College of Opticians of Ontario

BRIEFING NOTE

TO: **Board of Directors**

FROM: **Governance Committee**

DATE: **October 3, 2022**

SUBJECT: **5.2 Technology and Cyber Security Policy 2-13**

☒ For Decision ☐ For Information ☐ Monitoring Report

Purpose:

To review a proposed new operational boundaries policy for risk tolerances for the Registrar, CEO regarding the management of technology and cyber security at the college.

Background:

The College Performance Measurement Framework (CPMF) was implemented by the Ontario Ministry of Health (Ministry) in 2020 to measure in a standardized and consistent manner how well the colleges are executing their mandate.

Standard 4ii of the 2021 CPMF relates to colleges being required to demonstrate regularly reviewing and updating their college's data and technology plan to reflect how it adapts its use of technology to improve college processes in order to meet its mandate.

Currently:

1. The Board regularly reviews and receives monitoring reports on operational boundaries policies relating to the protection of COO data and on achievement of KPIs on strategic objectives relating to streamlining technological processes.

2. Has general plans relating to data technology form part of the annual budgeting process where the Finance Committee and Board are presented with relevant information relating to data technology needs for the year and can allocate funds accordingly.

3. The COO has established strategic objectives relating to streamlining COO processes, and the Board receives regular updates on the achievement of KPIs relating to these goals.

At present, the College only partially meets this standard. In its 2021 CPMF Report, the College indicated that it planned to improve its performance in this area by establishing a more formal operational boundaries policy specific to data technology and cyber security during the 2022 reporting period.

College of Opticians of Ontario

For Consideration:

A draft of a new Operational Boundaries policy called the Technology and Cyber Security policy 2-13 is outlined in **Appendix A** for review and discussion.

The purpose of this policy is to lay out the risk boundaries for the Registrar, CEO with respect to ensuring, reviewing and safeguarding the College's data and technology.

The Committee suggests that monitoring reports of this policy be presented by the Registrar to the Board every year and that it be reviewed for its content every three years by the Board.

Public Interest Considerations:

The new Technology and Cyber Security Policy 2-13 serves an important purpose in confirming that the Board is fulfilling its duties and responsibilities and that the appropriate processes are in place to ensure that they are giving due diligence to planning and oversight over the college's technology and cyber security. It will also help to identify and analyze potential risks before they negatively impact the College.

Diversity, Equity and Inclusion Considerations:

It is incumbent on the Board to consider whether the proposed policy is consistent with the COO's organizational values with respect to diversity, equity and inclusion.

Recommendation:

That the Board approve the Technology and Cyber Security Policy 2-13 as recommended by the Governance Committee.

APPENDIX A

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.