TOWN OF CALMAR

Standard Operating Procedure

Job/Activity: Mobile Device Management

Duration: on-going during employment

Scope:
The purpose of this Standard Operating Procedure (SOP) is to ensure that all Town issued mobile devices are securely managed, properly configured, inventoried, and used appropriately in accordance with the Town's Computer, Phone & Technology Use Policy and applicable legislation.

This SOP establishes consistent operational practices for the lifecycle management of Town issued mobile devices. It applies to all Town issued mobile devices, including but not limited to:

- Mobile phones,
- Tablets, and
- Laptops.

This SOP applies to employees, contractors, volunteers, and third parties authorized to use Town devices for Town business.

Known Hazards:

Extended period of usage may create strain on body of the user. No devices can be used while operating a motor vehicle, except for a Peace Officer.

Required Equipment and PPE:

Using visual/hearing aid as prescribed by a health professional. Taking breaks from time to time can also mitigate the hazards associated with extended period of using these devices.

Roles & Responsibilities:

Chief Administrative Officer (CAO)
Provides administrative oversight and authority for enforcement of this SOP.

IT Lead (Town of Calmar)
Oversees implementation of this SOP. Acts as the primary Town contact for mobile device management decisions. Coordinates with IT Contracted Services.

IT Contracted Services

Implements and manages Mobile Device Management (MDM) controls. Maintains inventory and configuration standards of devices. Responds to security incidents involving Town devices.

Device Users

Use Town issued devices in accordance with this SOP and applicable Town policies. Protect Town property, data, and credentials. Promptly report issues, loss, or theft.

Device Enrollment & Inventory:

All Town issued mobile devices must be enrolled in the Town's Mobile Device Management (MDM) system prior to being issued to a user.

Devices must be named and registered using the standard nomenclature established by the Town of Calmar.

IT Contracted Services will maintain an accurate and up to date inventory of all Town issued mobile devices, including assigned user, device type, serial number, and status.

Security Controls:

All devices must have a screen lock enabled using a strong password, PIN, or biometric authentication where supported.

Devices must be configured to automatically lock after a reasonable period of inactivity (maximum 5 minutes).

Operating systems and applications must be kept up to date with the latest security patches and updates.

Encryption of Town data must be enabled where supported by the device and operating system.

Jailbreaking or rooting of Town devices is prohibited.

Application & Software Management:

Only applications and software approved by IT Contracted Services or the CAO may be installed on Town issued devices.

Users are prohibited from installing unauthorized applications or software.

IT Contracted Services or the CAO may remotely install, update, restrict, or remove applications as required for security or operational purposes.

Data Protection & Use:

Town data must only be stored on Town approved systems and applications.

Town data must not be transferred to or stored on personal devices, personal cloud storage, or nonapproved platforms.

Confidential or Restricted information must be managed in accordance with applicable Town policies and legislation.

Users must not attempt to bypass security controls or protections implemented on Town devices.

Lost, Stolen, or Compromised Devices:

Lost, stolen, or suspected compromised devices must be reported immediately to IT Contracted Services and the IT Lead.

IT Contracted Services will take appropriate action to protect Town data, including but not limited to:

- Remote locking,
- Remote data wipe, and/or
- Credential revocation.
- Failure to report a lost or stolen device promptly may result in disciplinary action.

Device Return, Replacement & Reassignment:

Town issued devices must be returned to IT Contracted Services or the CAO:

- Upon termination of employment or engagement,
- When a device is replaced or upgraded, or
- When requested by Administration.
- Devices must be returned in reasonable condition, accounting for normal wear and tear.
- IT Contracted Services will securely erase all Town data prior to device reassignment or disposal.

Monitoring & Compliance:

The IT Lead and/or IT Contracted Services may conduct periodic or ad hoc compliance checks of Town issued devices as directed by the CAO.

Monitoring is limited to Town owned devices and is conducted for security, compliance, and operational purposes only.

Users must cooperate with required device updates, inspections, or remediation actions.

Physical Integrity of Devices:

Physical alterations to Town issued devices are prohibited, including but not limited to:

- Stickers,
- Engravings, or
- Personalized skins or cases not issued by the Town.

Devices must retain their original appearance and comply with the Town's Visual Identity standards where applicable.

Protective cases approved or provided by the Town are permitted.

Enforcement:

Failure to comply with this SOP may result in:
- Removal of device access,
- Disciplinary action in accordance with Town administrative policies,
- Termination of employment or engagement,
- Recovery of damaged or lost equipment costs,
- Referral to law enforcement when warranted,

Review & Updates:

This SOP will be reviewed annually or when significant changes occur in technology, risk, or legislation.

Communication:

Internal	External
Communication between IT Lead and CAO will be done via Teams.	Request for support and/or question to the Contracted Services will be done via email and/or their ticketing systems.
Enforcement actions by the CAO will be done in person and via emails.	

This SOP was created on: June 9, 2026

This SOP was last reviewed on: Insert date.

Chief Administrative Officer

Director Corporate Services

Director, Infrastructure and Growth