training
- Training shall cover:
    - Policy requirements
    - Security best practices
    - Privacy considerations
    - Incident reporting
    - Support procedures
- Training shall be provided before access is granted
- Training completion shall be documented
- Training effectiveness shall be assessed
- Training materials shall be regularly updated

13.2 Security Awareness

- BYOD security awareness shall be maintained
- Awareness activities may include:
    - Regular communications
    - Security alerts
    - Best practices
    - Threat updates
    - Incident lessons learned
- Awareness shall address current threats
- Awareness effectiveness shall be assessed
- Awareness materials shall be regularly updated
- Awareness shall be integrated into organizational culture

13.3 Documentation

- BYOD documentation shall be maintained
- Documentation shall include:
    - Policies and procedures
    - User guides

    - Support information
    - Security requirements
    - FAQ resources
- Documentation shall be accessible to users
- Documentation shall be regularly updated
- Documentation effectiveness shall be assessed
- Documentation shall be included in training

14. Roles and Responsibilities

14.1 Management

- Approve BYOD policy
- Provide resources for BYOD security
- Review BYOD security performance
- Address significant BYOD security issues
- Support BYOD security initiatives
- Ensure compliance with requirements
- Approve risk acceptance when necessary

14.2 Information Security Team

- Develop and maintain BYOD security policy
- Define BYOD security requirements
- Review BYOD security controls
- Monitor BYOD security compliance
- Investigate BYOD security incidents
- Provide security guidance and expertise
- Report on BYOD security status

14.3 IT Department

- Implement BYOD technical controls
- Manage MDM solution
- Provide BYOD technical support
- Monitor BYOD compliance
- Support security incident response
- Implement security updates and patches
- Report on BYOD operational status

14.4 BYOD Users

- Comply with BYOD policy

- Maintain device security
- Report security incidents and concerns
- Complete required training
- Follow security best practices
- Protect organizational data
- Support security initiatives

15. Compliance and Exceptions

15.1 Compliance Monitoring

- BYOD compliance shall be regularly monitored
- Monitoring shall include:
  - Device compliance
  - User behavior
  - Security controls
  - Policy adherence
- Non-compliance shall be addressed
- Compliance trends shall be analyzed
- Compliance reports shall be provided to management
- Compliance monitoring shall be regularly reviewed

15.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate - Tracked and reported - Minimized to the extent possible - Consistent with legal and regulatory requirements

16. Related Documents

- Information Security Policy
- Acceptable Use Policy
- Mobile Device Policy
- Data Classification Policy
- Incident Management Policy
- Remote Access Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

17. Approval

This Bring Your Own Device (BYOD) Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____