Cybersecurity and Electronic Device Policy

Version 4
Oct. 2, 2025
Information Technology

Cybersecurity and Electronic Device Policy

1. Table of contents

2. Introduction

2.1 Policy statement

The Alberta Motor Vehicle Industry Council (AMVIC) is a delegated regulatory board created by the Automotive Business Regulation in accordance with Section 136(5) of the *Consumer Protection Act*. AMVIC regulates the automotive business industry in Alberta through the powers delegated to it under the *Consumer Protection Act.*

AMVIC maintains critical and private data on information systems accessed through electronic devices. Protection of these systems, data and devices is imperative to the operation and reputation of AMVIC and is a priority for all employees.

2.2 Purpose

The purpose of this policy is to ensure the security and integrity of AMVIC's information systems, data and technology resources. It also provides direction in regards to the operation and protection of electronic devices used by AMVIC employees during the execution of their employment duties.

2.3 Definitions

In this policy:

i. "Electronic devices" or "devices" means electronic devices such as computers, tablets, servers, cloud-based applications, internal and external hard drives, flash drives, office security system, office door locks, Wi-Fi, telephones, cellular telephones, printers, and memory cards or any other electronic device that has memory.

ii. "AMVIC cloud" means the cloud environment AMVIC uses. Currently the AMVIC cloud is known as oneDesktop, soon to be oneWorkspace.

iii. "AMVIC regulatory system" means the cloud-based system AMVIC uses for licensing, registration, inspections and enforcement of the automotive industry. Currently the system is internally known as Open Regulate or Thentia Cloud and externally known as AMVIC Online.

iv. "CPIC" means the Canadian Policy Information Centre.

v. "IT" means the AMVIC information technology department.

3. Policy

3.1 Duties and responsibilities

IT reports to the chief financial officer (CFO) and the CFO is responsible for overseeing the development, implementation and maintenance of this policy.

All users of AMVIC electronic devices are expected to comply with applicable laws and AMVIC policies, procedures and guidelines. AMVIC electronic data must be protected to prevent loss of data or a data breach. Any data breach must be reported immediately by following the Privacy Breach Procedure.

AMVIC relies on third-party service providers to support key components of its IT infrastructure and must maintain proper oversight to ensure security, compliance and operational continuity.

3.2 Application of the policy

3.2.1 General information

a. All AMVIC electronic data will be stored in one or more of the following secure and password protected environments:
    i. The AMVIC cloud.
    ii. The AMVIC regulatory system.
    iii. Computers and tablets protected with Microsoft Windows BitLocker (password protected).
    iv. Encrypted flash drives, external hard drives and memory cards.
    v. A secure file transfer service approved by IT such as Sync or Dropbox.
b. AMVIC electronic data should be primarily stored in the AMVIC cloud or AMVIC regulatory system because data outside those systems is not backed up.
c. AMVIC electronic data should never be stored on or saved to unencrypted devices or devices that are not password protected.
d. Devices should be screen locked when unattended.
e. Antivirus software will be enabled on all AMVIC computers, tablets, and servers. The AMVIC cloud and AMVIC regulatory system have antivirus and security protocols managed by their respective service providers.
f. All AMVIC employees should scrutinize emails and text messages they receive to ensure they are not spam, ransomware, malware, phishing or clickbait. If an AMVIC employee suspects a threat,

they should delete the message. **If an AMVIC employee is unsure or accidently clicks on a malicious link or opens a malicious attachment, they must contact IT immediately.**

g. IT will ensure computers, tablets, servers and cloud based applications are updated and patched to a reasonably current state.

h. Employees are expected to observe distracted driving laws while using an AMVIC cellular telephone and operating a vehicle.

i. Employees are expected to use Wi-Fi with the cellular telephone when practical to minimize cellular data usage.

j. Cellular telephones are generally assigned to investigators, field inspectors, IT and the management team as appropriate. Assignment of cellular telephones to other employees will be at the discretion of the chief executive officer.

3.2.2 General access passwords and passcodes

a. General access passwords and passcodes are shared to enable AMVIC employees to access shared use devices. These devices include Wi-Fi, door keypads, computers in meeting and board rooms, the audio video recording systems, and vendor specific passwords for sites such as Canadian Black Book. The remote bank deposit password will be shared only to accounting employees.

b. The guest Wi-Fi password may be shared with individuals external to AMVIC at the discretion of IT.

c. IT is responsible to maintain these passwords and passcodes. IT will ensure these passwords and passcodes are strong enough to reasonably mitigate risks to AMVIC.

d. These passwords and passcodes are to be shared internally only with AMVIC staff. **If an AMVIC employee ever suspects a password or passcode has been compromised, they must notify IT immediately.**

3.2.3 Individual passwords, passcodes and PINs

a. Individual passwords, passcodes and PINs are critical to the security of AMVIC electronic devices and AMVIC data. Individual passwords, passcodes and PINs also protect AMVIC employees where usage by an employee can be identified. IT may also require employees to use multi-factor authentication applications in conjunction with passwords, passcodes and PINs to authenticate as applicable.

b. AMVIC employees should never share an individual password, passcode or PIN.

c. Passwords, passcodes and PINs must be complex and strong to prevent them from being guessed or cracked.

d. Passwords must be a minimum of eight characters and include at least one uppercase letter, one number and one special character. Repetitive letters and numbers are not acceptable. Some devices and software cannot accommodate some of the requirements above, but it is the responsibility of each AMVIC employee to make their password as complex as possible.

e. Passcodes and PINs must be at least four digits long and be complex. Passcodes and PINs such as "1234" or "1111" are not acceptable.

f. It is acceptable to share the password, passcode or PIN for cellular telephones, flash drives and Apple ID with IT.

g. **If AMVIC employees ever suspect a password, passcode or PIN has been compromised, or if they receive multi-factor authentication requests when they are not accessing the associated service or application, they must notify IT immediately.**

3.2.4 Unacceptable use of AMVIC electronic devices

a. AMVIC employees should not access devices or data they are not authorized to access; or run programs that attempt to calculate or guess passwords.

b. AMVIC employees should not share a password, passcode or PIN they are not authorized to share.

c. AMVIC employees should not delete or alter data unless they are authorized to do so.

d. To maintain compliance with anti-spam legislation, AMVIC employees should not send bulk emails without expressed consent from the recipients.

e. AMVIC employees should not store AMVIC data outside of the AMVIC cloud, AMVIC regulatory system, computer and tablets protected with Microsoft Windows BitLocker, encrypted flash drives, encrypted external hard drives and encrypted memory cards, or a secure file transfer service approved by IT, such as Sync or Dropbox.

f. Any effort designed to conceal the true identity of a user, or reduce the traceability of a resource being used to access AMVIC electronic devices is prohibited. This includes programs which disguise an IP address, MAC address or geo-location of the device being used to access any AMVIC electronic devices. Exceptions may be granted for approved covert activities conducted by investigators or industry standards officers. Exceptions can be granted by AMVIC managers in consultation with IT.

g. AMVIC employees should not use devices to access pornography or any illegal content.

h. Non-AMVIC electronic devices including flash drives or hard drives should never be connected to AMVIC electronic devices by AMVIC employees unless they know the source of the device and they are confident it does not contain malicious code. IT may provide approval to connect a non-AMVIC device to an AMVIC device or network.

i. AMVIC electronic devices are not meant to be used for personal purposes, however, periodic personal use is acceptable as long as the personal use does not:

   i. Interfere with the functionality of AMVIC systems;

   ii. Increase AMVIC costs;

   iii. Include commercial purposes other than AMVIC business;

   iv. Provide personal gain;

   v. Inappropriately imply AMVIC representation or endorsement; and

   vi. Access inappropriate websites.

j. In the event personal use increases AMVIC costs, the employee will reimburse AMVIC for the additional cost.

3.2.5 Physical security

The physical security of AMVIC offices, devices and data is a priority and must be observed by all AMVIC employees. This is for the safety of employees and the protection of AMVIC property and data.

a. Outside of business hours or when the office is not occupied, all deadbolts, electronic locks and mechanical push button locks must be locked to ensure the office is secure and the security system in the Edmonton office must be set to “away”.

b. During office hours and while the office is occupied, all doors with electronic locks and mechanical push button locks must be locked.

c. The CPIC room has restricted access and will remain locked when not occupied.

d. Key holders to the CPIC room are restricted and keys are assigned and tracked by the chief financial officer.

e. All AMVIC devices must be password, passcode or PIN protected and must be locked when unattended.

f. When outside the AMVIC office or an employee’s home office:

   i. AMVIC employees should not leave devices unattended; when practical, AMVIC employees should carry devices with them.

ii. If AMVIC employees must leave a device unattended outside of the AMVIC office or their home office, they should ensure the device is secure.

iii. Devices should never be left in a vehicle for an extended period of time or overnight or in an unlocked vehicle.

iv. If a device is in a locked vehicle for a short period of time it must be stored out of view.

v. A device outside of an AMVIC office must always have the local data encrypted.

3.2.6 Lost or stolen devices

a. **In the event of a lost or stolen electronic device, employees must report the incident immediately to IT or the chief financial officer.** The report should include details such as the time, date, location, and circumstances of the loss or theft.

b. IT will make every effort to remotely track and, if necessary, wipe the lost or stolen device to prevent unauthorized access to sensitive data. IT will, among other things, reset the password and block all access to network resources, including e-mail, until such a time that the employee can change their passwords.

c. IT will conduct a security review to assess the impact of the loss or theft and determine whether any confidential information was compromised and follow the Privacy Breach Procedure where necessary.

d. Employees may be responsible for the replacement cost of the lost or stolen device, depending on the circumstances. AMVIC will provide a replacement device as deemed necessary for continued work responsibilities.

3.2.7 Damaged devices

a. Employees are expected to take preventive measures to avoid damage to electronic devices, such as using protective cases, keeping liquids away from devices and handling them with care.

b. Employees should promptly report any damage or malfunction of their electronic devices to IT. This includes accidental damage, spills, drops or any other incidents that may affect the device's functionality. The report should include details such as the nature of the damage, the circumstances surrounding the incident and any potential impact on work responsibilities

c. IT will assess the extent of the damage and determine whether the device can be repaired. If the device is repairable, IT will initiate the necessary repairs. If not, a replacement device may be provided. In cases where repairs are expected to take an extended period, IT may provide employees with temporary devices to minimize disruption to work responsibilities.

d. If the damage is determined to be due to negligence or misuse, the employee may be responsible for the cost of repairs or replacement.

3.2.8 Third-party service providers

a. Prior to engaging with any third-party service provider, an evaluation of the vendor's security posture, compliance history and service-level capabilities must be completed to ensure they meet AMVIC's security and service standards. Where applicable, the vendor must demonstrate adherence to industry-standard cybersecurity frameworks (e.g. ISO 27001, SOC 2, NIST).

b. Contracts with third-party service providers must include cybersecurity and data protection clauses, including but not limited to:

   i. Data ownership and confidentiality;

   ii. Requirements for data encryption;

   iii. Incident notification;

   iv. Service level commitments; and

   v. Termination and data return.

c. IT will monitor vendor performance in accordance with service levels outlined in contractual agreements.

4. Administration

4.1 Related documents and legislation

AMVIC Code of Conduct
Audio-Visual Recording Policy
CPIC Policy
Employee Handbook

4.2 Procedures

Privacy Breach Procedure

4.3 Forms

4.4 Amendment history

Version	Date	Summary of update
1.	Nov. 19, 2019	Original.
2.	Sept. 15, 2022	Amendments to name of regulatory system and file transfer services used by IT. Reviewed and approved by AMVIC CEO, Malcolm Knox.
3.	Jan. 2, 2024	Added sections 3.2.6 Lost or stolen devices and 3.2.7 Damaged devices. Grammatical corrections in section 3.2.4. Reviewed and approved by AMVIC CEO, Malcolm Knox.
4.	Oct. 2, 2025	Amendments to sections 2.1 and 2.2 to include systems accessed via electronic devices. Amended 2.3 definition iii. to include Thentia Cloud. Amendment to section 3.1 to include IT and CFO responsibilities and reliance on third-party service providers. Section 3.2.3 amended to include use of authentication applications. Added section 3.2.8. Minor formatting throughout and updated name of policy to include Cybersecurity. Reviewed and approved by AMVIC CEO, Malcolm Knox.

4.5 Scheduled review date

October 2028