SECTION:	CORPORATE INFORMATION TECHNOLOGY
DEPARTMENT/DIVISION:	CORPORATE SERVICES/CORPORATE INFORMATION TECHNOLOGY
SUBJECT:	**REMOTE ACCESS POLICY**

POLICY STATEMENT

It is the policy of The Corporation of the City of Thunder Bay (the City) to define the requirements and User responsibilities to protect the City's IT Resources from unauthorized use and/or malicious attack when IT Resources are accessed remotely.

PURPOSE

The purpose of this policy is to set standards for Remote Access to the City of Thunder Bay's IT Resources by authorized Employees of the City of Thunder Bay and approved affiliated outside boards and agencies. Remote Access is given for the purpose of performing duties assigned to their position such that access does not result in an unacceptable level of risk to the City's IT Resources.

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

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

(c) "Internet Service Provider" or "ISP" is an organization that provides services for accessing, using, or participating in the Internet.

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

(e) ''Multi Factor Authentication" is an extra layer of security used to make sure that people trying to gain access to an IT Resource are who they say they are. They will be able to produce two of the following:

a. Something you know: such as a username and password; and
b. Something you have: this is something a user would have in their possession, such as a digital certificate given out by CIT.

(f) "Remote Access" is the connection to the City's IT Resources through off-site, Internet access.

(g) "User" refers to all employees, elected officials and students and any other person or entity who use the City's IT Resources with authorization.

(h) "Virtual Private Network" or "VPN" refers to the use of a public network (the Internet) to connect to a private internal network over a secure channel.

CONDITIONS

In using the City's IT Resources remotely, Users must understand their responsibilities and comply with the following requirements.

REMOTE NETWORK AND APPLICATION ACCESS

1. Authorized employees may access network and application resources through a VPN connection for the purpose of conducting City business.

2. Users must comply with the Acceptable Computer Use Policy and related IT policies when accessing IT Resources remotely.

3. An internet connection is required for Remote Access. Users are responsible for acquiring internet access through an Internet Service Provider.

4. VPN use is controlled through Multi Factor Authentication.

5. Individual applications can be accessed through a portal offering a secure connection using Multi Factor Authentication.

6. Users are authorized to use only City of Thunder Bay computer equipment to connect to the IT Resources through VPN; personal devices are not permitted for direct access to the City's network.

7. Only CIT authorized VPN client software will be used to connect to the City's network. CIT is responsible for installing and configuring this software.

USER RESPONSIBILITIES

1. Users shall not allow any unauthorized third parties to access the City's network and IT Resources.

2. Users shall ensure that all actions performed using Remote Access follow applicable policies, by-laws and any legislative requirements.

3. Users shall take reasonable precautions to ensure proper physical care of computer equipment borrowed from CIT for the purpose of Remote Access.

CIT RESPONSIBILITIES

1. It is the responsibility of CIT employees, as determined by the Director – CIT, to review and authorize Remote Access and the use of City computer equipment.

2. The IT Compliance and Risk Specialist, or designate, may monitor, audit, and/or report on User activity to ensure compliance in the event of an authorized audit or investigation.

3. In coordination with the Director – CIT, the IT Compliance and Risk Specialist or designate will determine factors that will require making changes to this policy.

SCOPE

This policy applies to all City of Thunder Bay employees, elected officials, approved affiliated outside boards and agencies, and students utilizing corporate computing devices to Remotely Access the City of Thunder Bay's data and network.

REFERENCE

Acceptable Computer Use Policy (03-05-01)
Codes of Conduct for Employees (06-01-38)
External IT Service Provider - Remote Access Policy (03-05-03)
Records Management Policy (03-06-01)

APPROVED BY:	City Council	***Date:***	March 25, 2024
Replacing/Amending:	N/A		
Originating Department:	Corporate Services		
Contact:	Director, Corporate Information Technology		
Departmental Procedural Manual:	Yes		
Affected Departments:	All		