SECTION:	*CORPORATE INFORMATION TECHNOLOGY*
DEPARTMENT/DIVISION:	CORPORATE SERVICES / CORPORATE INFORMATION TECHNOLOGY
SUBJECT:	**DATA BACKUP AND RECOVERY POLICY**

POLICY STATEMENT

It is the policy of The Corporation of the City of Thunder Bay (the City) to provide an effective backup and recovery plan for data stored within the Corporate DataCentre. All electronic information managed by the Corporate Information Technology (CIT) Division is copied to a secure storage media on a regular basis, for disaster or data recovery. This policy outlines the creation and retention schedules of backups to limit potential data losses.

PURPOSE

The purpose of this policy is to outline the City of Thunder Bay's data backup and file and system level recovery standards for electronic data that is under the care and control of CIT. Data backup mechanisms help safeguard the information assets of the City, prevent the loss of data in case of data corruption, hardware or software failure, disaster, or malicious or accidental deletion. Maintaining data backups supports timely restoration of information and business processes, should such events occur.

DEFINITIONS

When a term set out below appears in the text of this Policy with its initial letters capitalized, the term is intended to have the meaning set out for it in this section. Wherever a term below appears in the text of this Policy in regular case, it is intended to have the meaning ordinarily attributed to it in the English language.

(a) "Backup" refers to the practice of saving files onto an electronic storage media for the purpose of preventing unplanned data loss in the event of equipment failure, destruction, accidental deletion, or sabotage. Backups allow business processes to resume in a reasonable amount of time with minimal data loss by restoring the data from a previous copy where feasible.

(b) "Backup Retention" refers to the time lapse between when a backup is created and when the storage is reused. The retention is how long data will be kept before the backup data is expired and/or overwritten.

(c) "CIT" or "Corporate Information Technology" refers to a Division of the Corporate Services Department within the City of Thunder Bay.

(d) "City" refers to The Corporation of the City of Thunder Bay.

(d) "DataCentre" is a group of networked servers used by the City of Thunder Bay to facilitate the storage and processing of data. These servers are located at various sites throughout the City and are managed by CIT.

(e) "Dedicated Office Worker" – City of Thunder Bay employees that rely on a computer for most or all day to fulfill their job responsibilities.

(f) "Front Line Worker" – City of Thunder Bay whose primary job function does not include using a computer. For example, firefighters, paramedics, nurses, mechanics, etc.

(g) "IT Resources" refers to the City's entire Information Technology infrastructure, including software programs, desktops, laptops, smartphones, tablets, peripheral devices, email and internet systems, data, information, and other work products installed or created with these tools, whether active or archived. This also includes transmission methods and services, such as wired and wireless networks.

(h) "Restore" refers to the act of bringing back electronic data to an earlier or original state.

(i) "User" refers to an individual, typically an employee, volunteer, or third-party, that is accessing IT Resources provided by the City of Thunder Bay.

CONDITIONS

DESKTOP FILES

1. Files and data stored on a User's desktop are excluded from Disaster and File Level Recovery.

2. Files and data are to be stored on the network server to ensure that appropriate Backups can be created as outlined in this policy.

BACKUPS FOR DISASTER RECOVERY

1. All data that resides in the City's DataCentre is backed up daily; daily backups are kept for 14 days.

2. One copy of the daily Backup is to be stored offline to protect the City from cyber security breaches that target online backup locations.

3. Additional Backups will be performed before any major technical or business-related changes to a system or application, as determined necessary by Manager – Network, Technology and Cloud Services or designate.

4. A monthly backup of data residing in the DataCentre is created each month and kept for six months.

BACKUPS FOR FILE LEVEL RECOVERY

1. All files, such as word processing, spreadsheets and presentations, stored on network drives are backed up separately to allow for file level restores.

2. Versions of each file are kept for a minimum of seven days.

3. In the event of accidental deletion or corruption of information, Users may submit a request for restoration of information to the IT Service Desk.

MICROSOFT 365 CLOUD STORAGE

1. All documents and mail files for Dedicated Office Workers are backed up daily and retained for 30 days. Additional backups are performed and kept for six months for Dedicated Office Workers.

2. All documents and mail files for Front Line Workers are maintained for 30 days.

CIT RESPONSIBILITIES

1. Manager - Networks, Technology & Cloud Services, or designate, is responsible for identifying individuals and alternates for carrying out backup and restore tasks.

2. Manager - Networks, Technology & Cloud Services, or designate, is responsible for requesting the testing of backups twice a year, at minimum.

3. IT Client Services – Help Desk Analysts are responsible for supporting file level recovery requests submitted by Users.

4. Distribution of the Policy to City employees for education and reminder purposes, as deemed necessary by CIT.

5. In coordination with the Director – CIT, the IT Compliance and Risk Specialist is responsible for determining circumstances requiring the modification of this policy.

SCOPE

The policy applies to all electronic information residing in the DataCentre.

SUPPORTING INFORMATION

Acceptable Computer Use Policy (03-05-01)

Approved by City Council on dd/mm/yyyy Replacing/Amending/Withdrawn:	_____ *Review Date:* _____ (last review and identify review frequency)
Originating Department:	Corporate Services
Contact:	Director - Corporate Information Technology
Departmental Procedural Manual:	