

SCANNED



Standard Operating Procedure

Job/Activity: Automated System

Duration: on-going during employment

Scope:

The purpose of this Standard Operating Procedure (SOP) is to ensure that all automated or electronic systems used by the Town of Calmar are securely managed, properly configured, monitored, and used in accordance with applicable legislation and Town policies.

This SOP establishes consistent operational practices for automated systems that collect, store, or process information on behalf of the Town.

It applies to all automated systems used by employees, contractors, volunteers, or third parties performing work for the Town.

For clarity, the Town of Calmar does not currently employ artificial intelligence (AI), machine learning, or automated decision-making systems to make decisions that directly affect individuals. The Town currently employs 1 automated system strictly for administrative processing purposes. The system, Great Plains, is used to generate tax notices/invoices and utility invoices. This system operates on predefined rules and does not make discretionary decisions. It is employed to facilitate electronic generation and transmission of information.

The current automated system access is restricted to select employees, protected by password, requires access from specific and limited devices within the Town hall (remote access is not enabled), and the data is contained on a server that is encrypted. The personal data contained in the system is provided by the individual themselves when they subscribe to the electronic billing service. Residents can choose to opt-in or opt-out. Once the invoices are generated, a report is run to detect any anomalies and/or errors.

Known Hazards:

Unauthorized system access, data breaches, data loss, or improper system configuration.

Required Equipment and PPE:

Town-issued computing equipment.

Secure credentials and approved access methods.

Procedure:

Once an automated or electronic system has been approved, all employees must use said system within the framework and for the purpose that it was designed. The system cannot be calibrated or altered without the approval of the CAO. Each new system will have a standalone SOP that will explain in details the step-by-step procedure for accessing, data entering, processing, reporting, and monitoring. For the purpose of developing SOPs, Automated systems include those systems that use machine learning, algorithms, or artificial intelligence (AI).

Users of automated systems may not plagiarize and shall always attribute AI-generated content that is used for work purposes.

Users of automated systems must comply with this SOP and any and all related bylaws, policies, and SOP's of the Town of Calmar when utilizing AI tools for conducting any business for, or on behalf of, the organization.

Users of automated systems are prohibited from inputting data specific to the organization, including confidential or proprietary business information belonging to the organization when using AI tools. This includes but is not limited to copying, pasting, typing, or in any way submitting any form of personal information (e.g., names contact information, addresses, dates of birth, SINs, etc.) about employees, volunteers, and other members of the organization's community into AI tools.

At the current time, Town usage of AI is extremely limited. AI is being used to sort emails, identify actionable items, create summaries, and other similar tasks. AI is not being used in any decision-making processes. Furthermore, it is limited to Copilot, which is embedded in the 365 Premium licenses environment we currently have, which includes security measures and controls to protect the Town's IT environment.

All inputs into AI prompts via text, speech, images, or any other means must be anonymized to avoid disclosing confidential information of the organization.

When employees use AI to assist in the performance of job-related responsibilities, the organization expects them to recognize the limitations of AI they are using, avoid over-reliance on such tools, carefully review output for errors, and remain vigilant to identify potentially erroneous, incomplete, or otherwise problematic outputs. Employees who have concerns with the output of an AI tool should report their concern to their direct supervisor.

No AI user may use AI for personnel decision-making purposes without the express written consent of Human Resources.

Roles & Responsibilities:

Chief Administrative Officer (CAO)

Provides administrative oversight and approval authority for automated systems involving personal information. Ensures Privacy Impact Assessments are completed when required.

IT Lead (Town of Calmar)

Oversees implementation of this SOP. Acts as the primary Town contact for system management decisions and coordinates with IT Contracted Services and the CAO.

IT Contracted Services

Implements and manages automated system controls. Maintains security monitoring and responds to system incidents.

Employees

Report/escalate as soon as possible to the CAO any concern, malfunction, issues, anomalies, or deviation of results in an automated system/process.

Employees must recognize limitations of AI tools, avoid over-reliance, and verify all outputs prior to use.

System Approval & Use:

All automated systems must be approved by the CAO prior to implementation or use.

Role-based access controls must be applied to all systems.

Systems must collect only information necessary for Town operations and be monitored for compliance and security risks.

Systems must include safeguards such as encryption, access controls, monitoring, and documented configurations, including human oversight.

Systems must be monitored for risks including unauthorized access, errors, and emerging privacy concerns. As the Town does not currently use AI decision-making systems, focus remains on data integrity and system reliability.

When systems are decommissioned, data will be securely destroyed or migrated as directed by the CAO.

Enforcement:

Failure to comply with this SOP may result in disciplinary action or removal of system access.

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.	Vendor communication will be via email and/or ticketing systems.

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