CUPE EMPLOYEES' PENSION PLAN

INFORMATION TECHNOLOGY RISK MANAGEMENT POLICY

1. PURPOSE

The Joint Board of Trustees of the CUPE Employees' Pension Plan (the "JBT") has adopted this Information Technology Risk Management Policy (the "Policy") to document certain of its information technology risk management practices. These include practices for reviewing, and responding to, information technology risk management incidents that may affect the JBT, the CUPE Employees' Pension Plan (the "CEPP"), or any beneficiaries of the CEPP.

2. DEFINITIONS

In this Policy, the following words and phrases have the following meanings:

"**IT**" means information technology.

"**IT Risk**" means the risk of financial loss, operational disruption or damage, or reputational loss, as a result of the inadequacy, disruption, destruction, failure, or damage by any means, of, or to, IT systems, infrastructure, or data. For clarity and notwithstanding the generality of the foregoing, the JBT's IT Risks:

(a) include, but are not limited to, cyber risks;

(b) include any and all risks related to the use of IT; and

(c) can be external, or internal, to the JBT.

"**Material IT Risk Incident**" means any IT Risk incident that the JBT determines is material. The JBT will consider, and determine, if an IT Risk incident is a Material IT Risk Incident in accordance with this Policy and with reference to any applicable legal requirements and regulatory guidance.

"**Personal Information**" means information about an identifiable individual that is private in nature and not readily available to the public.

"**Privacy Breach**" means any unauthorized access to, or unauthorized disclosure of, Personal Information resulting from the inadequacy, disruption, destruction, failure, or damage by any means, of, or to, IT systems, infrastructure, or data.

3. IT RISK MANAGEMENT GUIDANCE

The JBT's practices for the management of IT Risks are consistent with the IT Risk Management Guidance (the "Guidance") effective April 1, 2024 published by the Financial Services Regulatory Authority of Ontario ("FSRA"). The JBT's practices for the management of IT Risks include continued compliance with legal requirements related to IT Risks and the protection of Personal Information, including the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). These practices also include industry accepted practices for the effective management of IT Risks set out in the Guidance as follows:

a) Governance – The JBT governs, and oversees, its IT Risks in accordance with pension industry accepted practices.

b) Risk Management – The JBT relies on pension industry accepted practices to effectively manage its IT Risks.

c) Data Management – The JBT uses pension industry accepted practices to effectively manage, and secure, confidential data.

d) Outsourcing – The JBT effectively manages the IT Risks associated with any outsourced, or co-sourced, activity, function, or service.

e) Incident Preparedness – The JBT is prepared to effectively detect, log, manage, resolve, recover, monitor, and report on, IT Risk incidents in a timely manner.

f) Continuity and Resiliency – The JBT is prepared to ensure the continuity of its IT assets and its ability to deliver critical services during, and following, an IT Risk incident.

g) Notification of Material IT Risk Incidents – The JBT is prepared to notify FSRA if a Material IT Risk Incident occurs.

The JBT retains third parties to carry out certain activities, functions, and services. The JBT expects each third party it retains to follow pension industry accepted practices for the effective management of IT Risks. In addition, the JBT expects each third party it retains to immediately report to the JBT if an IT Risk incident occurs that affects that party's operations and that may affect the JBT, the CEPP, or any of the CEPP's beneficiaries. The JBT intends to seek to address IT Risks and the Guidance in contractual arrangements for outsourced activities, functions, and services.

Any IT Risk incidents that may affect the JBT or the CEPP, including any of the CEPP's beneficiaries, will be addressed in accordance with the Incident Preparedness and Response Procedure detailed in Section 4.

4. INCIDENT PREPAREDNESS AND RESPONSE PROCEDURE

(a) Identification and Internal Reporting

The JBT expects that all IT Risk incidents that may affect the JBT or the CEPP, including any of the CEPP's beneficiaries, will be immediately reported to the JBT. This expectation applies to each member of the JBT and each third party retained by the JBT. The JBT will advise each third party it retains of this expectation.

(b) JBT Assessment of an IT Risk Incident

If the JBT is advised that an IT Risk incident has occurred that may affect the JBT or the CEPP, including any of the CEPP's beneficiaries, the JBT will consider the following questions:

(i) Is the IT Risk incident a Material IT Risk Incident?
(ii) Does the IT Risk incident constitute a Privacy Breach?

In addition, if the JBT determines that the IT Risk incident constitutes a Privacy Breach, the JBT will consider, and determine, whether it is reasonable to believe in the circumstances that the Privacy Breach creates a real risk of significant harm to the individual(s) whose Personal Information was involved in the Privacy Breach.

(i) <u>Is the IT Risk incident a Material IT Risk Incident?</u>

The JBT will consider, and determine, whether the IT Risk incident is a Material IT Risk Incident based on the impact of the IT Risk incident on the JBT's or the CEPP's operations and/or the CEPP's beneficiaries. When considering, and determining, whether an IT Risk incident is a Material IT Risk Incident, the JBT will consider relevant factors and may consult with legal counsel, IT systems and security experts, and other advisors.

Indicators that a Material IT Risk incident has occurred include, but are not limited to, the IT Risk incident:

- disrupts the JBT's or the CEPP's operations to an extent that the CEPP can not be effectively administered;

- is likely to negatively affect other entities or individuals regulated by FSRA or is likely to reoccur with other entities or individuals regulated by FSRA;

- compromises confidential CEPP member data, including Personal Information; or

- impacts the ability of the JBT or the CEPP to pay benefits.

(ii) Does the IT Risk Incident constitute a Privacy Breach?

The JBT will consider and determine if the IT Risk incident constitutes a Privacy Breach. If the JBT determines that the IT Risk incident constitutes a Privacy Breach, it will consider the following question at (iii) below.

(iii) Does the Privacy Breach create a Real Risk of Significant Harm?

The JBT will determine whether it is reasonable to believe in the circumstances that the Privacy Breach creates a real risk of significant harm to the individual(s) whose Personal Information was involved in the Privacy Breach. In making this determination, the JBT may consult with legal counsel, IT security and systems experts, and other advisors.

In accordance with PIPEDA, the factors that are relevant to determining whether a Privacy Breach creates a real risk of significant harm to the individual(s) whose Personal Information was involved in the Privacy Breach include the sensitivity of the Personal Information involved in the Privacy Breach and the probability that the Personal Information has been, is being, or will be, misused.

(c) Containment

The JBT will take reasonable and appropriate steps to identify the scope of any IT Risk incident, including a Privacy Breach and/or Material IT Risk Incident, and take reasonable and appropriate steps to contain it. These steps may include, but are not limited to:

- Actions to end any unauthorized access;

- Work with IT systems and security experts, legal counsel, and other

advisors;

- Documenting the nature of the IT Risk incident;
- Documenting activities to contain the IT Risk incident; and
- Taking care not to compromise any ability to investigate, and not to destroy evidence that may assist to determine the cause of, the IT Risk incident.

(d) External Notification - Material IT Risk Incident

If the JBT concludes that an IT Risk incident is a Material IT Risk Incident, the JBT will advise FSRA of the incident as soon as is reasonable after determining that the IT Risk Incident is a Material IT Risk Incident. In accordance with the Guidance, this notification will normally be provided to FSRA within seventy-two (72) hours or sooner after the JBT concludes that a Material IT Risk Incident has occurred. This notification will be provided to FSRA by emailing FSRA's IT Risk Incident Notification Form to the applicable email address provided by FSRA or by such other notification method that is acceptable to FSRA. The JBT will respond to follow-up inquiries, if any, from FSRA about the IT Risk incident.

The JBT will consider notifying any relevant insurer of the IT Risk incident. To assist in the JBT's consideration of whether to notify any relevant insurer of the IT Risk incident, the JBT may consult with legal counsel, IT systems and security experts, and other advisors

(e) External Notification - Privacy Breach

If the JBT concludes that it is reasonable to believe that a Privacy Breach creates a real risk of significant harm to the individual(s) whose Personal Information was involved in the Privacy Breach, the JBT will report the Privacy Breach to the Privacy Commissioner of Canada and, unless prohibited by law, the affected individual(s). Each such report will be provided in accordance with PIPEDA. The JBT will also consider whether any other third parties should be advised of the Privacy Breach. If the JBT determines that any of such parties should be advised of the Privacy Breach, the JBT will advise any such third parties of the Privacy Breach. To assist in the JBT's consideration of whether any other third parties should be advised of the Privacy Breach, the JBT may consult with legal counsel, IT systems and security experts, and other advisors.

The JBT will respond to follow-up inquiries, if any, about the Privacy Breach.

(f) Investigate

To determine what other steps are required to respond to the IT Risk incident, including a Privacy Breach and/or Material IT Risk Incident, the JBT will investigate the IT Risk incident. This will include an investigation of the circumstances, and impacts, of the IT Risk incident. To assist this investigation, the JBT may engage legal counsel, IT systems and security experts, and other advisors.

(g) Prevention

After investigating an IT Risk incident, the JBT will review, and consider, how future potential future IT Risk incidents may be prevented. To assist in this review, and consideration, the JBT may consult with legal counsel, IT systems and security experts, and other advisors. The JBT will implement such actions as it determines are appropriate to prevent a future IT Risk incident.

(h) Record Keeping

Records of all IT Risk incidents that are reported to the JBT, including those that constitute Material IT Risk Incidents and Privacy Breaches, will be maintained. These records are to include the date of the incident, a description of the incident (including, if applicable, the nature of the information involved in the incident), and whether the incident was reported to FSRA, the Privacy Commissioner of Canada and/or any affected individual(s). These records will be maintained for at least five years or such longer period as determined by the JBT.

:cp/cope 491
December 5, 2024