SECTION:	*CORPORATE INFORMATION TECHNOLOGY*
DEPARTMENT/DIVISION/ SECTION:	*CORPORATE SERVICES / CORPORATE INFORMATION TECHNOLOGY*
SUBJECT:	***MOBILE DEVICE POLICY***

POLICY STATEMENT

It is the policy of The Corporation of the City of Thunder Bay (the City) to ensure the security of mobile devices, including smartphones and tablet computers which access City of Thunder Bay corporate information and/or connect to the corporate network.

PURPOSE

The purpose of the policy is to define standards for allowing access to the City of Thunder Bay corporate information and network from a mobile device. Mobile devices are important tools used by the City of Thunder Bay to achieve business goals but also present a risk to information security. Appropriate measures are required to safeguard against unauthorized access.

DEFINITIONS

When a term set out below appears in the text of this Policy with its initial letters capitalized, the term is intended to have the meaning set out for it in this section. Wherever a term below appears in the text of this Policy in regular case, it is intended to have the meaning ordinarily attributed to it in the English language.

(a) "CIT" or "Corporate Information Technology" refers to a division of the Corporate Services Department within the City of Thunder Bay.

(b) "City" refers to The Corporation of the City of Thunder Bay.

(c) "Corporate Issued" refers to a piece of equipment that was acquired, approved, and provided to an employee by CIT.

(d) "Internet Service Provider" or "ISP" is an organization that provides services for accessing, using, or participating on the internet.

(e) "IT Resources" refers to the City's entire Information Technology infrastructure attached to the corporate network, including software programs, desktops, laptops, smartphones, tablets, peripheral devices, POS (point of sale) devices, email and internet systems, data, information, and other work products installed or created with these tools whether active or archived. This also includes transmission methods and services such as wired and wireless networks.

(f) "Jailbroken" refers to a device that has removed some standard security permissions which provide the user and applications with increased access to the core operating system and increased capacity to bypass security systems.

(g) "Mobile Device" is a piece of portable electronic equipment that is capable of storing corporate data and connecting to the City of Thunder Bay network through a public network (the Internet). Examples of some mobile devices are tablets and smartphones.

(h) "Mobile Device Management" or "MDM" is a software application installed on a mobile device to give the City the ability to manage the device. It allows for setting policies (such as mobile device passcode enforcement), allowing access to an internal network, distribution of applications and having the ability to remotely wipe the device in cases of loss or theft.

(i) "User" refers to all employees, elected officials, students and any other person or entity who use the City's IT Resources with authorization.

CONDITIONS

The following conditions must be adhered to when using Corporate Issued mobile devices. Mobile devices are property of the City and must be authorized models as supplied by the Telecommunications Coordinator in each Department.

1. All Corporately Issued Mobile Devices are the property of the City of Thunder Bay.

2. Mobile devices must have the Mobile Device Management (MDM) application deployed and used by CIT.

3. Mobile devices reported as lost or stolen will attempt to be remotely wiped.

4. Mobile devices which no longer have the default security settings imposed by the manufacturer or have had their default security settings tampered or Jailbroken, will have their IT Resource's access removed.

5. Mobile devices operating system and patches are to be kept current.

6. Mobile devices are not covered under the Backup and Retention Policy for regularly scheduled backups.

USER RESPONSIBILITIES

1. Users must keep the MDM application on their Corporate Issued device. If removed, CIT has the right to disable synchronization of corporate data to the mobile device until the MDM application has been reinstalled by CIT.

2. Mobile devices must be configured with a secure passcode as defined in the MDM. Passcodes must not be shared.

3. If a mobile device is lost, damaged, or stolen, the User is expected to report this to CIT as soon as reasonably possible.

4. The User is responsible for updating appropriate systems and software as needed.

CIT RESPONSIBILITIES

1. CIT's primary responsibility is setting up and troubleshooting issues related to email, calendar, and contacts. At their discretion, CIT may provide support with other aspects such as applications, photos, etc., at their discretion.

2. The CIT Division will make accurate training and education material available to Mobile Device users as needed.

3. Troubleshooting issues and providing support for Users experiencing issues on their Corporate Issued Mobile Device through the Help Desk.

4. CIT Leadership will update related procedures and circulate changes as needed.

5. The Compliance & Risk Specialist, in conjunction with the Director – CIT, will determine what changes will require a review of, and updates to, this policy.

SCOPE

All individuals using mobile devices owned by the City of Thunder Bay that have access to corporate networks, data, and systems, are covered by the items in this policy.

SUPPORTING INFORMATION

Municipal Freedom of Information and Protection of Privacy Act, R.S.O 1990
Records Authority By-Law BL 20-2022
Acceptable Use Policy (03-05-01)
Backup and Retention Policy (XX-XX-XX)
Records Management Policy (03-06-01)
Remote Access Policy (XX-XX-XX)

Approved by City Council on dd/mm/yyyy		
Replacing/Amending/Withdrawn:	X	***Review Date:***
Originating Department:	Corporate Services	
Contact:	Director – Corporate Information Technology	
Departmental Procedural Manual:	N/A	