Application Hosting Policy Implementation Notice

Application Hosting Policy Implementation Notice

From: <u>Treasury Board of Canada Secretariat</u>

On this page

1. Purpose

The purpose of this Policy Implementation Notice (PIN) is to provide direction to federal institutions involved in the selection, procurement and management of application hosting services on their responsibilities regarding application hosting in accordance with the *2024 Application Hosting Strategy* and applicable Treasury Board of Canada Secretariat (TBS) policy instruments.

2. Effective date

This PIN takes effect on October 4, 2024. This PIN is to be reviewed and updated as required.

3. Authority

This PIN supports subsections 4.1.1.1, 4.4.1.1, 4.6.1.1 and 5.2.1 of the _Policy on Service and Digital_.

Additionally, all actions relating to the PIN must comply with Appendix F: Standard on Enterprise Information Technology Service Usage Restrictions of the _Directive on Service and Digital_ and subsection 3.2 of the _Application Hosting Considerations and Restrictions_ provisions.

All exceptions are to be assessed through the Government of Canada (GC) Enterprise Architecture Review Board (EARB).

4. Application

This PIN applies to all federal institutions described in section 6 of the _Policy on Service and Digital_.

Federal institutions not subject to the _Policy on Service and Digital_ are encouraged to adopt this PIN as good practice.

5. Context

The strategy was developed to support the GC in having cost-effective application hosting solutions that enhance operational efficiency, improve cyber security, develop a digital workforce, and deliver exceptional value to Canadians. This PIN supports federal institutions in putting the strategy into action and ensures that care and consideration are taken at every step of the application life cycle.

6. Direction

> ▶ In this section

When application hosting needs (new or migration) arise, federal institutions are required to collaborate with TBS and Shared Services Canada (SSC) to make sure that efficient and effective solutions are implemented.

6.1 Planning application hosting requests

Federal institutions are responsible for:

- **Conducting continuous analysis of their application portfolios:** Reviewing application portfolios continuously, identifying opportunities to address technical risk, technical debt and security risks, and aligning investments with high business value applications. Institutions subject to the GC Application Portfolio Management (APM) process must provide regular updates.

- **Identifying business needs:** Identifying the essential requirements and conditions to meet the operational objectives of the application hosting request linked to an investment in the GC Enterprise Portfolio Management system or with an internal reference number.

- **Identifying assets:** Tagging assets to the maximum extent possible so that all resources deployed can be associated with the application identification number originating from the GC APM inventory. Expenses associated with information technology assets and programs must be allocated to the appropriate program funding source for financial accountability and resource optimization purposes.

- **Decommissioning:** Retiring applications that are no longer providing value to service delivery to reduce costs and risk to the GC and migrating the data.

- **Designing and experimenting:** Evaluating different options to solve a business problem or opportunity, at which point application hosting needs will be considered.

- **Modernizing:** Making sure that applications:
    - are sustainable
    - have been modernized to the extent possible and in alignment with business value
    - are ready to be hosted in accordance with Appendix H: Standard on At-Risk Information Technology of the *Directive on Service and Digital*

- **Aligning to enterprise:** Adopting common solutions where possible to reduce duplication of effort, costs and future maintenance complexity.

- **Determining costing and source of funds:** Identifying a source of funds commensurate with the estimated cost.

6.1.1 Departmental Architecture Review Board

Before submitting an application request, federal institutions must receive approval from their Departmental Architecture Review Board on all application hosting initiatives as required under subsection 4.1.1.1 of the *Directive on Service and Digital*.

6.2 Submitting application hosting requests

6.2.1 GC Hosting Service Portal

Federal institutions (referred to as applicants) must use the GC Hosting Services Portal to submit application hosting requests to SSC.

As part of the hosting intake submission process, applicants must use the Application Hosting Selection Tool. The tool will assess the input and identify a preferred hosting location and hosting intake process to be followed. TBS and SSC will then review the results of the assessment and provide a decision to the applicant.

6.2.2 Exceptions to use of the selection tool

In exceptional cases where the Application Hosting Selection Tool is not appropriate for assessing the submission, the GC EARB could consider an exception to the tool's use.

6.3 GC EARB evaluation

6.3.1 Review of decision

For all application hosting decisions, if the applicant's chief information officer (CIO) or head of information technology disagrees with the decision, the CIO or head of information technology may request that their case be brought to GC EARB for review. GC EARB will determine whether a review is warranted based on considerations brought forward by the applicant. If a review is required, GC EARB will evaluate the hosting request against the new considerations and existing criteria and make a decision about how and where to host the application.

6.3.2 Additional GC EARB cases

Subsection 4.1.1.2 of the *Directive on Service and Digital* establishes when a digital initiative must be brought to GC EARB. When applicable business solution architectures are brought to GC EARB beyond the conceptual architecture phase, an official application hosting decision is required as referenced in subsection 6.2.1 of this PIN.

6.4 Service delivery data

To support informed and evidence-based decision-making, federal institutions are required to provide SSC with:

- clear and detailed service requirements
- accurate and timely responses
- collaboration and partnership

Beginning no later than April 1, 2025, SSC will provide both aggregate and institution-specific service performance data to the Office of Chief Information Officer of Canada at least once a year and within the first 90 days of the fiscal year.

6.5 Monitoring

On an annual and regular basis, SSC will monitor and report on federal institutions' implementation of application hosting solutions to the Office of Chief Information Officer of Canada. Monitoring and reporting should initially focus on applications processed through the Application Hosting Selection Tool, with legacy applications as a future target for reporting.

7. Compliance

TBS will monitor institutional progress and engage responsible senior officials as necessary and appropriate to validate the successful adoption of and compliance with the direction specified above.

For an outline of the consequences of non-compliance, refer to Appendix C: Consequences for Institutions and Appendix D: Consequences for Individuals of the _Framework for Management of Compliance_.

8. Enquiries

Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries for information at publicenquiries-demandesderenseignement@tbs-sct.gc.ca about this implementation notice.

Employees of federal institutions may contact moderntechnologies/technologiesmodernes@tbs-sct.gc.ca for information about this implementation notice.

9. References

Additional information may be found in the following resources:

9.1 Legislation

- *Financial Administration Act*
- *Shared Services Canada Act*

9.2 Related policy instruments

- *Policy on Service and Digital*
- *Directive on Service and Digital*
- Standard on Enterprise Information Technology Service Usage Restrictions
- Standard on At-Risk Information Technology
- Order in Council 2015-1071
- *Framework for the Management of Compliance*

9.3 Other references

- *2024 Application Hosting Strategy*
- *Application Hosting Considerations and Restrictions*
- *Government of Canada Cloud Guardrails*

Date modified:

2024-10-22