| | |
|---|---|
| **SECTION:** | *CORPORATE INFORMATION TECHNOLOGY* |
| **DEPARTMENT/DIVISION:** | CORPORATE SERVICES / CORPORATE INFORMATION TECHNOLOGY |
| **SUBJECT:** | **SECURE CLOUD USAGE POLICY** |

## *POLICY STATEMENT*

It is the policy of the Corporation of the City of Thunder Bay to utilize Cloud applications in a safe and secure manner. Corporate Information Technology is committed to securing the organization's IT Resources and data while utilizing the benefits of cloud technology where reasonable, enabling employees to carry out their jobs as efficiently as possible.

## *PURPOSE*

The purpose of the Secure Cloud Usage Policy is to identify requirements for reviewing, procuring, implementing, securing, and using Cloud Services.

## *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) "Backup" – the saving of 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.

(c) "Backup Retention" – 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) "Bind" – City of Thunder Bay employees who have been given the authorization to enter into contracts or agreements. This authorization can be permanent or delegated on a case-by-case basis. Refer to approved procurement bylaws and/or policies for information on who has the authority to bind.

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

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

(f) "Click-Through Agreement" – A form or webpage outlines the responsibilities of the user accessing the program. This agreement requires a user to click a button that says "yes" or "I agree" before downloading, opening, or proceeding with a program.

(g) “Cloud Service Provider” or “CSP” – a vendor that provides centrally located software, infrastructure, or platforms as a service that has capacity to store data outside of IT Resources.

(h) “Cloud Services” – Application and infrastructure resources that exist on the Internet and share scalable resources across a network.

(i) “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.

(j) “Infrastructure as a Service” or “IaaS” – infrastructure delivery model where virtualized computing resources are provided over the internet on a subscription basis.

(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) “Personally Identifiable Information” (PII) – refers to information that when used alone or with other relevant information can identify an individual. Some examples are full name, Social Insurance Number, mailing address, medical records, etc.

(m) “Platform as a Service” or “PaaS” – a cloud delivery model in which a platform for customers to develop, run, and manage web applications is provided on a subscription basis.

(n) “Restore” – bringing back electronic data to an earlier or original state.

(o) “Software as a Service” or “SaaS” – a software delivery and licensing model in which the software is centrally hosted by a service provider and is licensed on a subscription basis.

(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.

## *CONDITIONS*

### *LICENSING AND SECURE ACCESS CONSIDERATIONS*

1. The use of Cloud Services (including but not limited to Microsoft Azure, Google Docs, Apple, AWS, DropBox) for City business requires a contract that has been approved by CIT and/or Legal Services.

2. Only City employees authorized to legally bind the corporation can agree to contracts that require such authorization.

3. Cloud Services that require individual Users to agree to terms through a Click-Through Agreement must be reviewed by Legal Services and/or CIT before proceeding. Click-Through Agreements are legal contracts and must be treated as such.

4. Use of Multifactor Authentication when using Cloud Services is preferred when Personally Identifiable Information (PII) or sensitive business data is stored in the Cloud.

The Multifactor Authentication should be reviewed by CIT prior to licensing. Where multifactor authentication is not available, the business area will accept any related risks which can cause loss, compromise, or inability to access valuable data.

5. CIT shall assist the business area in assessing the vendor's exit strategy for disengaging prior to signing a contract.

***CLOUD SERVICE PROVIDER (CSP) CONTRACT REQUIREMENTS***

1. CSPs must report any security incidents related to physical or logical data compromises immediately to appropriate City personnel and take all appropriate actions to mitigate the security risk.

2. A post-mortem report must be provided to CIT, or designated contact, after remediation of security incidents.

3. The cloud provider must facilitate periodic security audits and, when requested, provide results to IT Compliance and Risk Specialist and their Departmental contact.

4. CSPs shall ensure that all City data is collected and returned to the City, or provide written certification of data destruction, within a timeline satisfactory to the City.

5. CSPs must maintain data redundancy/backups. The schedule of these backups must be acceptable to the City and CIT. Upon request, the CSP must be able to provide a full copy of the data or data backup.

6. CSPs must provide business continuity and disaster recovery plans prior to entering into a signed agreement.

***USER RESPONSIBILITIES***

1. The use of Cloud Services must adhere to existing corporate policies and procedures relating to acceptable use of IT Resources.

2. The User is responsible for requesting access to information systems as needed.

3. Should the User no longer require access for their work duties – they shall inform the Administrator that their user access is to be removed.

4. A minimum level of authentication and authorization must be maintained.

5. Users must not share login credentials with others.

6. Personally owned and managed Cloud Services may not be used for work-related purposes including the storage, management, manipulation, sharing, or exchange of company related or owned data.

7. An addition or change in Cloud Services should be reviewed by the Director – CIT or designate; further review by the Access & Privacy Officer or Legal Services may be required before proceeding.

***ADMINISTRATOR RESPONSIBILITIES***

1. The owner of the information system, custodian of the data within it, or the appropriate designate, is responsible for authorizing access by providing approval to CIT for Users when deemed necessary.

2. The Administrator is responsible for maintaining a log of Users who have approved access to the information system they oversee.

3. The Administrator is responsible for ensuring their department maintains copies of all agreements and relevant documentation related to the procurement of the Cloud Service they oversee.

4. The Administrator is responsible for assessing the life cycle of the Cloud Services with a base assumption that the Service will be a department operating cost for five (5) years.

***CIT RESPONSIBILITIES***

1. Access for employees who no longer require access for their job function or are no longer employed with the City, will be removed upon request.

2. Periodic audits of User IDs and access should be conducted by the IT Compliance & Risk Specialist or designate.

3. Upon receiving appropriate authorization, CIT will provide the User with a unique login ID. Second factor authentication will be required upon login.

4. The Compliance & Risk Specialist, in conjunction with the Director – CIT, will determine what changes will require a review of, and updates to, this policy.

## *SCOPE*

This Secure Cloud Usage Policy applies to all business processes and data, information systems and components, and personnel of The City of Thunder Bay using third party services capable of storing or transmitting electronic data owned or lease by the City.

## *SUPPORTING DOCUMENTS*

Municipal Freedom of Information and Protection of Privacy Act, R.S.O 1990
Records Authority By-Law BL 20-2022
Supply Management By-Law BL 113-2011
Acceptable Use Policy (03-05-01)
IT Resource Management and Security Policy (XX-XX-XX)
Records Management Policy (03-06-01)

| | |
|---|---|
| ***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:*** | |