SECTION:	*CORPORATE INFORMATION TECHNOLOGY*
DEPARTMENT/DIVISION/ SECTION:	*CORPORATE SERVICES / CORPORATE INFORMATION TECHNOLOGY*
SUBJECT:	***IT RESOURCE MANAGEMENT AND SECURITY POLICY***

POLICY STATEMENT

It is the Policy of The Corporation of the City of Thunder Bay to outline security measures and responsibilities that limit risks to the City of Thunder Bay's Information Technology (IT) Resources, as well as its business partners, and citizens of the City of Thunder Bay.

PURPOSE

The purpose of the IT Resource Management & Security Policy is to maintain and enhance the security of IT Resources. This policy will outline responsibilities to protect the confidentiality, integrity, and availability of IT Resources, while protecting the reputation of the City of Thunder Bay with respect to the City's ethical, regulatory, and legal responsibilities.

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) "Administrator" – refers to the individual position responsible for the administration and oversight of a business application or Cloud service and the data hosted within.

(b) "City" – the Corporation of the City of Thunder Bay.

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

(d) "Critical IT Resources" - IT Resources that are required to be operational for the City of Thunder Bay to continue providing services to the citizens, clients, employees etc.

(e) "Data at Rest" – refers to data that is not actively moving across devices or networks, and is stored on a desktop, laptop, mobile phone or other electronic storage system.

(f) "DataCenter" – a group of networked servers managed by CIT, used to facilitate the storage and processing of data. These servers are in various corporately owned buildings throughout the City.

(g) "Data in Motion" – refers to the active transfer of data or information from one location to another through the internet or a private network.

(h) "Electronic Documents" – files or documents that are stored on an electronic device, either saved to a server network or within the device, including but not limited to: spreadsheets, PDFs, data, source code, programs, web content systems, internally developed applications, text and instant messages, and emails.

(i) "Encryption" – the backend process of converting readable text, documents, and data into a code that can only be read by authorized users with a password or security key.

(j) "Extended Detection and Response" or "XDR" - IT Tools whose primary function is to provide visibility, analysis, and responses into internal and external resources. This visibility assists with protecting all IT Resources.

(k) "IT Resources" – 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 with these tools whether active or archived. This also includes transmission methods and services such as wired and wireless networks.

(l) "Mobile Device" – a piece of portable electronic equipment that is capable of storing corporate data and connecting to the City network through a public network (the Internet). Examples of some mobile devices are tablets and smartphones.

(m) "Penetration Testing" – also known as a Pen Test or Ethical Hack, is an authorized simulated cyberattack on IT Resources conducted to identify vulnerabilities in the security and configuration of IT Resources which can then be remediated by staff.

(n) "Personal Identifiable Information" or "PII" – Any information or data that can reasonably be linked to an identifiable individual.

(o) "Policy" – refers to the IT Resource Management & Security Policy, including related procedures as set out herein.

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

(q) "Superuser" – a special user account with unlimited privileges and access that is used to administer systems or applications.

(r) "Service Account" – credentials used to login on the network or applications to perform a regular function, bypassing the need for staff to login with their IDs.

(s) "Security Information and Event Manager" or "SIEM" – a computer security solution that conducts real-time monitoring and analysis of events to help recognize potential threats and vulnerabilities prior to a disruption to operations.

CONDITIONS

CORPORATE INFORMATION TECHNOLOGY (CIT) RESOURCE MANAGEMENT

The CIT Division provides Corporate support to business units by:

1. Supporting business units using IT Resources, with the selection, configuration, installation and training of hardware and software business technologies based on needs.

2. Purchasing all approved desktops, laptop computers, or other forms of data processing hardware, software, and peripherals, in alignment with the Supply Management By-Law.

3. Establishing standards for hardware, software, video, and communications technologies to provide stable, secure, and reliable services.

4. Purchasing, providing assistance with the purchase, and supporting of all other approved technologies and technology services that will be, or will utilize, City IT Resources.

SECURE CORPORATE NETWORK AND IT RESOURCES

1. Installing, configuring, and testing all corporate network connections and changes to firewall and router configurations must only be done when assigned by CIT management.

2. A current corporate network diagram that identifies all connections and networks, including any wireless networks, must be maintained by the Manager – Network, Technology and Cloud Services, or designate.

3. It is the responsibility of the Networks, Technology & Cloud Services section to provide appropriate threat detection and response programming to IT Resources.

4. Application default passwords and settings are changed prior to any IT Resource implementation.**Error! Bookmark not defined.**

5. All critical IT Resources shall be configured to track and record audit logs that link individuals to actions. Logs are to be forwarded to a centralized security information and event manager (SIEM) so that they are tracked, reviewed, and monitored and stored in a secure location.

6. Penetration Testing must be conducted at least annually by a reputable source.

7. CIT reserves the right to conduct Penetration Testing for business applications in development or operational technologies connected to IT Resources as required.

8. Electronic confidential information must be protected when transported or transmitted.

9. Operating Systems, updates and security patches must be kept up to date on all IT Resources.

DATA PROTECTION & ENCRYPTION

1. In consultation with CIT and where deemed required, Encryption will be implemented for data in motion and for data at rest. All access to and use of the City's confidential information must be for authorized City business and approved by User's supervisor or manager.

2. IT Resources containing Electronic Documents must be properly disposed of so that the information cannot be retrieved or reassembled when no longer required to be retained.

3. Group, shared, or generic accounts and passwords must not be used unless approved by IT Compliance & Risk Specialist or designate.

4. Administrator, superuser, and service account passwords must be stored in a secure location. If these are stored on an electronic format, the device and/or data must be encrypted, and access restricted accordingly.

5. For any browser-based transactions of cardholder data, the system must be configured to utilize HTTP Secure, over TLS version 1.2 or greater, for encryption. All versions of SSL are considered weak encryption mechanisms and must not be used.

AUTHORIZED SOFTWARE

1. Only authorized, supported, and licensed software shall be installed on City owned or managed IT Resources.

2. Only CIT staff who have been granted Administrator access shall install authorized and licensed software.

3. Software that is end-of-life and no longer supported is considered unauthorized software and shall not be installed on IT Resources. Continued use of such software is acceptable if the User installed the software when it was authorized and supported by CIT.

PHYSICAL SECURITY

1. Access to corporate network access points is restricted to authorized CIT personnel.

2. Doors to physically secured facilities shall always remain locked.

POWER AVAILABILITY

1. All servers must be connected to universal power supplies (UPS).

2. All hubs, bridges, repeaters, routers and switches and other critical network equipment shall be UPS protected.

3. Sufficient power availability shall be in place to keep the network and servers running until the Disaster Recovery Plan can be implemented.

4. UPS hardware must be installed on all servers to implement an orderly shutdown in the event of a total power failure.

5. All UPSs (Universal Power Supplies) shall be periodically tested.

6. Emergency generators shall be in place and tested periodically in the primary or secondary DataCenter.

7. The appropriate temperature and humidity must be maintained in the primary or secondary DataCenter.

SCOPE

This policy applies to the use of information, computer devices and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by the City and supported by CIT.

This policy does not apply to IT Resources that are used for the Water Treatment Plant and Water Pollution Control Plants SCADA components.

SUPPORTING INFORMATION

Freedom of Information and Protection of Privacy Act, R.S.O 1990
Personal Health Information Protection Act, S.O 2004
Personal Information Protection and Electronic Documents Act, S.O 2000
Records Authority By-Law BL 20-2022
Acceptable Use Policy (03-05-01)
Backup and Retention Policy (XX-XX-XX)
Mobile Device Policy (XX-XX-XX)
Records Management Policy (03-06-01)
Remote Access Policy (XX-XX-XX)
Electronic Monitoring Procedure (HR-05-36)

Approved by City Council on dd/mm/yyyy Replacing/Amending/Withdrawn:	X	***Review Date:***	X
Originating Department:	Corporate Services		
Contact:	Director, Corporate Information Technology		
Departmental Procedural Manual:			