| LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA<br>POLICY MANUAL | |
|---|---|
| **SECTION** | Information Management / Information Technology |
| **POLICY** | 5405 – Appropriate Use of Information Technology Resources |

**Objective**

To ensure that the Legislative Assembly's information technology resources are safeguarded and used appropriately while protecting the privacy, confidentiality, and security of the Legislative Assembly's information.

**Application**

This policy applies to all employees of the Legislative Assembly appointed under section 39 of the *Constitution Act* (R.S.B.C. 1996, c. 66).

**Authority**

Legislative Assembly operational policies are approved by the Clerk of the Legislative Assembly, as per *Policy 1000 – Legislative Assembly Policy Framework.*

**Key Definitions**

"**confidentiality**" means the principle that information is not made available or disclosed to unauthorized individuals or entities;

"**data**" means raw material such as facts or figures stored in a structured manner that, given context, turns into information or transactions contained in information systems, applications and databases;

"**device**" means an IT resource through which a user can create or access information;

"**information**" means representations of facts, ideas and opinions on subjects, events and processes, regardless of medium or format, including data contained in IT resources;

"**information incident**" means a single or series of events involving the collection, storage, access, use, disclosure, or disposal of Legislative Assembly information that threatens privacy or information security and/or contravene law or policy;

"**IT**" means information technology;

"**IT infrastructure**" means the computer, network and storage components that make up the Legislative Assembly's information systems;

"**IT resource**" means information and communications technologies including but not limited to information systems, devices, storage, streaming video, social media and the Legislative Assembly electronic network;

"**principle of least privilege**" means employees are given the minimum level of access required to carry out their work (i.e., access is not an entitlement based on status, rank or office);

"**sensitive information**" means information that is not public information and that, if compromised, could cause injury to a person, a Member, or the Legislative Assembly;

"**supervisor**" means the person the employee directly reports to.

## 1. General

.01 As users of IT resources, employees play an essential role at all times in ensuring the appropriate use of Legislative Assembly resources, privacy, confidentiality and security of information, and the efficient operation, integrity and security of IT resources.

.02 An employee must comply with *Policy 4015 – Standards of Conduct* when using IT resources, whether use is related to their employment duties or permitted incidental personal use.

## 2. Responsibility Overview

.01 An employee is responsible for ensuring that Legislative Assembly information:

a) is stored on IT resources that are supplied, managed and protected by the IT Department or that have otherwise been approved for use;
b) is encrypted if stored on a removable media device and that the device is not shared;
c) is not stored on the local disk of a device, as it is not subject to the Legislative Assembly's backup solutions; and
d) is protected from unauthorized access by locking screens when devices are unattended and by ensuring that screens are not visible to onlookers.

.02 A supervisor is responsible for ensuring that employees:

a) have access to the least amount of sensitive information necessary to perform their duties and have the appropriate security rights and access to an IT resource, and to review at minimum annually the same against the principle of least privilege; and
b) are aware of their responsibilities regarding the appropriate use of IT resources as set out in this policy.

**3. Use of Legislative Assembly IT Resources**

.01 An employee must use Legislative Assembly-provided accounts (e.g., email and file storage) when conducting Legislative Assembly business.

.02 An employee must access their Legislative Assembly email account or IT services using a Legislative Assembly-issued device or utilize conditional access via multi-factor authentication when using a non-Legislative Assembly-issued device.

.03 Auto-forwarding a Legislative Assembly account to an email account outside the Legislative Assembly email system is prohibited.

.04 An employee must not share or otherwise compromise authentication information (passwords, mobile personal identification numbers (PINs), access cards, etc.), including by sharing passwords with the IT Service Desk or other technical support staff and writing down or otherwise storing passwords physically or in unauthorized digital applications.

.05 Delegated access to IT resources on behalf of an employee must be documented in writing and utilize separate access rights, rather than the sharing of access credentials, where possible. Where a software application does not permit unique access credentials, an exception must be requested by the responsible department head in writing to the Director of IT and mitigating business controls must be defined, documented and implemented by the requestor.

.06 An employee must not disable or otherwise tamper with standard security protection software or information security controls provisioned on IT resources provided by the Legislative Assembly.

**4. Use of Legislative Assembly IT Resources Outside of Canada**

.01 When planning to take one or more IT resources outside of Canada, the employee or their supervisor should advise the IT Service Desk in advance, with as much notice as possible, to ensure that the resources will be fully functional without jeopardizing the integrity of Legislative Assembly IT infrastructure.

**5. Prohibited Use**

.01 Use of IT resources for any activity that may expose the Legislative Assembly to civil liability or any of the following purposes or is prohibited:

a) deliberately introducing malware, viruses or other malicious software code to a device or the network;
b) deliberately tampering with IT resources;

c) revealing passwords, PINs or authentication mechanisms to others;
d) directing or engaging in activities that involve unauthorized access to or collection of personal or sensitive information;
e) bullying or harassment;
f) viewing, downloading, or communicating defamatory, discriminatory, violent, obscene or otherwise inappropriate content;
g) engaging in activities that have a commercial purpose or for the purposes of solicitation, advertising or personal financial gain, including online gambling;
h) misappropriating or infringing on the patent, copyright, trademark or other intellectual property rights of any third party, including copying material from third parties (including text, graphics, music, videos or other copyrightable material) without proper authorization;
i) violating any applicable procedures, policies or laws; and
j) any other purpose deemed inappropriate by the Chief Information Officer.

.02 Due to the security risks associated with the use of portable storage devices, such as USB flash drives and external hard drives, the following uses are prohibited:

a) storing sensitive, as detailed in *Policy 5410 – Information Security*, Legislative Assembly data on unencrypted portable storage devices;
b) sharing portable storage devices and any associated passwords;
c) using Legislative Assembly-issued removable storage devices on non-Legislative Assembly IT devices; and
d) accessing unknown removable storage devices on Legislative Assembly IT devices.

.03 To protect personal privacy, the recording of virtual meetings is limited. A meeting may be recorded by the Legislative Assembly, with advance notice to all meeting participants, for the following purposes:

a) training;
b) providing a reliable record to assist with drafting meeting minutes; or
c) to provide access to parliamentary proceedings.

.04 Recordings of confidential or unpublished Legislative Assembly content must be stored using IT resources whose data remains in Canada.

## 6. Permitted Personal Use

.01 Reasonable personal use of Legislative Assembly IT resources is permitted provided it is lawful, in line with *Policy 4015 – Standards of Conduct* and:

a) is limited during core business hours and does not interfere with the employee's duties and responsibilities;
b) does not compromise the security of Legislative Assembly IT resources or Legislative Assembly information, specifically personal or sensitive information; and
c) is not used for personal gain.

.02 To protect privacy, ensure efficient use of storage, and mitigate personal data loss, an employee should avoid storing personal data on an IT resource.

.03 The Legislative Assembly is not responsible for the loss of any personal data saved on the Legislative Assembly network or stored on an IT device.

## 7. Non-Compliance

.01 Regardless of whether an information incident has occurred, any suspected or actual breaches of this policy must be reported in accordance with the below table for any actions identified under section 8:

| Employee | Report To |
|---|---|
| Clerk of the Legislative Assembly | Chief Information Officer |
| Member of the Clerk's Leadership Group | Chief Information Officer |
| Chief Information Officer | Clerk of the Legislative Assembly or designate for the purposes of this section |
| Director of IT and Director, Digital Information Governance and Strategy | Chief Information Officer |
| All other employees | Director of IT and Supervisor |

.02 An employee found to have contravened this policy may be required to complete training or may be subject to disciplinary action,

including termination for cause, as detailed in *Policy 4050 – Progressive Discipline*. Breaches may result in criminal prosecution or civil liability.

## 8. Monitoring and Compliance

.01 Allegations of inappropriate access, collection, use, disclosure, or disposal of Legislative Assembly information or inappropriate use of Legislative Assembly IT resources may be reviewed. Reviews may include, but are not limited to, the search and/or seizure of IT resources without notice to the individual under investigation.

.02 An employee must cooperate with an investigation when requested to do so.

.03 Upon receipt of an allegation of inappropriate use, the Chief Information Officer must review the facts and any information or evidence that is reasonably available in serving as the basis of the allegation when determining the merits of initiating an investigation.

.04 If an allegation warrants action, prior to initiating an investigation, the Chief Information Officer (or person designated by the Clerk of the Legislative Assembly) must, except in urgent situations where immediate action is necessary:

a) seek the advice of the Law Clerk and Parliamentary Counsel and the Chief Human Resources Officer, as appropriate; and
b) obtain the approval of the person listed in the table below:

| Employee | Approver |
|---|---|
| Clerk of the Legislative Assembly | Subcommittee on Administration and Operations of the Legislative Assembly Management Committee |
| Member of the Clerk's Leadership Group | Clerk of the Legislative Assembly |
| Chief Information Officer | Clerk of the Legislative Assembly or designate for the purposes of this section |
| Director of IT and Director, Digital Information Governance and Strategy | Chief Information Officer |
| All other employees | Supervisor |

.05 The Chief Information Officer (or a person designated by the Clerk of the Legislative Assembly) must report on the findings of the investigation to the person whose approval was sought under section 8.03.

.06 The Chief Information Officer (or a person designated by the Clerk of the Legislative Assembly) may utilize the services of a third party and may securely transfer any seized IT resources to a third party for the purpose of completing an investigation.

**Contact**

Please contact the Information Technology Department with any questions regarding this policy at ServiceDesk@leg.bc.ca.

**References**

***4015 – Standards of Conduct***
***4050 – Progressive Discipline***
***5410 – Information Security***

Kate Ryan-Lloyd

Approved and authorized by
Kate Ryan-Lloyd, Clerk of the Legislative Assembly

*February 2, 2022*

Date

| POLICY HISTORY | |
|---|---|
| Version 1 | April 14, 2005 |
| Version 2 | March 6, 2017 |
| Version 3 | February 2, 2022 |