**Personal Device Usage Policy**

* **Overview:**

The Company would like to provide greater mobile device choice to its knowledge workers and simultaneously reduce end-user mobile device complexity. Providing secured company email/calendar/ contacts data, mobile applications and secure intranet access on employee personal mobile devices allow these employees to use the devices they prefer.

* **Purpose**

The purpose of this document is to define the responsibilities, guidelines, and terms of use for employee owned mobile devices configured for Company data use.

* **Definitions**
* **Mobile Device** – Employee-provided smartphone, tablet or laptop intended to be used to perform Company-related work activities
* **Company Computing Resources** – Computer hardware, software, data and network resources used by the Company, including applications, intranet web access and Company email/ calendar/contacts
* **Users** – Employees, contractors, consultants, temporary workers, and other persons or entities authorized to use approved Mobile Devices to access Company Computing Resources
* **Device Management** – Management, security, and monitoring of all Mobile Devices that access to Company Computing Resources.
* **Scope**

This document applies to employees who wish to access Company Computing Resources on a personal Mobile Device. Personal Mobile Devices referenced in this document are limited specifically to those listed in the Approved and Certified Mobile Devices for BYOD.

* **Eligibility**

The Company is making the Bring Your Own Device (BYOD) program available to Users who are willing to agree with the policies and guidelines, and have a device that is listed in the Approved and Certified.

* **Responsibilities**
* **Information Technology Responsibilities**
* Information Technology (IT) is responsible for configuring and supporting the User’s Mobile Device to access Company Computing Resources.
* IT is responsible for smartphone system removal and performing a “remote wipe” of company data from a User’s lost or stolen Mobile Device. In some situations, IT may perform a full device wipe after providing sufficient notice to the User to allow for personal data backup.
* IT is responsible for smartphone system removal and performing a “remote wipe” of Company data from a User’s Mobile Device upon termination of employment with the Company.
* IT is responsible for maintaining a list of stipend-eligible employees and providing Accounting/Payroll access to that list.
* **User Responsibilities**
* The User is responsible for using Company Computing Resources on his or her personal Mobile Device within the same constraints as on a Company-owned device by adhering to all device and network acceptable use guidelines referenced within.
* The User will not download or transfer sensitive business data to their Mobile Device outside of managed and approved mobile Computing Resources and applications.
* The User will password-protect the Mobile Device.
* The User must maintain the original Mobile Device operating system and keep the device current with security patches and updates, as released by the manufacturer.
* The User agrees not to share the Mobile Device with other individuals or family members.
* The User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments.
* The User will not backup/download/transfer sensitive business data/documents to any third party service.
* The User is responsible for contacting the IT Help Desk immediately in the event that their Mobile Device is lost or stolen.
* The User is responsible for contacting the IT Help Desk immediately if they have replaced their Mobile Device.
* **Procedures and Security**
* **Program Signup**

Employees wishing to participate in the program must complete and submit a request, and agree by signing in the appropriate space on the form that they have read and understood this document. Participating employees approved to receive a stipend must agree to the Mobile Device Stipend Terms and Conditions by signing and attaching the form.

* **Mobile Device Limitation**

The Company allows one (1) personal device for Company Computing Resources access for each participating User. Additional licenses will be based on business need and will require CIO approval.

* **Mobile Device Restrictions and Controls** The Company may place various security controls and restrictions on your device. These include the enforcement of a passcode and limiting of device capabilities, such as device camera, access to cloud services and restriction of certain applications. Specifics on these polices can be found in the Current Enforced Policies for BYOD Devices document.
* **Accessing Company Computing Resources**
* As a prerequisite for accessing Company Computing Resources on a User’s personal device, the User must first enroll their device in the Company Device Management system.
* Once a participating employee enrolls their approved Mobile Device and the device is configured by the Device Management system, all corporate access and data will be managed and controlled by the Device Management system.
* **Jailbroken or Rooted Devices**

Jailbroken Apple iOS devices and rooted Android devices pose a risk to Company data contained within the secure communications app. Therefore, the Company will disable or remove company data access on devices determined to be jailbroken or rooted.

* **Expectation of Privacy**

The company will manage the configuration of the Mobile Device and, as such, will have access to information on the device including location, installed applications, data usage and other device related information.

**Source:** <http://content.maas360.com/www/images/silverStripe/breakingblackberry/wp_maas360_breaking_blackberry_PersonalDeviceUsage.pdf>