

BRIEFING NOTE

TO: Board of Directors

FROM: Fazal Khan, Registrar, CEO

DATE: September 28, 2026

SUBJECT: Technology and Cyber Security Policy (2-13) Monitoring Report

☐ For Decision

☐ For Information

☒ Monitoring Report

Purpose:

To provide the Board with a monitoring report on the Technology and Cyber Security Policy, in accordance with the monitoring report schedule approved by the Board.

Registrar, CEO Interpretation and Evidence:

The Technology and Cyber Security Policy (2-13) was approved by the Board in 2022. The information contained in this monitoring report represents compliance with a reasonable interpretation of the policy. The monitoring report covers the period from **September 2025 to September 2026**.

The next Technology and Cybersecurity Policy Monitoring Report is due in **September 2027**.

Policy Requirement	Interpretation and Evidence
Taking steps to ensure that adequate technology is in place to permit the College to meet its public protection mandate.	Technology Planning and Lifecycle Management: The Registrar and CEO is responsible for ensuring the College maintains appropriate technology to support its operations. Hardware is regularly maintained and replaced as it approaches the end of its useful life or warranty period to reduce the risk of service interruptions. Technology requirements and associated budget needs are reviewed annually with the Finance Committee and incorporated into the budget presented to the Board for approval. IT Security and Monitoring: The College's IT service provider is responsible for network, cloud and endpoint security and continuously monitors the College's IT environment. The Registrar receives monthly proactive monitoring reports to support ongoing oversight of system performance and security. Hardware Update: No computer hardware replacements were required in 2026. In 2025, seven laptops were upgraded in

	preparation for Microsoft ending support for Windows 10, reducing the need for additional hardware replacements in the current year.
Regularly reviewing the College's data and technology plan to identify areas for improvement or adaptation.	Technology Planning: The Registrar and CEO regularly reviews the College's data and technology plan with the IT provider's Executive Strategist. These reviews consider required upgrades or updates to existing systems, emerging technology needs, and opportunities to strengthen the College's cybersecurity through additional software, tools or security measures. The IT provider also proactively alerts the College between scheduled reviews where an issue or risk is identified that requires more immediate attention.
Taking reasonable steps to safeguard the College's information technology infrastructure. This will include taking reasonable steps to: a) Minimize the likelihood and impact of service disruptions and/or cybersecurity threats; And Protect the College's data loss, damage, theft, or unauthorized collection, use or disclosure.	Information Technology Safeguards: The Registrar and CEO has implemented a number of measures to safeguard the College's information technology infrastructure and reduce cybersecurity and business continuity risks, including: • Requiring all College staff to complete ongoing cybersecurity awareness training, including modules designed to educate staff about emerging threats and periodically test their knowledge and awareness. • Phased migration from existing partial-cloud based platform to the latest, fully cloud based database to ensure continued alignment and support from our vendor. This project will ensure efficient future functionality upgrades and continued safeguarding of registrant data • Ensuring College documents and information are stored and backed up within shared systems to minimize the potential for data loss if an individual device is lost, damaged or compromised. • Ensuring the College's IT provider regularly tests its cybersecurity monitoring tools and controls to identify potential vulnerabilities and address any weaknesses identified.

	• Maintaining appropriate insurance coverage to provide financial protection against risks associated with data loss, damage, theft, and unauthorized access, collection, use or disclosure of information. • Overseeing the maintenance of the College's database on a secure cloud-based platform to further safeguard registrant and College information and support business continuity. • Maintaining an inventory of College hardware and applying additional security measures when College devices are taken outside Ontario.
--	---

Public Interest Considerations:

The College's technology and cybersecurity practices support the public interest by protecting the confidentiality, integrity and availability of registrant and College information. Ongoing monitoring, secure cloud-based systems, staff training and appropriate technology planning also support business continuity and help ensure the College can continue carrying out its regulatory functions in the event of a technology or cybersecurity incident.

Diversity, Equity, and Inclusion Considerations:

Technology planning considers accessibility and differing user needs when implementing or updating systems and digital tools. Maintaining reliable and accessible technology helps support equitable access to the College's services and information for staff, registrants, applicants, Board members and other stakeholders.

Risk Management Considerations:

The College uses multiple safeguards to reduce technology and cybersecurity risk, including 24/7 IT monitoring, regular system and security reviews, cybersecurity awareness training, secure cloud-based storage and backups, hardware tracking, and appropriate insurance coverage. Together, these measures help reduce the likelihood and potential impact of unauthorized access, data loss, system disruption and other cybersecurity incidents, while supporting timely identification and response when risks arise.

Recommendations/Action Required:

- 1) Does the Board agree that the Registrar, CEO's interpretation of the Technology and Cybersecurity Policy was reasonable?
- 2) Does the Board agree that the Registrar, CEO complied with this policy as reasonably interpreted?

POLICY TYPE: OPERATIONAL BOUNDARIES

2-13 Technology and Cyber Security Policy

The Registrar, CEO will not operate without:

1. Taking steps to ensure that adequate technology is in place to permit the College to meet its public protection mandate.
2. Regularly reviewing the College's data and technology plan to identify areas for improvement or adaptation.
3. Taking reasonable steps to safeguard the College's information technology infrastructure. This will include taking reasonable steps to:
 - a. Minimize the likelihood and impact of service disruptions and/or cybersecurity threats; and
 - b. Protect the College's data from loss, damage, theft, or unauthorized collection, use or disclosure.