

Update on embedding privacy and security by design principles into the City's procurement process

Date: October 16, 2023

To: General Government Committee

From: Chief Procurement Officer and Chief Information Security Officer

Wards: All

SUMMARY

Per City Council's directive [2021.AU8.8](#) (Item 13), the Chief Procurement Officer, the Chief Information Security Officer, in consultation with the City Clerk and the City Solicitor, updated the City's procurement process for technology related initiatives. This has been achieved by deploying a set of privacy and cyber security requirements in the procurement process that ensure suppliers deliver products and services consistent with industry best practices.

By embedding privacy and cyber requirements into the early stages of procurement, the City has reinforced its commitment to the "security by design" strategy. This strategy emphasizes the integration of modern cyber security and risk management practices into the procurement, design, and development of IT systems.

These developments to the City's procurement process have strengthened cross-divisional collaboration, communication, and helped shape a unified vision that modernizes the City's cyber security posture and safeguards the City's sensitive information and systems.

RECOMMENDATIONS

The Chief Procurement Officer, the Chief Information Security Officer, in consultation with the City Clerk and the City Solicitor, recommend that:

1. General Government Committee receive this report for information.

FINANCIAL IMPACT

There are no financial impacts associated with this report.

The Interim Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial implications as identified in the Financial Impact section.

DECISION HISTORY

On April 7 and 8, 2021, City Council adopted the report, [AU8.8, Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System](#). The report included a request for the Chief Procurement Officer, in consultation with the Chief Information Security Officer and the City Clerk, to report to the General Government Committee on how to embed privacy and security by design principles and mandatory privacy and cyber security requirements into the City's current procurement process and a governance process to manage exceptions.

COMMENTS

Three procurement processes have been updated to include mandatory privacy and cyber security requirements:

1. Request for Proposal;
2. Request for Quotation; and
3. Non-Competitive Procurement with a value of over \$50,000.

The following requirements have been embedded into the procurement and implementation lifecycle of technology systems:

- Baseline privacy and cyber security requirements questionnaire:
 - A baseline privacy and cyber security questionnaire must be completed by all suppliers during the initial phase of technology procurements. Suppliers that do not achieve a minimum baseline score are excluded from the procurement.
- Comprehensive privacy and cyber security risk assessments:
 - Once a supplier has been identified, the supplier will undergo comprehensive privacy and cyber security risk assessments. Conducting assessments in this manner proactively identifies vulnerabilities, ensures that regulatory requirements are met, and protects the City's sensitive data and its systems.
- Updated terms and conditions for confidentiality, privacy, cyber security, and access to information in agreements:
 - Strong privacy and cyber security terms and conditions in agreements are essential to protect the City's information, reduce legal risk, and mitigate threats while ensuring supplier accountability. A set of standardized cyber security and privacy terms and conditions has been developed which can be drawn on and appended to technology agreements, as needed. These terms and conditions require suppliers to maintain clear cyber incident response procedures, address various aspects of data handling, and to mitigate the City's financial implications in the event of a privacy or cyber breach.

Collectively, these requirements will bolster the City's privacy and cyber security defenses against ever-evolving threats, and represent the City's commitment to protecting sensitive data and promoting the reliability of the City's technology supply chain.

CONTACT

Hillary Keirstead, Manager Policy & Program Planning, Purchasing and Materials Management, 416-392-0643, Hillary.Keirstead@toronto.ca

Andree Noel, Deputy Chief Information Security Officer, Office of the Chief Information Security Officer, 416-392-8699, Andree.Noel@toronto.ca

SIGNATURE

Geneviève Sharkey
Chief Procurement Officer

Maneesh Agnihotri
Chief Information Security Officer