TORONTO

# REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENTS

# Status of Audit Recommendations and Key Cybersecurity Risks

**Date:** March 8, 2022
**To:** General Government and Licensing Committee
**From:** Chief Information Security Officer
**Wards:** All

## REASON FOR CONFIDENTIAL INFORMATION

The attachments to this report involve the security of property belonging to the City of Toronto.

## SUMMARY

The purpose of this report is to present the biannual report to the General Government and Licensing Committee on the City-wide cyber security program, including an update on the cyber security confirmation program underway with City divisions, agencies and corporations, and to report back on the City's response to the Log4j cybersecurity threat.

This report contains three confidential attachments from the Office of the Chief Information Security Officer:

Attachment 1 The City's Cyber Health describes the City's cyber health as seen from three lenses: cyber resilience, cyber maturity, and cyber awareness.

Further, these attachments provide details on:

A. Overall cyber health of the organization, the progress made in the past six month and the benefits/efficiencies achieved as a result of the Cyber program implementation, including embedding "cybersecurity by design" principles to support the City's modernization efforts;

B. The status of all outstanding audit recommendations that have not been implemented to date, including any increase to the City's cybersecurity risk profile

C. Additional supports required to address cybersecurity risks in an expedited manner.

Subsequent reports to the GGLC will include updates on the following:

- Projects, initiatives, procurement, and operations where cybersecurity requirements or directives were not included in the process

The attachments also include highlights of the progress the Office of the Chief Information Security Officer (CISO) has made, in collaboration with Technology Services Division (TSD) and the City's critical infrastructure Divisions, in embedding cyber security risk management practices in their projects, initiatives, procurement, and operations.

Attachment 2 Status of the Confirmation Program describes the status of the confirmation program in the first quarter of 2022, including rates of compliance, remediation plans and strategies to reduce risk and ensure corporate compliance.

Attachment 3 LOG4J Update describes the situation, sequence of action, incident response and reporting steps taken and the current status of the "Log4j" threat to the City, its agencies, boards and commissions.

## RECOMMENDATIONS

The Chief Information Security Officer recommends that:

1. City Council direct that Confidential Attachments 1, 2 & 3 remain confidential in their entirety, as they involve the security of property belonging to the City of Toronto.

## FINANCIAL IMPACT

Any costs associated with addressing the details on all 3 confidential attachments have been included in the 2022 operating budget.

## DECISION HISTORY

On December 15, 16 and 17, 2021, City Council request the Chief Information and Security Officer to report to the March 22, 2022 meeting of the General Government and Licensing Committee on the matters identified in the confidential attachment to motion 1 by Councillor Stephen Holyday.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.GL27.29

On November 9, 10 and 12, 2021, City Council request the City Manager to report to the next meeting of the Audit Committee on the ongoing governance structure that will be in place to effectively identify, plan for and mitigate cybersecurity risks across the City of Toronto, including all City divisions, agencies and corporations, and the governance framework to ensure that City divisions, agencies and corporations are effectively managing their cybersecurity risks and responding as new risks arise.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU10.4

On April 7 and 8, 2021, City Council requested the Chief Information Security Officer to report to the General Government and Licensing Committee on a biannual basis regarding the City-wide cybersecurity program,
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.5

Other cyber security related reports and City Council decisions include:

Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2016.AU5.10

Information Technology Vulnerability Assessment and Penetration Testing - Wrap-up of Phase I and Phase II
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2017.AU8.6

Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2019.AU4.1

Cyber Safety - Critical Infrastructure Systems: Toronto Water SCADA System
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2020.AU5.6

Cybersecurity Incidents at the City and its Agencies and Corporations: Integrated Incident Response Plan is Needed
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.9

Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.8

## COMMENTS

This report contains 3 confidential attachments that provide detail on the overall cyber security health of the City.

## CONTACT

Abiodun Morolari, Chief Information Security Officer, 416-396-4693,
Abiodun.Morolari@toronto.ca

Dalton M'Cormack, Manager Office of the CISO, 416-392-3404,
Dalton.MCormack@toronto.ca

## SIGNATURE

Abiodun Morolari
Chief Information Security Officer

## ATTACHMENTS

Confidential Attachment 1 - The City's Cyber Health

Confidential Attachment 2 - Status of the Confirmation Program

Confidential Attachment 3 - Log4J Update