LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA POLICY MANUAL	
SECTION	Information Management / Information Technology
POLICY	5410 – Information Security

Objective

To protect the integrity, availability, confidentiality, and security of Legislative Assembly information and Legislative Assembly IT resources through the establishment of information security requirements, principles, and processes to mitigate risks and safeguard information.

Application

This policy applies to Members of the Legislative Assembly, employees, volunteers, contractors, and subcontractors of a Member or a caucus, employees of the Legislative Assembly appointed under section 39 of the *Constitution Act* (R.S.B.C. 1996, c. 66), and any other user of Legislative Assembly IT resources or the Legislative Assembly network.

Authority

Legislative Assembly organizational policies are approved by the Legislative Assembly Management Committee, as per *Policy 1000 – Legislative Assembly Policy Framework*.

Key Definitions

"**device**" means any electronic computing or communication technology, including, but not limited to computers, laptops, tablets, smartphones, telephones, printers, monitors, and headsets;

"**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 or contravenes law or policy;

"**information security threat**" means an activity that is flagged by the ITD for further assessment as it relates to the security of Legislative Assembly information or the security and efficient operation of Legislative Assembly IT resources (e.g., a spike in traffic to a website, unusual account activity, a suspicious email, inappropriate use of IT resources);

"ITD" refers to the department responsible for information technology;

"**Legislative Assembly IT resource**" means an IT resource that is an asset of the Legislative Assembly, which includes any devices, peripherals, apps, and software licences allocated or managed by the ITD or purchased or developed with Legislative Assembly funds, and IT resources owned, licensed, or managed by the ITD such as the Legislative Assembly network, information systems and storage, and any related equipment, hardware, and peripherals;

"**Legislative Assembly network**" means the system connecting computers and devices across the Legislative Assembly, remote locations, and constituency offices for the secure sharing of information;

"**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.

1. General

.01 This policy outlines ITD controls to protect Legislative Assembly IT resources and the information contained in those resources from inappropriate use, unauthorized access, data leaks, and cyber attacks. ITD information security controls apply to all Legislative Assembly IT resources including user devices, the Legislative Assembly network and internet-facing devices connected to physical and virtual infrastructure (i.e., devices with sensors, processing ability, software, and other technologies that connect and exchange data with other devices).

.02 Information security controls for the broadcasting network and specialized broadcasting equipment authorized to be managed independent from the Legislative Assembly network are managed by Hansard Broadcasting Services and are not included within the ITD's scope under this policy. Hansard Broadcasting Services must ensure information security controls applied to the broadcasting network and specialized equipment align with this policy and are approved by the Chief Information Officer.

.03 Information security controls established by the ITD must be guided by the following principles:

a) confidentiality: sensitive information can only be accessed by those authorized to do so;
b) integrity: information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and
c) availability: information is accessible when needed in a timely manner.

.04 Information security is a shared responsibility by all users of Legislative Assembly IT resources. All actual or suspected information incidents, unusual activity, unauthorized access, suspected inappropriate use, violations of law, loss of or damage to Legislative Assembly IT resources, and accidental misuse (e.g., clicking on a link

in a phishing email) must be reported without delay to the ITD using the Service Desk User Portal accessible via the Legislative Assembly's intranet or via email to ServiceDesk@leg.bc.ca.

2. Roles and Responsibilities

.01 The Chief Information Officer must:

a) provide leadership and direction on information security controls;
b) oversee programs that manage information security activities and monitor for, assess, and respond to policy violations and information security threats and information incidents; and
c) document and maintain internal procedures or standards for the ITD concerning encryption, information incident escalation and reporting, IT asset management, physical or environmental security, security and risk assessments or standards for software, and testing security vulnerabilities.

.02 The ITD must:

a) follow industry best practices for information security;
b) secure the Legislative Assembly network and infrastructure against information security threats and information incidents;
c) proactively monitor for and remediate misuse of Legislative Assembly IT resources by users;
d) ensure all ITD employees receive training to respond to information security threats and information incidents;
e) provide training or resources to all users of Legislative Assembly IT resources, on at least an annual basis, to build awareness of information security threats, threat reporting, and proactive security practices; and
f) advise Legislative Assembly Administration departments with specialized equipment on information security controls.

.03 Legislative Assembly Administration departments with specialized equipment managed independently of the Legislative Assembly network must collaborate with the ITD to ensure appropriate information security controls are applied to specialized equipment.

.04 Every individual with a Legislative Assembly user account must:

a) comply with *Policy 5405 – Appropriate Use of Information Technology Resources* or *Policy 7410 – Appropriate Use of IT*

Resources for Members and Employees of a Member or Caucus, as applicable*;*

b) follow directives from the Chief Information Officer about safeguarding information and Legislative Assembly IT resources; and

c) participate in information security training if mandated by the ITD.

3. Access to Legislative Assembly IT Resources

.01 Access to Legislative Assembly IT resources, including the Legislative Assembly network, is controlled through unique user accounts. Access to Legislative Assembly IT resources is granted to a user based on a user's operational requirements and responsibilities to ensure a user may only access the information and perform actions required to perform their role.

.02 When a user leaves the Legislative Assembly or is absent for an extended leave, the user's accounts must be disabled or deleted in accordance with parameters established from time to time by the ITD. User accounts that are suspended, disabled, deleted, or changed will be recorded as such and removed by the ITD from any systems connected to such accounts.

.03 The ITD may implement information security safeguards, controls, and conditions aligned with relevant industry best practices for users of Legislative Assembly IT resources.

.04 The Chief Information Officer may review information security controls and implement adjustments at any time. If necessary, the Chief Information Officer or their designate may limit user access to Legislative Assembly IT resources.

4. Information Security Threat

.01 To ensure Legislative Assembly IT resources remain secure and available to users, the ITD may monitor metadata and network traffic logs for user compliance and unusual activity in order to mitigate potential or real threats. This may include but is not limited to monitoring for malicious links, exfiltration of data, inappropriate use, and unusual user account activity.

.02 When an information security threat is identified, the ITD must respond with necessary actions and risk mitigation measures to protect Legislative Assembly IT resources and Legislative Assembly information. In responding to an information security threat or violation of Legislative Assembly policy, the ITD may:

a) limit, remediate, or isolate user access;
b) suspend or restrict user access to Legislative Assembly IT resources;
c) block user installation or access to apps and software on Legislative Assembly IT resources and support users with alternative solutions;
d) require user training to remediate issues; and
e) seize any Legislative Assembly IT resource and take any actions necessary to safeguard and protect the Legislative Assembly network environment.

.03 In responding to an attempt to breach the Legislative Assembly network or exfiltrate information, the ITD must prioritize the protection of the Legislative Assembly network, including all sensitive or personal information, and must use the most minimally intrusive means available to remediate the threat.

5. Information Incident

.01 An information security threat becomes an information incident when there is:

a) an operational impact to the confidentiality, security, or integrity of the Legislative Assembly network or Legislative Assembly IT resources; or
b) any unauthorized access, collection, retention, use, disclosure, or disposal of personal, sensitive, or Legislative Assembly information.

.02 In the event of an information incident, the ITD must resolve the incident according to internal procedures. In responding to the information incident, the ITD must:

a) contain the information incident;
b) assess the damages and risks associated with the information incident;
c) implement remedial actions to prevent a similar information incident from occurring in the future; and
d) notify Legal Services at the earliest opportunity.

.03 If an information incident results in significant damage to Legislative Assembly IT resources or results in a loss of information, the ITD must report the incident to the Chief Information Officer.

.04 The ITD must maintain information incident management procedures to ensure a quick and effective, response to information security

threats and information incidents. All information incidents must be subject to root cause analysis to determine the cause and appropriate solution to the problem.

6. Management of Legislative Assembly IT Resources

.01 The ITD must:

a) maintain an inventory of Legislative Assembly IT resources and validate the inventory on a regular basis;
b) document the return or reassignment of Legislative Assembly IT resources in the possession of a user upon their departure from the Legislative Assembly;
c) remove Legislative Assembly information from devices that are no longer needed by the Legislative Assembly;
d) securely dispose of Legislative Assembly IT resources in a manner appropriate for the sensitivity of the information the IT resource contained; and
e) establish and maintain procedures for the above-noted activities a) to d).

.02 The ITD must ensure all Legislative Assembly IT resources are equipped with approved tools to prevent, detect, and mitigate information security threats. The ITD must ensure all portable devices, such as laptops, mobile phones, and tablets are enhanced with technical security measures (e.g., passwords, encryption, real-time risk and threat monitoring) to mitigate the risk of an information incident should the device be stolen or lost.

.03 The ITD must take all reasonable precautions to ensure that sensitive information is not compromised during hardware upgrades, maintenance, or repairs and must establish procedures for:

a) tracking, recording, and conducting Legislative Assembly IT resource upgrades, maintenance, and repairs; and
b) reporting and resolving problems with hardware and software.

.04 The ITD must ensure appropriate physical and environmental security controls to prevent unauthorized physical access or damage to Legislative Assembly IT resources (e.g., servers, equipment, device inventory).

7. Operational Security and Communication Security

.01 The ITD must maintain and ensure the information systems used for day-to-day operations and communication are secure. The ITD must:

a) plan, document, and implement change request procedures to ensure changes to Legislative Assembly IT resources are applied correctly and do not compromise the security of information and information systems;
b) monitor and ensure information systems are maintained throughout the product lifecycle;
c) define, document, assess, and test data recovery processes monthly;
d) implement processes for monitoring, reporting, logging, analyzing, and correcting errors or failures in Legislative Assembly IT resources reported by users and detection systems;
e) ensure segregation of services, information systems, and users of Legislative Assembly IT resources to support business requirements based on the role requirements, management of risk, and segregation of duties; and
f) implement controls on the Legislative Assembly network to prevent unauthorized access or bypassing of security controls.

.02 The ITD must maintain encryption standards to support the safeguarding of information and reduce the risk of unauthorized access to Legislative Assembly information. The ITD must ensure all information stored electronically or transmitted over public networks is encrypted according to encryption standards.

8. Assurance and Compliance

.01 In collaboration with Legislative Assembly Administration departments and caucuses, the ITD must regularly report on departmental, caucus, and constituency office adherence to Legislative Assembly information management and information technology policies and identify any information security vulnerabilities specific to the user group requiring action or attention.

.02 The ITD must validate the efficacy of information security controls by regularly scanning for vulnerabilities and periodically testing internal procedures and measures taken to protect Legislative Assembly IT resources and Legislative Assembly information.

Contact

Questions regarding this policy may be directed to the Information Technology Department at ServiceDesk@leg.bc.ca.

References

Policy 5405 – Appropriate Use of Information Technology Resources
Policy 7410 – Appropriate Use of IT Resources for Members and Employees of a Member or Caucus

Approved and authorized by the Legislative Assembly Management Committee on May 7, 2024.

POLICY HISTORY	
Version 1	May 7, 2024