Low Code/No Code Development and Maintenance Policy

Ministry of SaskBuilds and Procurement (SBP)
Maintained by: Information Technology Division (ITD)

Issued: May 2026
Next review: May 2027

Purpose

Low code/no code (LC/NC) tools are platforms that allow users to create applications and automations with minimal hand-coding. These tools enable rapid development and deployment, making it an attractive option for government clients looking to streamline processes and improve efficiency.

This policy outlines the rules and guidelines for creating and maintaining automation using LC/NC tools within the Government of Saskatchewan (GOS).

It aims to ensure:

- Secure, efficient, and centralized management of automated processes, particularly those involving sensitive data.
- Compliance with the Freedom of Information and Protection of Privacy Act - while enabling timely and accurate responses to information access requests.
- Security, compliance, business continuity and Intellectual property risks are mitigated.

This policy also serves to foster innovation across ministries by enabling teams to create simple-use functionality while adhering to enterprise standards for security, compliance, and sustainability.

Scope

This policy applies to all employees, contractors, and third parties developing applications using LC/NC platforms like Power Platform for GOS use. There are exceptions to the policy described in Appendix A.

Policy

1. **Managed LC/NC Functionality**
    - Functionality that meets the following criteria will be maintained by SBP ITD:
        - Process sensitive or regulated data (class A/B);
        - Are public facing, accessible by multiple ministries or non-GOS users; and
        - Support core business processes.
    - See Appendix A - Exceptions to the policy.
2. **Development Standards**
    - All LC/NC applications, including those on O365 and Geographic Information Systems platforms, must adhere to security, data governance and compliance standards established by GOS. *Information Security Policies (https://taskroom.saskatchewan.ca/services-and-support/information-technology/it-security/information-security-policies).*
    - Developers are encouraged to collaborate with the information technology (IT) department to ensure proper standards are followed for creating and maintaining personal productivity applications or non-critical applications.
    - Each data set used in LC/NC applications must be classified and used according to Information Classification guidelines.
      Information Classification Guidelines (https://taskroom.saskatchewan.ca/services-and-

support/information-technology/it-security/it-security#)

3. **Monitoring and Compliance**
    - The IT division will monitor all applications to ensure compliance with this policy.
    - Non-compliant applications may be subject to review, remediation, reassignment to ITD for maintenance, or decommissioning.

Exceptions

See Appendix A: Exceptions to the policy.

Process/Guidelines/Information for LC/NC functionality within Power Platform

ITD is committed to supporting GOS by creating and maintaining LC/NC automation solutions using Power Platform upon request. These solutions will be designed in collaboration with requesters to ensure they meet business requirements while ensuring consistent quality, reliable performance and proper documentation, enabling efficient and sustainable automation that aligns with ministry goals.

This service can be requested by submitting a Power Platform request through ServiceNow. Once received, the team will assess the request for fit with Power Platform based on the functionality needed, the scope of the request and the need for further assessment through IT Governance bodies like Innovation Tables etc.

If deemed a fit, a quote will be provided and the build will follow. Ministries will be responsible for testing the functionality and signing off on deployment.

All ministries with one or more Power Platform applications are encouraged to provide a representative to join the Power Platform working group. This group will be led by the ITD Power Platform Administrator and will convene periodically to discuss relevant updates to the service and platform as well as serve as a forum to discuss best practices for Power Platform and collaborate on innovative ways to use the tools.

Authority

Information Security Policies (https://taskroom.saskatchewan.ca/services-and-support/information-technology/it-security/information-security-policies).

Information Classification Guidelines (https://taskroom.saskatchewan.ca/services-and-support/information-technology/it-security/it-security#).

Accountability

ITD is responsible for monitoring the applications to ensure they meet security standards, identifying any non-compliant functionality and initiating communication with the creator to begin remediation as appropriate. The creator is responsible for investigating identified issues, implementing corrective actions to ensure compliance, and collaborating with ITD throughout the remediation process.

Non-compliance

Failure to comply with this policy may result in the removal of access to LC/NC tools and environments, decommissioning of functionality and other disciplinary actions as deemed necessary by GOS.

Related Documents/Appendices

Appendix A: Exceptions to the policy.

Contact Information

For more information regarding this policy, please contact:

Mike Roney
ITD Director, Digital Platforms and Services
Mobile: 306-510-8153

Appendix A – Exceptions to the policy

Document management and collaboration on SharePoint is excluded from this policy, provided it adheres to the Government of Saskatchewan (GOS) security and data management guidelines.

Geographic Information Systems (GIS) Applications: Applications primarily developed for GIS, including mapping and spatial analysis tools, are excluded, provided they align with GOS standards for GIS platforms.

Reporting and analytics within an enterprise platform that does not take data from multiple systems, generate new data and has no public facing component are excluded.

Power Apps and flows created by vendors when deployed as part of a Dynamics 365 solution are excluded.

Survey tools (ex. MS Forms, Alchemer): Creating surveys using office tools - users are still expected to adhere to data privacy and security standards when collecting, storing, and sharing survey data.