REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Status update of the IT Disaster Recovery Plan

Date: June 24, 2022
To: Audit Committee
From: Chief Technology Officer
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 status update of IT Disaster Recovery Plan pursuant to a City Council decision under AU10.8 - Status of Audit Recommendations for the Technology Services Division at its meeting on November 9, 2021. At this meeting, City Council requested the City Manager to report to the Audit Committee in the second quarter of 2022 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. In that meeting, City Council also requested the Chief Technology Officer to report to the Q2 2022 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.

The City creates and manages large volumes of electronic information or data. The impact of data loss or corruption of data from hardware failure, human error, hacking, malware, or a natural disaster could be significant. In such a case, a Technology Disaster Recovery Plan is designed to assist an organization in executing recovery processes in response to a disaster to protect business IT infrastructure and promote recovery.

The Technology Services Division (TSD) has collaborated with multiple Divisions, Agencies and Corporations to gather inputs related to the status of their IT Disaster Recovery Plan should the City's systems, technology, communications, or backups be

made unavailable. This information is documented in 'Section 1: City-wide assessment of Information Technology Disaster Recovery Plans' of this report and analysis is provided in Confidential Attachment # 1 - Status Update of the IT Disaster Recovery Plan.

'Section 2 - TSD Disaster Recovery Plan' of this report details the status of the Technology Services Division's Disaster Recovery Plan, including implementation, testing and a full project plan for outstanding work that will highlight the road map for the transition from current state to the future state, based on best practices that have been identified by the project team. The analysis and details of implementation plan are provided in Confidential Attachment # 1.

RECOMMENDATIONS

The Chief Technology Officer recommends that:

1. City Council direct that the confidential information contained in Confidential Attachment # 1 remain confidential in its entirety, as it involves the security of the property of the City

FINANCIAL IMPACT

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

The Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial impact information.

DECISION HISTORY

On November 2, 2021, 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. Also, the Chief Technology Officer was 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

On May 26, 2008, City Council adopted audit report AU 7.3 - Disaster Recovery Panning for City Computer Facilities. The report 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 infrastructure.

COMMENTS

Until recently, most IT Disaster Recovery Plans focused on in-house hosted systems, which are hosted in one of the City's data centres. In the current landscape, the complexity of computing is increased by the introduction of cloud-based services, which are delivered on demand to companies and customers over the internet.

Section 1: City-wide assessment of Information Technology Disaster Recovery Plans

This section provides methodology used to consolidate inputs from various Divisions, Agencies and Corporations. For this report, Divisions, Agencies & Corporations are together referred as Entities. The purpose of this assessment was to assess the Disaster Recovery status amongst all entities. This assessment will guide future actions to be taken to recover IT systems in case of an unforeseen situation.

Methodology of City-wide assessment

To ensure information of the current state was gathered, TSD, in consultation with Office of CISO, prepared a confirmation program and distributed to 14 City divisions with responsibilities for divisional IT teams, 12 Agencies and 5 Corporations: for a total 31 entities. TSD guided the entities to complete the questionnaire, as required. All business units within Technology Services Division (TSD) also completed the questionnaire. All these entities are listed in Attachment 1: Distribution list for the questionnaire.

The questionnaire was designed in collaboration with the Office of Chief Information Security Officer (CISO) to ensure that all aspects of disaster recovery are documented. The questionnaire included information gathering on following aspects of disaster recovery:

- Information Technology Disaster Recovery Plan
- Information Systems/Applications and Databases Recovery
- Foundational IT Core Technology Recovery
- Data Backups - such as tape, hard disk, remote back up services etc.
- Disaster Recovery Testing
- IT Disaster Recovery Communication Plan and Contact Information

Results of City-wide assessment

Out of the total 31 entities, responses from 28 entities were received for analysis. TSD has not been included in the list of 31 entities and the responses submitted by TSD are captured in Confidential Attachment # 1. The responses received from the 28 entities were analyzed by TSD and the resulting analysis is provided in Confidential Attachment # 1. The number of responding entities is shown in Table 1 below.

Table 1: Result of City-wide assessment

Entity	# entities who received questionnaire	# entities who responded to the questionnaire	# entities who did not responded to the questionnaire	# entities out of scope
Divisions	14	14	0	0
Agencies	12	10	0	2
Corporations	5	4	0	1
Total	31	28	0	3

These entities are listed in Attachment 1: Distribution list for the questionnaire

The details of analysis are provided in Section 1: Analysis of City-wide Assessment of IT Disaster Recovery Plans of Confidential Attachment # 1.

Section 2 - TSD Disaster Recovery Plan

This section responds to the update about the Corporate Technology Services Disaster Recovery Plan. The City’s technology landscape is proceeding through modernization and transformation aligned to City's technology strategy, some of which are driven by the Cloud First strategy and the Data Centre Modernization Program. As appropriate the Cloud First strategy would require transitioning any new applications and migrating existing applications and IT services to the public cloud. TSD's modernized Data Centre ensures on-premise infrastructure will support business continuity plans.

The details of analysis and implementation plan are provided in Section 2: TSD Disaster Recovery Plan of Confidential Attachment # 1.

CONTACT

Mala Gautam, Manager Strategy & Compliance, 416-338-2956,
Mala.Gautam@toronto.ca

Lin Zhu, Deputy Chief Technology Officer, 416-338-7535,
Lin.Zhu@toronto.ca

SIGNATURE

Lawrence Eta
Chief Technology Officer

ATTACHMENTS

Attachment 1 - Distribution list for the questionnaire
Confidential Attachment # 1 - Status Update of the IT Disaster Recovery Plan