

BRING YOUR OWN DEVICE (BYOD) POLICY

This is a customizable starting template, not a finished legal document. Replace every [BRACKETED] field with your specifics, delete or adapt any clause that does not fit your organization, and have a licensed attorney in the governing jurisdiction review it before you adopt or distribute it. CyberSygn is not a law firm and this template is not legal advice.

This Bring Your Own Device Policy (this "**Policy**") is issued as of [EFFECTIVE DATE] (the "**Effective Date**") by [COMPANY LEGAL NAME], a [STATE] [ENTITY TYPE, e.g. corporation] with its principal place of business at [COMPANY ADDRESS] (the "**Company**"), and applies to every [EMPLOYEE / CONTRACTOR] who uses a personally owned device to access Company systems or data (each, a "**Worker**").

Recitals. Workers increasingly use personal smartphones, tablets, and computers for work. This convenience creates risks to the security and confidentiality of Company data and to Worker privacy. The Company issues this Policy to set the conditions under which a Worker may use a personal device for work, to protect Company data, and to define the respective rights of the Company and the Worker. By acknowledging this Policy, the Worker agrees to the terms below.

1. Scope and Eligibility

1.1 Covered devices. "**Device**" means any personally owned smartphone, tablet, laptop, desktop, or wearable that a Worker uses to access, store, or process Company email, applications, networks, or data.

1.2 Voluntary participation. Use of a personal Device for work is voluntary. A Worker who prefers not to participate may request a Company-issued device, subject to availability and Company approval.

1.3 Approval. Before using a Device for work, the Worker will register the Device with [IT / SECURITY TEAM] and obtain approval. The Company may decline to approve, or may revoke approval for, any Device that does not meet its security requirements.

2. Security Requirements

2.1 Baseline controls. The Worker will keep the Device protected with a strong passcode or biometric lock, current operating-system and security updates, device encryption where available, and reputable security software where applicable.

2.2 Mobile device management. The Worker agrees to install and maintain any Company-required management or security software ("**MDM**") on the Device as a condition of accessing Company data. The Worker will not disable, circumvent, or remove MDM controls while the Device is used for work.

2.3 Prohibited modifications. The Worker will not "jailbreak," "root," or otherwise modify the Device in a way that defeats its security controls, and will not connect the Device to Company systems while it is compromised.

2.4 Network use. The Worker will avoid accessing Company data over untrusted public networks without using the Company's approved virtual private network or equivalent protection.

3. Acceptable Use

3.1 Compliance. The Worker will use the Device to access Company data only in accordance with this Policy, the Company's acceptable-use and data-protection policies, and applicable law.

3.2 Authorized applications. The Worker will access Company data only through applications and services approved by the Company, and will not transfer Company data into unapproved personal cloud storage, messaging apps, or accounts.

3.3 No unauthorized sharing. The Worker will not allow family members or other third parties to use the Device in a way that exposes Company data, and will keep the work environment on the Device logically separated from personal use where the Company provides a means to do so.

4. Company Data and Confidentiality

4.1 Ownership of data. All Company email, files, and data accessed through or stored on the Device remain the property and Confidential Information of the Company, regardless of the Device's ownership.

4.2 Containerization. Where the Company provides a managed workspace or container, the Worker will keep Company data inside it and will not copy Company data into personal areas of the Device.

4.3 Backups. The Company is not responsible for backing up the Worker's personal data. The Worker is solely responsible for backing up personal photos, contacts, and files stored on the Device.

5. Privacy and Monitoring

5.1 Scope of access. The Company's management tools are intended to protect and manage Company data on the Device, not to surveil the Worker's personal activity. The Company will limit its access to what is reasonably necessary for security and management and consistent with applicable law, which varies by jurisdiction.

5.2 What the Company may access. The Company may, consistent with Section 5.1, view Device compliance status, manage Company applications and data, enforce security settings, and, where supported, separately wipe Company data.

5.3 What the Company will not do. Except as required by law or a lawful investigation, the Company will not access the Worker's personal communications, photos, browsing history, or location for non-work purposes.

6. Remote Wipe and Data Removal

6.1 Conditions for wipe. The Company may remotely remove Company data from the Device if the Device is lost or stolen, the Worker's engagement ends, the Device falls out of compliance, or a security incident requires it.

6.2 Selective vs. full wipe. Where technically supported, the Company will perform a selective wipe limited to Company data. The Worker acknowledges that on some Devices only a full wipe is possible, in which case the Worker's personal data may be erased, and the Worker accepts that risk by participating.

6.3 Worker cooperation. The Worker will report a lost or stolen Device to **[IT / SECURITY CONTACT]** immediately and will cooperate with any wipe or investigation.

7. Costs, Reimbursement, and Liability

7.1 Expenses. **[OPTIONAL: The Company will reimburse the Worker a stipend of [\$ AMOUNT] per [MONTH] toward Device and data-plan costs / The Worker is responsible for Device and data-plan costs.]** Reimbursement obligations vary by jurisdiction, and the Company will comply with any applicable requirement to reimburse necessary business expenses.

7.2 Device loss or damage. The Company is not responsible for loss of, or damage to, the Device or the Worker's personal data resulting from work use, MDM, or a permitted wipe, except to the extent required by applicable law.

7.3 Wage-and-hour. Non-exempt Workers will not perform work on the Device outside authorized working time, and will record all time worked, consistent with applicable wage-and-hour law.

8. Separation and Offboarding

8.1 On separation. When the Worker's engagement ends, the Worker will allow the Company to remove Company data from the Device, will return any Company-licensed software, and will cease accessing Company systems.

8.2 Certification. The Company may require the Worker to certify in writing that all Company data has been removed from the Device.

9. General Provisions

9.1 No contract. **[OPTIONAL: For at-will jurisdictions:]** This Policy does not create a contract of employment or alter the at-will nature of any employment relationship.

9.2 Governing law. This Policy is governed by the laws of the State of **[STATE]**, to the extent consistent with applicable federal and local law.

9.3 Updates. The Company may update this Policy and will communicate material changes. Continued use of a Device for work after notice constitutes acceptance.

9.4 Severability. If any provision is unenforceable, the rest remains in effect.

9.5 Acknowledgment. By signing below, the Worker confirms they have read, understood, and agree to comply with this Policy as a condition of using a personal Device for work.

ACKNOWLEDGMENT AND CONSENT

I have received, read, and understood this BYOD Policy. I consent to the installation of Company management software on my Device and to the removal of Company data as described, and I agree to comply with this Policy.

WORKER	COMPANY REPRESENTATIVE
Signature: _____	Signature: _____
Printed name: [NAME]	Printed name: [NAME]
Title: N/A	Title: [TITLE]
Date: _____	Date: _____

Template provided by CyberSygn. Not legal advice. CyberSygn is not a law firm. Consult a licensed attorney in your jurisdiction before relying on this document.