PERIMATICS

13701 NE Bel-Red Rd, Suite 103
Bellevue, WA 98005
https://www.perimatics.com

PERSONAL DEVICE POLICY

1. OVERVIEW

Perimatics needs to protect the information assets of the company from abuse and theft. This policy outlines the rules in place to allow convenient access for personal devices at work without compromising information security.

2. PURPOSE

Perimatics grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. Perimatics reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

3. SCOPE

This policy applies to all Perimatics staff who create, deploy, or support application and system software. Perimatics' employees 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.

4. POLICY

1.1 Acceptable use

- Perimatics defines acceptable business use as activities that directly or indirectly support the business of Perimatics.
- Perimatics 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 applications and websites during work hours/while connected to the corporate network at the discretion of the company. Such applications/websites include bit-torrent, peer-to-peer file sharing systems, dark web access of any kind, and pornographic content access.
- Devices' camera and/or video capabilities are disabled while on-site.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another company
    - Harass others
    - Engage in outside business activities

The following apps are not allowed:

- apps not downloaded through iTunes or Google Play

Employees may use their mobile device to access the following company-owned resources:

- email
- calendars
- contacts
- documents that do not contain any sensitive, customer, Protected Health Information (PHI) or Personally Identifiable Information (PII) data of anyone.

1.2 Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed. Tablets including iPad and Android are allowed.
- All devices must use an operating system no older than the previous to the latest operating system available in the market.
- Phone and device operating systems must be patched to the latest security patch available for that device configuration within one month of market availability of such a patch.
- Connectivity issues are not supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

1.3 Reimbursement

- The company will not reimburse the employee for a percentage of the cost of the device or services.

1.4 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: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.

- After five failed login attempts, the device will lock.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only 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 must be remotely wiped if
    - the device is lost
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

1.5 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 expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- 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.

5. ENFORCEMENT

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

6. DISTRIBUTION

This policy is to be distributed to all Perimatics staff responsible for support and management.

7. POLICY VERSION HISTORY

Version	Date	Description	Approved By
1.0	11/15/2018	Initial Policy Drafted	COO