

## **Status Update on the Information Technology Disaster Recovery Program**

**Date:** November 16, 2023

**To:** Audit Committee

**From:** Chief Technology Officer, Chief Information Security Officer, and the Executive Director, Toronto Emergency Management

**Wards:** All

### **REASON FOR CONFIDENTIAL INFORMATION**

---

The attachment to this report involves the security of property belonging to the City of Toronto.

### **SUMMARY**

---

This report provides a status update on the Information Technology (IT) Disaster Recovery Plan pursuant to a City Council decision under [AU13.9 - Status Update of the IT Disaster Recovery Plan](#) on July 19, 2022. In this motion, the City Council has requested the Chief Technology Officer, in co-ordination with the Chief Information Security Officer and the Executive Director, Toronto Emergency Management to report to the Audit Committee in the third quarter of 2023 on the status of the IT disaster recovery plan from each City of Toronto division, agency and corporation including the status update for the Enterprise IT Disaster Recovery Program, business continuity, and cyber major incident response.

The City of Toronto creates and manages large volumes of information systems and data. The impact of data loss and outage of information systems due to hardware failure, human error, hacking, malware, or a natural disaster could be significant. Should such an event occur, an IT Disaster Recovery Plan is designed to assist in the recovery efforts while protecting IT assets and ensuring business continuity.

This report provides information on the approach undertaken by Technology Services Division (TSD), in collaboration with Toronto Emergency Management (TEM) and the Office of the Chief Information Security Officer (CISO), in gathering input from the City's different divisional IT units, agencies and corporations about the current state of their

plans relating to IT disaster recovery, business continuity, and cyber incident response. Additionally, this report provides information on the status of the Enterprise IT Disaster Recovery Program led by TSD, which aims to improve the overall disaster recovery capability of the City of Toronto's mission-critical applications and foundational IT systems in the face of unforeseen events such as natural disasters, major cyber-attacks and/or hardware failures. An update is given on the City's business continuity and cyber major incident response plan. The analysis and details of this update are provided in Confidential Attachment #1.

## **RECOMMENDATIONS**

---

The Chief Technology Officer, the Chief Information Security Officer and the Executive Director, Toronto Emergency Management recommend that:

1. City Council direct that the Confidential Attachment 1 to this report remain confidential in its entirety, as it involves the security of property of the City.

## **FINANCIAL IMPACT**

---

The status update contained in this report does not have any financial impact. However, the implementation of the Enterprise IT Disaster Recovery Program referred to in this report may result in financial implications which will be presented in future budget requests for consideration and approval.

## **DECISION HISTORY**

---

On July 11, 2022, the Audit Committee requested the Chief Technology Officer, in coordination with the Chief Information Security Officer and the Executive Director, Toronto Emergency Management to report to the Audit Committee in the third quarter of 2023 on the status of the Information Technology Disaster Recovery Plan from each City of Toronto division, agency and corporation, including the status update for City of Toronto's Corporate Technology Services Disaster Recovery Plan, business continuity, and cyber major incident. This was considered by the City Council on July 19, 2022 under [AU13.9 - Status Update of the IT Disaster Recovery Plan](#).

On November 2, 2021, the Audit Committee requested the City Manager to report to the Audit Committee with information from each City of Toronto division, agency and corporation on their Information Technology Disaster Recovery Plan should the City's systems, technology, communications, or backups be made unavailable. The Chief Technology Officer was also requested to report to the Audit Committee with an update on the status of City of Toronto's Corporate Technology Services Disaster Recovery Plan, including implementation, testing and a full project plan for any outstanding work. <http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU10.8>

The aforementioned Council motions are both anchored on audit report [AU 7.3 - Disaster Recovery Planning for City Computer Facilities](#), which provided a snapshot of what the City has accomplished and what work remains to be completed in preparing contingency plans in the event of a disaster disabling City technology services. This audit report was adopted by the City Council on May 26, 2008.

## COMMENTS

---

### Section 1: City-wide assessment of IT disaster recovery plans

This section provides an update to [2022.AU13.9](#), including an overview on the method in gathering input from City divisions, agencies, and corporations on the status of their disaster recovery plans. This assessment aims to collect insights to provide a foundation for future actions in recovering IT systems in the event of a disaster.

For the purpose of this report, City divisions, agencies and corporations are collectively referred as 'entities'.

#### *Methodology*

The approach in collecting insights on the current state of IT disaster recovery plans at the City involved the use of a questionnaire administered to 31 entities (i.e. 14 divisions, 12 agencies and, 5 corporations), as well as business units within the Technology Service Division (TSD). The list of entities who have been engaged in this exercise are provided in *Public Attachment 1: Distribution List for the IT Disaster Recovery Questionnaire*.

The questionnaire was developed by TSD, in collaboration with TEM and Office of the CISO, to gain a comprehensive view on disaster recovery, business continuity and cyber major incident response across the 31 entities. TSD provided guidance to these entities in completing the questionnaire, as required.

The questionnaire was composed of 25 questions, across 8 different sections. These sections include the following:

- Information Technology Disaster Recovery Plan
- Information Systems / Application and Data Recovery
- Foundational IT Core Technology Recovery
- Back-ups
- Disaster Recovery Testing
- IT Disaster Recovery Communication Procedure and Contact Information
- Business Continuity Plan
- Cyber Major Incident Response Plan

#### *Respondents*

Of the 31 entities, 28 responded to the questionnaire and 3 of the 31 were deemed out of scope. The 28 respondents formed the basis for analysis in this report. Feedback

from business units within TSD was also factored in the overall response analysis for this questionnaire. The breakdown of entities is shown in Table 1 below.

Table 1: Responses Received from Entities for the City-wide Assessment

Entity	No. of entities who received questionnaire	No. of entities who responded to the questionnaire	No. of entities who did not respond to the questionnaire	No. of entities out of scope
Divisions	14	14	0	0
Agencies	12	10	0	2
Corporations	5	4	0	1
Total	31	28	0	3

The 31 entities are listed in *Public Attachment 1: Distribution List for the IT Disaster Recovery Questionnaire*.

The analysis report from the 28 entities who responded to the questionnaire is provided in *Confidential Attachment 1 (Section 1: Analysis of City-wide Assessment of IT Disaster Recovery Plans)*.

**Section 2: Enterprise IT disaster recovery program**

Information Technology (IT) has become an integral part of managing and delivering services to internal and external stakeholders of the City of Toronto. Given its complexity, IT systems are prone to failure and disasters can strike at any time, causing significant disruption to systems and services provided by the City. In the event of such an IT disaster, the City's ability to quickly recover and restore its systems and services is critical to minimizing the impact to citizens and maintaining their trust. Therefore, having an Enterprise-wide IT Disaster Recovery Program is an essential strategy to reduce corporate risks at the City.

TSD, in collaboration with TEM and Office of the CISO, leads the Enterprise-wide IT Disaster Recovery Program anchored on a strategy that is aligned with the objectives of the City's Business Continuity Management Program and Cyber Incident Response Plan.

Details of the Enterprise IT Disaster Recovery Program are provided in *Confidential Attachment #1 (Section 2: The Enterprise IT Disaster Recovery Program, Business Continuity, and Cyber Incident Response Plan)*.

## CONTACT

---

Mala Gautam, Manager Strategy & Compliance, Technology Services Division,  
416-338-2956, [Mala.Gautam@toronto.ca](mailto:Mala.Gautam@toronto.ca)

## SIGNATURE

---

Sonia Brar  
Chief Technology Officer

Maneesh Agnihotri  
Chief Information Security Officer

Joanna Beaven-Desjardins  
Executive Director, Toronto Emergency Management

## ATTACHMENTS

---

**Confidential Attachment 1:** Status Update on the IT Disaster Recovery Program, Business Continuity, and Cyber Incident Response

**Public Attachment 1:** Distribution List for the IT Disaster Recovery Questionnaire