Personal Workplace Device Policy

1. **Overview**

Bringing your own device to work is a common occurrence. We recognize that for some employees bringing and using a personal electronic device, including tablets, laptops, smart phones and other devices is convenient and practical. However, the use of personal devices for work purposes and during work time must be well managed.

2. **Purpose**

This policy will help our employees understand the appropriate use of their personal electronic devices for work purposes and during working hours including security, access to the network and details of use.

- The purpose of this policy is to:
  - Protect the security and integrity of _____ (company name) information, data, technology and technology infrastructure.
  - Clarify for employees the limitations and scope of personal and business use of a personal electronic device during working hours and when accessing the company network including outside normal working hours.

3. **General Use and Permissions**

Our organization does grant our employees the right to bring and use their own personal electronic devices to work and for work purposes. These devices must be identified to and approved by IT before accessing the organizations network. We do reserve the right to revoke this permission at our own discretion if the user does not abide by the policies we have established.

All employees must agree to the terms and conditions of this policy and our expectations in order to connect personal electronic devices on the company network or for work purposes (such as emailing clients or colleagues, accessing and storing organizational information).

Employees must present their Personal Electronic Devices to IT for training and review for setup and security reasons. We reserve the right to remove any and all organization data from the employee’s personal device when we deem it necessary and

appropriate and will take every precaution not to remove or damage the user's personal information or data or access the same during the process of removing our data.

4. **Acceptable Use**
    - Activities that directly or indirectly relate or support the business of _____ (company name) are defined as acceptable use. For example communicating to those connected with the organization, accessing the organization's network, storing, transferring or inputting business information, research and related activities (within our general security guidelines including confidentiality restrictions).
    - The device may be used to connect to the organizations network to access applications, calendars, emails, documents, Intranet, etc. (based on an employees profile this access may be restricted or limited).

5. **Restrictions**
    - During working hours employees using their personal devices must refrain from accessing certain websites in accordance with our policy on 'appropriate websites'. These websites include but are not limited to . . . .
    - Employees are restricted from downloading applications that can access the company network which are not approved. Generally applications available from approved sources such as Google Play, iTunes and . . . . are permissible (check with IT or Security when in doubt before downloading any unapproved application).
    - Accessing personal games, messages, communications, photos, social networks and other content on a personal device during work hours must be reasonable and comply with the policies on appropriate work activities. See "Use of Time at Work Policy'
    - Use of personal device while driving or when operating equipment is not permissible except in certain situations where a device is appropriately used hands free.
    - Use of cameras for recording work related tasks or activities in the workplace is not permissible unless previously approved by IT, HR or a supervisor/manager
    - Devices may not be used to harasses, intimidate or other inappropriate activities
    - Device may not be used to gather, store or share proprietary information including information from our organization. When accessing our organizations network the device may not contain proprietary information from another organization and proprietary information from another organization may not be uploaded or otherwise stored on our organizations network.
    - Device may not be used to conduct outside business activities during working hours

6. **Current List of Approved Devices**
    - Smartphones: Including Android, Iphone, Blackberry, and Windows phones (list of models, operating systems and versions will be available from IT)
    - Tablets: Including Ipad, Android, Blackberry (list of models, operating systems and versions will be available from IT)

- If your device is not on the approved list of devices please see IT for an evaluation

7. **Cost Sharing**

Personal Electronic Devices used for work purposes may/may not be eligible for cost sharing (reimbursement).

- May be eligible for reimbursement and/or the organization will contribute X amount towards the purchase of a new device
- Our organization may pay a monthly allowance to a) cover an agreed upon maximum cost of the device including data plan or b) cover an agreed upon percentage cost based on an appropriate and approved data plan
- The organization will reimburse the employee only for approved additional charges such as roaming charges, plan overages when the device is used for organizations business (details such as dates, time and details about the business being conducted must be submitted before approval)

8. **Security**
    - Employee is required to ensure that their device is secure and all organizational data is secure when stored on their personal device
    - Employee is liable for costs or activities associated with their personal device, including risk associated with the partial or complete loss of the individual personal or the organization data due to operating system failure, crash, errors, software or hardware failures, malware, bugs or viruses or other failures that make the device unusable
    - It a personal device is lost or stolen the employee must notify the organization and IT immediately.
    - IT may install a GPS tracking program on the employee's device and/or the employee is urged to install a tracking device if the device is lost or stolen. The organization will only access the GPS under approved and appropriate circumstances and in accordance with Canadian privacy protection laws in our jurisdiction.
    - The organization may disconnect or disable the device from our network at any time and at our discretion.
    - The organization may remove any and all information related to the organization's business from the employee's personal device at our discretion. This includes remotely removing all data when the device is 1) lost or stolen, 2) the employee is no longer an employee, or 3) the organization has reason to believe the information is being misused or is not secure.
    - The employee will be required to use a secure password to access the company network frcourses perrsonal device at all times. Our organization's password requires a minimum 6-character password containing one upper case letter, number, and symbol.
    - Based on the employee's organizational profile, access to the organization network may be limited and restricted

Note failure to appropriately comply with and adhere to our policy on appropriate use of personal electronic devices in the workplace, including during and outside of work hours, can result in disciplinary actions up to and including termination (for more information refer to our policy on "Progressive Discipline").