Acceptable Use of Third-Party Natural Language Generators Directive

Cybersecurity Services Branch and Privacy, Policy and Governance Branch
Technology and Innovation

Version: 1.0

Approved by: ARMC/ADM IMT	**Owners:** ADM, Cybersecurity Services Division, Technology and Innovation ADM, Innovation, Privacy and Policy Division, Technology and Innovation	
Approval Date: 13 October 2023	**Last Reviewed:** 13 October 2023	**Review Date:** 13 October 2025
Contact: cybersecurity@gov.ab.ca Sa.InformationManagement@gov.ab.ca	**Policy Instrument type:** Directive	

Directive Statement

This directive details the obligations for, and requirements of, all Government of Alberta (GoA) staff (which includes, but is not limited to, contractors, volunteers, appointees, interns, and students working with a public body) when using third-party Natural Language Generators (NLGs).

NOTE: For information on NLG use cases that are prohibited, permitted with authorization, and permitted without authorization, please consult the Use of Third-Party Natural Language Generators Guideline.

Authority

This directive is issued under the authority of the *Government Organization Act* and the Records Management Regulation.

Application

This directive applies to all GoA departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards, and commissions as defined in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Agencies, boards, and commissions that are not contained within Schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this directive.

Information that is subject to the *Health Information Act* (HIA) must be managed in compliance with the HIA; the HIA and associated policy instruments are paramount to this directive.

Definitions

Natural Language Generators: Natural Language Generators (sometimes referred to as "Natural Language Processors") are computer programs that use linguistic and/or non-linguistic representations of information (such as large language models) to generate coherent and contextually appropriate human-like outputs in response to a human-provided input. Common examples of third-party Natural Language Generators include (but are not limited to) ChatGPT, Bard, and LLaMA.

Personal information: means recorded information about an identifiable individual, including (but not limited to) age, name, income, opinions, biometric information, and ethnicity. For a comprehensive list of content considered personal information—and the rules relating to when and how personal information can be collected, used, accessed, disclosed, and otherwise managed—please refer to the *Freedom of Information and Protection of Privacy Act* (FOIP Act).

Third-party - includes external parties and persons outside the direct reporting structure of the Information Controller or Information Custodian (e.g., an individual, a business or organization, personnel from another branch of government, or another level of government). Third-party also include vendors, service delivery agents, businesses, and citizens.

Directive Specification

General Usage Requirements

1. The GoA's information is legally the property of the Crown in right of Alberta, with some exceptions (e.g., licensed intellectual property).

1.1 Section 16(2) of the Code of conduct and ethics for the Public Service of Alberta states that GoA staff have "(t)he responsibility for maintaining the confidentiality of information or documents includes the responsibility for ensuring that such information or documents are not directly or indirectly made available to unauthorized persons."

2. Only publicly accessible content (including, but not limited to, reports, datasets, and code) may be input, disclosed, or otherwise provided to a third-party NLG—if the content is not already accessible to the general public, it may not be used.
3. Personal information in the custody and/or under the control of the GoA (e.g., staff personal information, client personal information, etc.) must not be input, disclosed, or otherwise provided to a third-party NLG.
   3.1 Staff are responsible for ensuring alignment with, and adherence to, legislated obligations (e.g., the FOIP Act, Records Management Regulation) when collecting, using, disclosing, destroying or otherwise managing personal information.
      3.1.1 Training regarding FOIP Act obligations is available through 1GX.
      3.1.2 For more information regarding the management of personal information and legislated obligations under the FOIP Act, please contact Privacy Services.
4. GoA staff are accountable and responsible for validating, verifying, and otherwise ensuring the accuracy of any outputs provided by a third-party NLG.
   4.1 Third-party NLG outputs must be clearly cited as NLG outputs when used verbatim (e.g., a disclaimer stating "this material was produced by ChatGPT on MM DD YYYY").
   4.2 Depending on their content and the context within which they were created, third-party NLG outputs generated in response to GoA staff inputs may be classified as either official or transitory records. Please refer to the Official and Transitory Records Directive for more information.
      4.2.1 All records, whether official or transitory, are subject to the FOIP Act, and may be responsive to information access requests and/or litigation.

Business Process Integration Requirements

1. In accordance with section 2.4.8 of the Information Security Management Directives, "(s)oftware installation on GoA managed devices must follow an approved and documented process." No individual installation, downloading, or other implementation of third-party NLGs shall occur on any GoA managed device without such an approved and documented process.
2. While this directive enables ad hoc and informal use of third-party NLGs, formal integration of third-party NLGs into business area processes (e.g., pre-drafting responses to routine queries from external stakeholders) requires completion of a Security and Threat Risk Assessment (STRA) in collaboration with Cybersecurity.
   2.1 The STRA will determine access and content management requirements (e.g., requiring use of a GoA email address for account creation, enabling NLG use in scenarios that may fall outside the parameters of this directive, etc.).
   2.2 The STRA may require the completion of an assessment of privacy risk in collaboration with Privacy Services.
   2.3 Business areas should also consult with legal counsel and/or the appropriate content management subject matter experts.

Compliance

Consequences of non-compliance with this directive could result in: the loss of content; breach of confidentiality; breach of privileged information; significant impact to GoA's proprietary rights; damage to GoA's reputation; exposure of Albertans to harm; and/or incurrence of unnecessary costs (including, but not limited to, inability to respond appropriately to a claim in court).

Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made by the Innovation, Privacy and Policy Division, Corporate Internal Audit Services, Cybersecurity, Office of the Information and Privacy Commissioner, Office of the Auditor General and/or Public Service Commission, and
- legislated disciplinary action (i.e., *Public Service Act*) may be taken.

Non-compliance or violation of this directive must be brought to the immediate attention of the Cybersecurity Division and/or Privacy Services; these business areas will work with the appropriate department management to ensure that the problem is resolved, and necessary steps are taken to eliminate potential future violations.

References and Supporting Resources

- Acceptable Use of GoA IT Assets Directive
- Information Controller and Information Custodian Directive
- Code of conduct and ethics for the Public Service of Alberta
- Data and Information Security Classification Standard
- Use of Third-Party Natural Language Generators Guideline

Contact

Area	Contact
Content Management	Sa.InformationManagement@gov.ab.ca
Cybersecurity	cybersecurity@gov.ab.ca
Privacy Services	privacy@gov.ab.ca