Exhibition Place

REPORT FOR ACTION

Information Technology Corporate Policies 2026 Review and Update

Date: March 31, 2026
To: The Board of Governors of Exhibition Place
From: Don Boyle, Chief Executive Officer
Wards: Ward 10 Spadina - Fort York

SUMMARY

This report recommends the approval of the new IT Corporate Policies, Standards, Standard Operating Practices (SOP's), and Guidelines for Exhibition Place detailed in Appendix A & B.

These policies were developed in response to the Confirmation Program which was the result of a City Council motion to extend the mandate of the City Chief Information Security Officer (CISO), now called Toronto Cyber Security to direct Agencies to formulate organizational cyber frameworks that align with the city's objectives and frameworks by adoption of Report EX14.3.

The policies were further revised to incorporate feedback from the recent City Auditor General Cyber Security Audit of Exhibition Place - Phase 1 which was approved by the Board in December 2025 and adopted by City Council at its meeting on March 25, 26 and 27, 2026 by adoption of Report AU11.5.

This report recommends the approval of the IT Corporate Policies and Guidelines which were formulated to align with the City's objectives and frameworks. The policies are detailed in Appendix A and B.

RECOMMENDATIONS

The Chief Executive Officer recommends that:

1. The Board approve the new IT Information Security Policy Framework, summary list of all policies and guidelines as Appendix A, and the policies and guidelines as Appendix B with the established annual review cycle.

FINANCIAL IMPACT

There are no financial implications with this report.

DECISION HISTORY

The 2022-2026 Strategic Plan has a goal to invest in our people and culture. The consistent application of policies is part of the conventional building blocks for an enabling workplace culture.

At its meeting of December 5, 2025, the Board approved the City Auditor General Cybersecurity Audit of Exhibition Place - Phase One: Physical Security, User Access Management and Staff Training by adoption of report EP20.1 which was subsequently adopted by City Council at its meeting of March 25, 26 and 27, 2026 by adoption of report AU11.5.
https://secure.toronto.ca/council/agenda-item.do?item=2026.AU11.5

At its meeting of December 12, 2024, the Board approved new and updates to the Employee and Corporate Policies.
https://secure.toronto.ca/council/agenda-item.do?item=2024.EP14.6

At its meeting of May 22 and 23, 2024, City Council adopted the following:

1. City Council direct the Chief Information Security Officer to establish a cyber security risk management partnership with agencies and corporations by:

a. incorporating their identified cyber risks into the City's governance and compliance risk management program;

b. conducting ongoing cyber security assessments on agencies and corporations, including Exhibition Place;

c. assessing rates of compliance; and

d. developing remediation plans and strategies to reduce risk and promote compliance.
https://secure.toronto.ca/council/agenda-item.do?item=2024.EX14.3

At its meeting of December 8, 2020, the Board approved updates to the Employee and Corporate Policies.
https://secure.toronto.ca/council/agenda-item.do?item=2020.EP15.4

At its meeting of May 31, 2018, the Board approved updates to the Employee and Corporate Policies, most of the revisions were required because of amendments to the Employment Standards Act, enacted by the Province through Bill 148.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2018.EP11.10

At its meeting of December 9, 2016, the Board approved of the Exhibition Place Employee policies which resulted from an entire review of all policies and best practices in the industry.
https://www.explace.on.ca/files/file/58b608e388d7e/Item-12-Employee-Policies.pdf

COMMENTS

Exhibition Place strives to ensure that all our policies are updated regularly and aligned with legislative requirements. Policy reviews occur every four years unless legislative changes or new policies are recommended. In these instances, these unscheduled policy submissions will be brought to the Board for their approval as appropriate.

Framework

The framework attached in Appendix B, establishes clear, enforceable controls for protecting Exhibition Place's technology assets, data, and operations from cyber threats. It builds directly on City of Toronto CISO practices while being tailored to our venue's unique needs (public events, guest networks, and diverse users). The policies formalize existing good practices, leverage tools already in use (Microsoft Intune and City CISO scanning/pen-testing services), and require negligible new costs.
This framework has been developed in direct response to observations raised in the City of Toronto Auditor General's Phase One Cybersecurity Audit of Exhibition Place in November 2025, particularly regarding user access management and staff awareness/social engineering controls. It also positions the organization strongly for the upcoming Phase Two audit findings expected to be presented to the Board in April 2026. By formalizing these policies and standards now, Exhibition Place demonstrates proactive governance and a commitment to aligning with broader City of Toronto information security expectations.

The framework attached in Appendix B, forms a cohesive security framework covering access control, system hardening, vulnerability management, user awareness, mobile devices, wireless networks, asset lifecycle, and privileged access.

Key Financial and Risk Implications

Risk Reduction: Addresses the most common breach pathways (phishing, weak credentials, unpatched systems, over-privileged accounts, and poor configurations), lowering the probability of business disruption, data loss, or reputational damage.

Insurance & Compliance: Meets growing expectations of cyber insurance providers and auditors; strengthens our renewal position and demonstrates prudent governance.

Cost Profile: Negligible incremental operating expense; most requirements use existing Microsoft licensing and City of Toronto resources. Implementation effort will be absorbed within current ICT staff capacity.

Operational Efficiency: Clear rules and procedures reduce ad-hoc work and improve audit readiness.

Board Oversight: Policies (especially privileged access) require explicit management approval, giving senior leadership and the Board visibility and control over high-risk accounts.

Summary of Core Policies

Access Management & Privileged Access: Requires unique accounts, strict approvals (including IT Director/Chief Financial Officer & Corporate Secretary for privileged), regular reviews, and immediate removal for leavers.

Credential & Password Policies: Enforces strong, unique passwords with differentiated rules by account type and secure handling practices.

Hardening & Configuration: Mandates secure defaults and removal of unnecessary services on all systems (includes Windows 11 24H2 baseline).

Vulnerability Management: Quarterly scans, annual penetration testing (via City CISO), and risk-based patching.

Phishing & Security Awareness: Requires annual training by all staff, phishing assessments, and immediate reporting.

Mobile Device & Wireless Security: Ensures encryption, approved apps, and isolated guest networks.

Asset Management & Network Segmentation: Tracks assets through secure disposal and uses VLANs to limit breach spread.

Supporting documents include request forms, technical standards, and SOPs. All policies mandate annual review.

Appendix A & B lists all the Exhibition Place new IT Corporate Policies.

- Appendix A is a summary list of all IT Corporate Policies which will align with the city's objectives and frameworks and are also listed as new policies.
- Appendix B provides the specific policies and guidelines.

CONTACT

Hardat Persaud, Chief Financial Officer & Corporate Secretary, 416-263-3031, hpersaud@explace.on.ca

John Koperwas, Director of IT, Telecommunications and Records & Archives, 416-263-3070, Jkoperwas@explace.on.ca

SIGNATURE

Don Boyle
Chief Executive Officer

ATTACHMENTS

Appendix A - Summary List of IT Corporate Policies and Guidelines

Appendix B - List of the Corporate Polices and Guidelines