**BRING YOUR OWN DEVICE TO WORK POLICY**

**PURPOSE**

[EMPLOYER'S NAME] [encourages/permits] [all employees/[SPECIFIED EMPLOYEES]] to use their own personal electronic devices, such as smartphones, tablets, laptops, wearable technology, and mobile phones ("**devices**"), to perform work for [EMPLOYER'S NAME] or on its behalf. However, any use of these devices for business purposes must align with the guidelines set forth in this policy. Furthermore, each employee is responsible for ensuring that their use of personal devices remains sensible, productive, ethical, and lawful.

This policy applies to the use of personal devices for work-related activities on behalf of [EMPLOYER'S NAME] during both working and nonworking hours, whether on or off [EMPLOYER'S NAME]'s premises.

This policy complies with all applicable laws and regulations in the state of Vermont, ensuring alignment with state-specific requirements for the use of personal devices for work purposes.

**PRIVACY EXPECTATIONS AND DATA MONITORING**

All materials, data, communications, and information, including but not limited to emails (incoming and outgoing), telephone calls and voicemails, instant messages, and online activity related to [EMPLOYER'S NAME]'s business ("**[EMPLOYER'S NAME] content**") are considered the property of [EMPLOYER'S NAME], regardless of the device used.

You are explicitly informed that to prevent misuse, [EMPLOYER'S NAME] reserves the right to monitor, access, review, and remotely erase [EMPLOYER'S NAME] content—or even the entire contents of the device, including personal content—without notice. This includes, but is not limited to, monitoring, intercepting, accessing, reviewing, or printing communications and activities on the device, even if it is in your possession. Therefore, you should have no expectation of privacy in any [EMPLOYER'S NAME] content. While personal content may be private under legal protections, it should not be assumed to be exempt from review if mixed with [EMPLOYER'S NAME] content.

[EMPLOYER'S NAME] may also preserve copies of [EMPLOYER'S NAME] content, or the entire contents of the device, at its discretion, and may delete these copies periodically without notice. Additionally, [EMPLOYER'S NAME] may share such copies in connection with investigations, litigation, or as required by law.

By acknowledging this policy, you consent to [EMPLOYER'S NAME] monitoring, reviewing, copying, disclosing, and wiping any [EMPLOYER'S NAME] content—or the entire contents of the device, including your personal content—at [EMPLOYER'S NAME]'s discretion. You also accept that the use of personal devices for business purposes is at your own risk and that [EMPLOYER'S NAME] will not be responsible for any loss or damage to content, devices, or functionality.

**DEVICE SECURITY REQUIREMENTS**

To ensure the protection of [EMPLOYER'S NAME]'s confidential information, all devices used for work or on behalf of the company must be registered and authorized by [PERSON/POSITION] in the [DEPARTMENT NAME] Department.

If a device used for work is lost, stolen, or accessed by unauthorized individuals, you must report it immediately to allow [EMPLOYER'S NAME] to assess the risk and take necessary actions, including remotely wiping [EMPLOYER'S NAME]'s content—or even all content on the device, including personal data. You must also provide access to the device if requested for business purposes, including in the case of security incidents or investigations.

[EMPLOYER'S NAME]'s [INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS POLICY] applies to all work-related device usage. Additionally, you must adhere to the following security practices:

* [Install required security software as directed by [EMPLOYER'S NAME] and provide any necessary access credentials.]
* [Follow [EMPLOYER'S NAME]'s guidelines for device configuration and settings.]
* [Ensure strong password protection and adhere to [EMPLOYER'S NAME]'s password policies.]
* [Configure the device to lock after [X] minutes of inactivity and suspend access after [X] failed login attempts.]
* [Keep the device’s operating system current, with all necessary security updates.]
* [Do not install or download unauthorized software, including apps, unless specifically allowed by [EMPLOYER'S NAME].]
* [Avoid changing security settings on the device without approval.]
* [Ensure only authorized individuals can access the device, including preventing family, friends, or unauthorized associates from using it.]
* [Do not store or transfer work-related or sensitive business content without [EMPLOYER'S NAME]'s consent.]
* [Avoid backing up or storing company data on personal or cloud-based storage without prior approval from [EMPLOYER'S NAME].]
* [Do not use the device as a personal hotspot unless approved by [EMPLOYER'S NAME].]
* [Avoid transmitting company information over unsecured networks.]

You are also expected to take all reasonable precautions to protect the device from theft, damage, or unauthorized access at all times.

**INTERNATIONAL TRAVEL**

When traveling internationally, whether for business or leisure, employees must take extra precautions to safeguard [EMPLOYER'S NAME]'s confidential information. All international travel with personal electronic devices containing [EMPLOYER'S NAME] content must comply with [EMPLOYER'S NAME]'s information security policies[, including the [POLICY NAME] Policy].

To ensure proper security, employees traveling internationally must:

* [Notify [PERSON/POSITION] of your travel plans, including dates and destination countries, at least [two weeks/[OTHER TIME PERIOD]] prior to departure.]
* [Follow all instructions provided by [PERSON/POSITION] regarding [EMPLOYER'S NAME] content on your device, which may include encryption, deletion of certain files, or using a loaner device while traveling.]
* [Comply with [EMPLOYER'S NAME]'s procedures for dealing with customs or border inspections of electronic devices, including:
	+ Informing border officials that the device contains confidential business information.
	+ Presenting your [business card/company identification badge/[OTHER]] to verify your employment with [EMPLOYER'S NAME].
	+ Assisting border officials with accessing encrypted or password-protected devices, as required under [EMPLOYER'S NAME]'s policies.]
* [ADDITIONAL PRECAUTIONS.]

It is critical to follow these steps to mitigate risks to [EMPLOYER'S NAME]'s data integrity and security when traveling internationally. Failure to comply with these requirements may result in disciplinary action.

**APPROPRIATE USE OF PERSONAL DEVICES**

All use of personal devices under this policy must adhere to [EMPLOYER'S NAME]'s policies against harassment, discrimination, and retaliation, including [NAME(S) OF POLICIES]. Devices must not be used in a manner that could be perceived as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religion, or any other protected characteristic under federal, state, or local laws.

Nonexempt employees must accurately track all time spent working on personal devices, including during nonworking hours. Use of devices for work outside regular hours requires prior written approval from [EMPLOYER'S NAME].

New employees using personal devices for the first time must ensure all information from prior employment is erased before use for [EMPLOYER'S NAME]'s business purposes.

Employees discontinuing use of a personal device for work or leaving [EMPLOYER'S NAME] must allow [EMPLOYER'S NAME] to remove work-related content and disable any employer-provided software or services on their devices.

Device use while operating equipment

Employees are strictly prohibited from talking, texting, emailing, or using devices while operating company-owned or personal vehicles, machinery, or equipment for [EMPLOYER'S NAME]. This prohibition applies regardless of device ownership and includes compliance with all applicable federal, state, and local laws on device use while driving or operating equipment.

For the safety of all employees and others, refrain from using devices in any way that compromises your attention while operating vehicles, machinery, or equipment.

**TECH SUPPORT FOR PERSONAL DEVICES**

Self-supported devices

[EMPLOYER'S NAME] does not provide technological support for personal devices used under this policy. By signing [this policy/the handbook acknowledgment], you acknowledge that you are solely responsible for the repair, maintenance, or replacement of your device, as well as any associated costs or services.

OR

Company-supported devices

[EMPLOYER'S NAME] provides the following technological support for personal devices used under this policy:

* [SPECIFY THE SUPPORT, SUCH AS DEVICE CONFIGURATION, SOFTWARE INSTALLATION, OR LIMITED TROUBLESHOOTING.]

Employees are responsible for coordinating any additional services not covered by [EMPLOYER'S NAME]'s support.

**COSTS AND REIMBURSEMENTS**

Employee-supported devices

Employees are responsible for all costs associated with their personal devices used under this policy, including device acquisition, voice and data usage charges, repair, and maintenance. By signing [this policy/the handbook acknowledgment], you acknowledge that any additional costs incurred due to work-related use, including increased voice or data plan charges, are solely your responsibility.

OR

Reimbursement for business use

[EMPLOYER'S NAME] reimburses employees for actual business-related device expenses, including a pro rata share of necessary repair or replacement costs. To qualify for reimbursement, employees must submit:

* A copy of their monthly statement or bill substantiating business-related voice and/or data usage.
* A receipt or bill substantiating repair or replacement costs, if applicable.

Submit reimbursement requests to [PERSON/POSITION]. For further details, contact [PERSON/POSITION].

OR

Flat rate reimbursement

[EMPLOYER'S NAME] offers a fixed reimbursement for business-related device usage:

* Voice services: $[NUMBER] per month.
* Data services: $[NUMBER] per month.
* Voice and data services: $[NUMBER] per month.
* Repair or replacement: $[NUMBER] per [month/year/[TIME PERIOD]].

To qualify for reimbursement, employees must submit substantiating documentation, such as monthly statements or repair receipts, to [PERSON/POSITION].

OR

Comprehensive coverage

[EMPLOYER'S NAME] fully reimburses employees for all costs associated with work-related device usage, including acquisition, voice and data plans, repairs, and replacements. For details on the reimbursement process, contact [PERSON/POSITION].

**CONFIDENTIALITY AND INTELLECTUAL PROPERTY RIGHTS**

[EMPLOYER'S NAME]'s confidential information and intellectual property, including trade secrets, are vital assets that must be safeguarded. Employees are expected to handle this information with care and ensure it is not compromised through the use of personal devices.

* Confidential information: Disclosure of any confidential information to individuals outside [EMPLOYER'S NAME] is strictly prohibited unless authorized. Employees must follow the guidelines set forth in [EMPLOYER'S NAME]'s [CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT OR POLICY].
* Intellectual property: The use of [EMPLOYER'S NAME]'s intellectual property on personal devices is also governed by [EMPLOYER'S NAME]'s [CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT OR POLICY].
* Work product: Any work product created, stored, or maintained on personal devices remains the property of [EMPLOYER'S NAME] and is subject to the terms of [EMPLOYER'S NAME]'s confidentiality and proprietary rights policies.

For further clarification, please review [EMPLOYER'S NAME]'s [CONFIDENTIALITY AND PROPRIETARY RIGHTS AGREEMENT OR POLICY] or contact [PERSON/POSITION].

**FAILURE TO COMPLY**

Failure to adhere to any provision of this policy will result in disciplinary action, which may include verbal or written warnings, suspension, or, in serious cases, termination of employment. The severity of the consequences will depend on the nature and impact of the violation.

For questions about this policy or its enforcement, please contact [PERSON/POSITION].

**POLICY ADMINISTRATION**

[EMPLOYER'S NAME] reserves the right to revise, modify, or discontinue this policy at its discretion and without prior notice.

The [DEPARTMENT NAME] Department oversees the administration of this policy. For questions about the policy or specific guidance regarding the use of personal devices for work, please contact the [DEPARTMENT NAME] Department.

**APPLICABILITY TO COLLECTIVE BARGAINING AGREEMENTS**

The provisions of this policy are designed to complement, not replace, amend, or override, any terms or conditions of employment outlined in a collective bargaining agreement between a union and [EMPLOYER'S NAME].

Employees covered by a collective bargaining agreement should refer to the specific terms outlined in that agreement.

In cases where this policy conflicts with the collective bargaining agreement, the terms of the collective bargaining agreement will prevail.

For additional guidance, consult your collective bargaining agreement or contact [PERSON/POSITION].

**ACKNOWLEDGEMENT OF RECEIPT AND REVIEW**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received and reviewed a copy of [EMPLOYER'S NAME]’s [NAME OF POLICY]. I understand that it is my responsibility to familiarize myself with the policy and adhere to its terms.

I also acknowledge that this policy is not intended to create an employment contract or alter my at-will employment status, unless otherwise specified in a written agreement signed by an authorized representative of [EMPLOYER'S NAME]. Any delay or failure by [EMPLOYER'S NAME] to enforce the provisions of this policy does not constitute a waiver of its rights to enforce them in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date