REGINA Infinite Horizons | City of Regina

Corporate Policy

Policy Title:	Applies to:		Reference #
Mobile Device Security Policy	City of Regina staff and elected officials and contractors/third parties		MDM-001
Approved by:	**Dates:**		**Total # of Pages**
Technology Governance Committee (TGC)	**Effective:**	Jan 17, 2013	4
	Last Review:	March 15, 2021	
	Next Review:	2 Years	

1. PURPOSE:

The purpose of this policy is to ensure mobile devices are secure and the computer systems and corporate information that are accessed from these devices are protected from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or data loss.

2. SCOPE:

This policy applies to all employees, contractors, elected officials, consultants, temporaries and other workers using a City of Regina corporately owned and/or BYOD mobile device that access, store or process corporate information.

3. DEFINITIONS:

The terms and definitions listed below are meaningful for this policy.

a) **BYOD**: Bring Your Own Device is a device owned by the employee/third party that is used for City business. There are two types of BYOD devices: A device owned by the employee/third party that is approved for City business and is placed on the City's mobile service provider plan; and a device owned by the employee/third party who uses their personal device and personal data plan to access corporate resources for their own convenience.
b) **Jailbreaking/Rooting**: Process used to modify the operating system running on an a mobile device to allow the user greater control over their device, including the ability to remove operating system imposed restrictions and install apps obtained through means other than the official App Stores.
c) **MDM**: Mobile Device Management is software that is used to manage the security of mobile devices that are used to access business data.
d) **Mobile Devices:** These include, but are not limited to, smart phones, cellular phones, tablet PCs and other similar devices.
e) **Screen Lock:** Mechanism to hide data on a visual display while the device continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.
f) **Selective Remote Wipe:** Process to remove corporate data from a device leaving personal information on the device but erasing data, documents, settings, and applications explicitly linked with the organization.

g) User: Anyone with authorized access to City information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants and other parties with valid state access accounts.

4. POLICY STATEMENT:

The following security policies will be in effect for all mobile devices that are used to access any City of Regina information:

- All devices must be registered and remain compliant with the City of Regina's Mobile Device Management (MDM) software to have access to City information. The City's MDM software will enforce security measures to ensure the protection of City information within all City of Regina Managed Applications such as Office 365. Protection measures may include the inability to copy, share or store City files within non-City applications.
- Users must accept the City's Mobile Device Terms of Use Waiver during enrollment into MDM.
- Corporate owned mobile devices will be limited to Samsung and iPhone models only, to ensure the security settings within the device comply with the City's MDM software.
- All devices must remain current with operating system (OS) updates.
- All corporate data in-transit will be encrypted.
- All corporate data at rest on mobile devices will be encrypted.
- All data on a corporate owned mobile device and all corporate data on a BYOD device is the property of the City and can be subject to City legislation and LAFOIP procedures.
- All users must ensure their device is not left unattended in such a way that data is available to outside parties.
- All mobile device users will be required to comply with the City's password policy when setting passwords.
- The City will limit the ability to access and/or share/save sensitive corporate data from/onto a mobile device.
- The City reserves the right to track the locations of corporately owned devices.

Client Support Team will remotely disable and/or remotely wipe a corporate owned device of data in the following circumstances (BYOD devices are subject to selective remote wipe in the following circumstances):

- When a device is lost or stolen.
- When the device manufacturer's content and security controls have been circumvented (i.e. jailbreaking/rooting).
- When an individual's employment with the City of Regina ends.
- If an employee is not in compliance with this policy.

Personally owned and corporately enabled BYOD devices that are not compliant with this policy will have access to City information removed and will be removed from the City's voice and data plans (if applicable).

Employee Responsibilities:

- When using a mobile device at the City of Regina, employees are required to understand and conduct themselves in accordance with the following policies:
    - Employee Code of Conduct
    - Email Acceptable Use Policy
    - Internet Acceptable Use Policy
    - Password Policy
    - Mobile Device Support Policy
    - Mobile Device Buyout and Phone Number Transfer Policy
    - Employee Privacy Guideline
- Employees must protect the mobile device against physical threats and are expected to take all reasonable steps to prevent theft or loss. (e.g. Devices should never be left unattended in public places, left in plain view in an unattended vehicle, or stored in other unsecure locations such as an unlocked, unattended desk at the office.
- Employees are responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a device being remotely wiped or remotely selective wiped for any reason. The City cannot guarantee that personal files will not be lost during a selective remote wipe process. It is recommended that employees backup their personal data frequently to minimize loss.
- Employees must report a lost or stolen mobile device to the Client Support Team (306-777-7980) immediately, to ensure the appropriate security measures are taken (such as wiping the device, cancelling the voice/data plan, etc.)
- Employees who exit the City are responsible to ensure that their device is factory re-set prior to returning it the to the City.
- Employees who buyout a device are required to work with Client Support Team to ensure all Corporate data is removed from the device.

Client Support Responsibilities:

- Client Support Team will maintain the City's MDM software to ensure access to City information is secure.
- Client Support Team will administer all devices with access to corporate applications and data and ensure compliance to this policy.
- Recommend modifications to this policy.

Technology Governance Committee Responsibilities:

- Approval of Policy

5. ENFORCEMENT:

Willful or negligent violation of this policy may result in loss of access privileges and/or disciplinary action in accordance with the City of Regina Corrective Discipline Policy.

6. REVISION HISTORY:

Date	Name	Purpose of Revision
Nov 2020	Christine Heroux	Updated

7. REFERENCE RELATED POLICIES & STANDARDS

Mobile Device Support Policy
Mobile Device Buyout Policy
Employee Code of Conduct
Email Acceptable Use Policy
Internet Acceptable Use Policy
Password Policy
Privacy Policy
LAFOIP