BYOD – BRING YOUR OWN DEVICE POLICY AGREEMENT TEMPLATE

This BYOD – Bring Your Own Device Policy Agreement (the "Agreement") is made and effective [DATE],

BETWEEN: **[YOUR COMPANY NAME]** (the "Company"), a corporation organized and existing under the laws of the [State/Province] of [STATE/PROVINCE], with its head office located at:

[YOUR COMPLETE ADDRESS]

AND: **[EMPLOYEE or PERSON YOU HIRED]** (the "Employee", "contractor", "intern" or "person completing work in your company"), a corporation or entity organized and existing under the laws of the [State/Province] of [STATE/PROVINCE], with its head office located at:

[COMPLETE ADDRESS]

NOW, THEREFORE, in consideration of the promises and agreements set forth herein, the receipt and sufficiency of which are hereby acknowledged by the parties, the parties intending to be legally bound hereby, do promise and agree as follows:

1. POLICY BRIEF & PURPOSE

The BYOD – Bring Your Own Device Policy outlines our guidelines for allowing employees to use their own smartphones, tablets, laptops and their own devices within an organization's network. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation. The [Company] reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of [The Company] and its data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

SCOPE

This BYOD – Bring Your Own Device Policy applies to all our employees, contractors, volunteers and partners who access our network and computers. Employees and workers must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

2. ACCEPTABLE USE

- The company defines acceptable business use as activities that directly or indirectly support the business of [YOUR COMPANY NAME]
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company.
    - Such websites include but are not limited to [LIST WEBSITE TYPES]

- Devices' camera and/or video capabilities [ARE/ARE NOT] disabled while on-site
- The following apps are allowed [include a detailed list of apps such as weather, productivity apps, Facebook, etc, which will be permitted)
- Employees may use their mobile devices to access the following company-owned resources: [email, calendars, contacts, documents, etc].

What is inappropriate BYOD usage?

Our employees must not use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Harass others
- Store or transmit proprietary information belonging to another company
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.
- The following apps are NOT allowed (apps not downloaded through iTunes or Google play, etc)
- [Company] has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask [*their supervisor/ IT manager/ etc*.]

Our company may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

3. DEVICES AND SUPPORT

Allowed Devices

The list should be as detailed as necessary including models, operating systems, versions, etc.

- TABLETS: including ipads and Adroid are allowed [includd detailed list]
- SMARTPHONES: including iPhone, Android, Blackberry, Windows phones are allowed [include detailed list].
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

4. REIMBURSEMENT

- The company [will/will not] reimburse the employee for a [% percentage] of the cost of the device [include the amount of the company's contribution], or the company will contribute [X amount of money] toward the cost of the device.

- The company will
    - a) Pay the employee an allowance
    - b) Cover the cost of the entire phone/data plan
    - c) Pay half of the phone/data plan, etc.
- The company [will/will no] reimburse the employee for the following charges: [list any here such as: roaming, plan overages, etc].

5. SECURITY

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is [input the company password policy in here, for example, passwords must be at least 6 characters with a combination of upper and lower case letters, numbers and symbols].
- Employees are automatically prevented from downloading, installing and using any ap that does not appear on the company's list of approved apps.
- Smartphone and tablets that are not on the company's list of supported devices [are/are not] allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if
    - The device is lost,
    - The employee terminates his or her employment,
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

6. MODIFICATION OF AGREEMENT

This Agreement may be supplemented, amended, or modified only by the mutual agreement of the parties. No supplement, amendment, or modification of this Agreement shall be binding unless it is in writing and signed by all parties.

7. ENTIRE AGREEMENT

This Agreement and all other agreements, exhibits, and schedules referred to in this Agreement constitute(s) the final, complete, and exclusive statement of the terms of the agreement between the parties pertaining to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings or agreements of the parties. This Agreement may not be contradicted by evidence of any prior or contemporaneous statements or agreements. No party has been induced to enter into this Agreement by, nor is any party relying on, any representation, understanding, agreement, commitment or warranty outside those expressly set forth in this Agreement.

8. SEVERABILITY OF AGREEMENT

If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part thereof shall be stricken from this Agreement, and such provision shall not affect the legality, enforceability, or validity of the remainder of this Agreement. If any provision or part thereof of this Agreement is stricken in accordance with the provisions of this section, then this stricken provision shall be replaced, to the extent possible, with a legal, enforceable, and valid provision that is as similar in tenor to the stricken provision as is legally possible.

9. RISKS/LIABILITIES/DISCLAIMERS

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software, or hardware failures, or programming errors that render the device unusable.
- The company reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

10. GOVERNING LAW

It is agreed that this agreement shall be governed by, construed, and enforced in accordance with the laws of the [State/Province] of [STATE/PROVINCE].

IN WITNESS WHEREOF, the parties have executed this Agreement on the dates set forth first above, with full knowledge of its content and significance and intending to be legally bound by the terms hereof.

COMPANY	EMPLOYEE/INTERNET USER
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Print Name and Title	Print Name and Title