1. **Purpose**

The purpose of this policy is to establish guidelines for the use of personal devices for work purposes (hereafter “BYOD Policy” or “BYOD Program”). This BYOD Program is intended to protect the confidentiality, integrity, and availability of [ORGANIZATION NAME] (hereafter “[ORG ACRONYM]” or “organization”) data, while also respecting the privacy of employees.

1. **Scope**

This policy applies to all employees who choose to participate in the BYOD Program and their registered devices. Devices may include, but not limited to, laptops, smartphones, tablets, and other mobile devices.

1. **Eligibility**

To participate in the BYOD Program, employees must:

1. Be current on all cyber trainings,
2. Agree to the terms of this policy, and
3. Enroll any device with which they intend to access [ORG ACRONYM] information with [ORG ACRONYM] IT Department.
4. **Acceptable Use**

Employees who participate in the BYOD Program are permitted to use their personal devices for work purposes as long as they comply with the terms of this policy. Employees are responsible for ensuring that any data or information on their personal device is secure and not accessible by unauthorized persons. Any use of a personal device for business purposes must conform to this policy and other [ORG ACRONYM] policies and each user is responsible for using their device in a productive, ethical, and lawful manner. Acceptable use includes:

1. Accessing organization email, calendars, and other work-related applications,
2. Storing organization data on personal devices, and
3. Using personal devices to connect to the organization network.
4. **Security Requirements**

Employees who participate in the BYOD Program are responsible for taking steps to secure their personal devices. These steps may include:

1. Using strong passwords and encryption,
2. Keeping software up to date,
3. Staying current on all [ORG ACRONYM] cyber trainings,
4. Being vigilant against phishing scams and other cyber threats, and
5. Refraining from use or access of organization data while traveling internationally.
6. **Monitoring and Privacy**

The organization respects the privacy of its employees. [ORG ACRONYM] shall not access or collect any personal data on the device without the employee's consent, except in the case of a data breach investigation. [ORGANIZATION NAME] will not remotely monitor personal devices but reserves the right to inspect personal devices subject to this policy in the event of a termination of employment or if an employee is the subject of a formal investigation.

1. **Lost or Stolen Devices**

If a personal device that is enrolled in the BYOD Program is lost or stolen, the employee must notify the organization within two hours. [ORG ACRONYM] may then take steps to secure [ORG ACRONYM] data on the device. These steps may include requesting the employee to remotely wipe the device or institute a temporary or permanent lock-out of organizational systems.

1. **Reimbursement**

[ORG ACRONYM] will not reimburse employees for expenses incurred while using their personal devices for work. These expenses may include:

1. The cost of data plans,
2. The cost of accessories, or
3. The cost of repairs.
4. **Changes to the BYOD Policy**

[ORG ACRONYM] reserves the right to change this policy at any time. Employees will be notified of any changes to the policy. If there are material changes to the BYOD Program, [ORG ACRONYM] may require enrollees to opt-in again.

1. **Opt-In**

By using a personal device for work purposes, the employee agrees to the terms of this policy. If the employee does not agree to the terms of this policy, they may not use their personal device for work purposes.

By signing below the employee, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, acknowledges their understanding above the above BYOD policy and agrees to be bound by its terms. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, hereby enrolls the following devices in the [ORG ACRONYM] BYOD Program:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Received on Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT Dept. Rep.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_