Exhibition Place

Item No. 10

November 1, 2012

To: The Board of Governors of Exhibition Place

ACTION REQUIRED

From: Dianne Young
Chief Executive Officer

Subject: E-Mail Policy – Board Employees

Summary:

This report recommends that an E-Mail Policy for employees of the Board be implemented. The specific language within the new policy is in substance identical to the policy adopted by the City's Information & Technology Division on June 25, 2007, but modified to address the particular nature of Exhibition Place.

Recommendations:

It is recommended that the Board approve an E-Mail Policy for Board Employees, as outlined in Appendix "A.

Financial Implications:

There are no financial implications arising from the recommendations in this report.

Decision History:

The Exhibition Place 2009 – 2012 Strategic Plan had an Organizational & Staffing Goal to *Review and revise our corporate systems* and as a Strategy to support this Goal *we will complete an annual review of By-Laws, Policies and Procedures of the Board of Governors and CNEA Board of Directors.*

Issue Background:

Given the growth in information and technology usage by employees, a detailed policy is necessary.

Comments:

The new E-Mail Policy attached replicates most of the directions found within the City of Toronto's "E-Mail Policy" and is more detailed with respect to the responsibilities of Board employees in relation to use of the corporate electronic mail system.

Contact:
Fatima Scagnol
Corporate Secretary
Tel: 416-263-3620
Fax: 416-263-3690
Email: FScagnol@explace.on.ca

_____
Dianne Young
Chief Executive Officer

1. Purpose

The purpose of this policy is to govern the use of the corporate electronic (e-mail) system.

2. Application

This policy applies to "Authorized Users" including "Remote Access Users" who access the electronic mail system through a local connection or by remote access.

3. Definitions

- **"Archiving Messages"** in an electronic mail context occurs when a message is removed from the on-line mailbox and stored on another storage device.

- **"Authorized Users"** means individuals who have been given permission to use the Board's information and technology resources as defined and includes Remote Access Users as defined.

- "**Board"** means the Board of Governors of Exhibition Place.

- **"Chief Executive Officer"** means the CEO appointed by the Board.

- **"Chief Financial Officer"** means the CFO appointed by the Board.

- **"City Solicitor"** means the Solicitor of the Board appointed by the City of Toronto.

- **"Corporate Record"** is an e-mail that shows evidence of a business transaction, decision or the sharing of corporate information in the course of daily business operations and provisions of services.

- **"Data Transfer"** means the movement of information or data from one information technology resource to another regardless of the method of transfer.

- **"E-mail"** and **"Electronic Mail"** will be used interchangeably. Electronic mail, often referred to as e-mail, is a paperless form of communication. E-mail includes anything that is in a user's Board mailbox, this could include: messages (including attachment), appointments, tasks, notes, phone messages and address book information.

- **"Forging"** an e-mail is using an unauthorized or false name to send mail, altering a message or creating a false status response.

- **"Information and Technology Resources"** (I&T Resources) include, but are not limited to: desktop computers, monitors, printers, notebooks, tablet computers, handheld computers, scanners; computer peripherals such as: CDRW drives, DVDRW drives, zip drives, digital projectors; peripherals such as: storage devices and power supplies; personal digital assistants (PDA's); network devices; software such as: Corporate

software, off-the-shelf software packages, software covered by enterprise license agreements and volume license agreements (including maintenance and support); data created using any of the Board's I&T Resources; Internet access; e-mail; telephones and voice mail; facsimile machines (if connected to the Board's computer network); photocopiers (if connected to the Board's computer network); and mobile devices.

- **"Information & Technology"** and **"I&T"** will be used interchangeably.

- ***Municipal Freedom of Information and Protection Privacy Act*** and ***Personal Health Information Act*** will be referred to as the *Acts.*

- **"Personal Information"** (and personal health information) means recorded information about an identifiable individual. For a more detailed definition, refer to the *Municipal Freedom of Information and Protection of Privacy Act*.

- **"Records"** are information however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and includes documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings and photographs.

- **"Remote Access Users"** are Authorized Users who have permission, by way of an authorized form with an explanation from a Senior Manager to the CFO, wherein access to the Board's internal network from a remote location outside of the normal office environment regardless of the connectivity method.

- **"Transitory Mail"** is typically information that has a temporary usefulness and does not need to be kept once immediate usage has expired. Transitory mail is information not required to document Board business.

- **"User Monitoring"** means recording, accessing, and reviewing or analyzing a User's activity on, or use of, the Board's I&T Resources, and may include review of data files, e-mails, and information sent from, received by, or stored on the Board's I&T Resources, including data, files, e-mails, and information deleted by a User but backed up by the Board's network system.

4. Policy

4.1 General

- All Authorized Users must comply with this policy.
- All Authorized Users are responsible for their use of the corporate e-mail system during business hours and non-business hours.
- All Authorized Users are responsible for managing their e-mail.
- All information created, acquired, or maintained by Authorized Users of the Board is deemed to be a corporate asset and as such is the property of the Board.
- All Authorized Users must take reasonable measures to ensure that e-mail is not transmitted to unnecessary or unintended recipients.
- Reassigning ownership of a generic mailbox (e.g. help@explace.on.ca) must be approved by the Senior Manager of the department that owns the account and the request, in writing, must be sent to the CFO.
- Requests to create, modify, suspend or delete an e-mail account must be made by the Senior Manager of the department and sent to the CFO.

- Only the Manager of IT/Telecom, or designates can create, on the direction of the CFO, create, modify, suspend or delete e-mail accounts.
- Requests to access an employee's e-mail account for business purposes without their knowledge must be made in writing to the CFO by the employee's Senior Manager.

4.2 **Inactive Accounts**

All Authorized Users are required to make reasonable efforts to ensure that their business related e-mails have been managed appropriately prior to their account being an inactive (i.e. leaving their employment with the Board, extended leaves, etc.).

In addition, Senior Managers should also confirm with the Authorized User that business-related e-mails have been archived appropriately prior to the account being recorded as inactive.

4.3 **Prohibited Uses or Unlawful and Unacceptable Use**

All Authorized Users are expected to use e-mail as a business tool and carefully consider the implications of their actions prior to using the e-mail system and if uncertain, should contact their Senior Manager or IT/Telecom for advice and clarification.

In addition to the prohibited and unacceptable uses described in the Board's "Information and Technology Acceptable Use Policy", e-mail specific prohibited and unacceptable uses include, but are not limited to the following:

- Transmission of an anonymous e-mail is not permitted;
- Forging any part of an e-mail is not permitted;
- Sending personal "broadcasting messages" is not permitted;
- The creation of a rule to automatically reply to Internet e-mail messages is not permitted unless authorization has been received or the e-mail account was created to satisfy business requirements and the e-mail address has been published for the convenience of the general public; and
- The creation of a rule to automatically forward e-mail is not permitted.

5. <u>Managing E-Mail Records</u>

- The management of the Board's e-mail is consistent with the Board's Records Management Policy.
- Business-related e-mail messages are considered Board records, while informal, transitory and spam e-mail messages are not considered records
- E-Mail (i.e. the message header, message content, attachments and messaging context information) is a corporate record when it shows evidence of a business transaction, decision or the sharing of corporate information in the course of daily business operations and provisions of services.
- Authorized Users sending or receiving business-related e-mail must recognize their importance as records and take appropriate actions to manage them responsibly.
- *The Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA) apply to e-mail records.

<u>Note</u> – The e-mail system does not have the capability to act as a records retention system and therefore should not be considered a document/records management system.

6. Confidentiality and Privacy Consideration

6.1 Confidentiality (MFIPPA *Act*)

The Municipal Freedom of Information and Protection of Privacy Act provides any person with a legal right of access, to any record in the Board's custody or control, regardless of media or format, limited by specific mandatory and discretionary exemptions.

Every authorized e-mail user must consider the consequences of:

- sending personal/sensitive information to the wrong e-mail account; and
- a privacy breach should an unauthorized user or third-party intercept and read the e-mail message.

All authorized users are responsible for using appropriate safeguards when sending and receiving sensitive personal or confidential information by e-mail. All authorized users must balance the need to protect personal information, against the urgency and business need for sending the information by e-mail. Users must consider using alternative forms of communication (e.g. verbal or hard copy) when dealing with sensitive business, refer to the person as the "employee" or "client" instead of using his/her name.

6.2 Employee Authorization

An employee may grant permission to authorized staff to access their mailbox to facilitate the resolution of problems.

6.3 Business Requirement

Directors/Managers or higher may access an employee's e-mail account when:

- Management needs to temporarily perform the duties of an employee when he/she is ill or to resolve a business crisis when the employee can not be reached.
- The Board is required by law to supply records of correspondence on a particular matter.

Note: - In the above instances, should a user's e-mail account be accessed, the user will be notified by the Director/Manager as soon as possible.

Refer to the Information & Technology Acceptable Use Policy on Privacy Considerations and User Monitoring for guidance on any business requirements not outlined here.

6.4 Protection of the Integrity of the Electronic Mail System

The Manager of IT/Telecom, upon the direction of the CFO, has the right to access an e-mail account if the account poses a threat to the integrity of the e-mail system.

7. Consequences of Non-compliance

Failure to comply with this policy may result in disciplinary action up to and including dismissal.

8. Roles & Responsibilities:

9.1 All Authorized Users are responsible for:

- Reading, understanding and complying with the E-Mail Policy

- All e-mail sent under their name
- Protecting their passwords
- Using e-mail responsibly and appropriately
- Guarding against unauthorized access to their e-mail account by closing the e-mail account when away from their desk and when leaving at the end of the business day
- Managing mailbox size by identifying and deleting personal and transitory messages regularly
- Requesting clarification through their senior manager if they have any concerns regarding compliance

9.2 **Directors/Managers are responsible for**:

- Ensuring Authorized Users have read the E-Mail Policy
- Being the first point of contact for Authorized Users to seek clarification of this policy
- Performing initial investigation of suspected E-Mail Policy violations and reporting to the CFO
- Reassigning ownership of generic e-mail accounts and public distribution lists, if designated owner is no longer able to perform the role
- Authorizing the creation of e-mail accounts, requesting timely removal of access and deletions for temporary or contracted users

9.3 **Information & Technology Authorized Staff is responsible for**:

- Handling requests to create, modify, enable, disable or delete e-mail accounts
- Providing instructions for using the features of the e-mail system
- Resetting passwords for e-mail accounts

9.4 **Information & Technology Manager, as directed by the CFO, is responsible for**:

- The security and integrity of the e-mail system
- Accessing e-mail accounts if the account poses a threat to the integrity of the e-mail system
- Accessing e-mail accounts if authorized by an employee to resolve a technical problem
- Notifying the user as soon as possible if their account has been accessed unless there is an investigation underway
- Creating, modifying, enabling/disabling and deleting e-mail accounts
- Tracking unused or dormant accounts

9.5 **Board's Representative re Corporate Access & Privacy is responsible for**:

- Providing advice and direction regarding the legal rights of access to information and privacy protection contained in the MFIPPA and PHIPA *Acts*

9.6 **CEO and CFO are responsible for**:

- Authorizing and requesting access to e-mail messages and file attachments, if there is a legitimate need to do so or when investigating misuse or violation of this policy

9. Related Board Policies and Applicable Legislation

Board Policies

- Conflict of Interest/Code of Conduct
- Fraud & Other Similar Irregularities

Applicable Legislation

- Canadian Charter of Rights and Freedoms
- Canadian Human Rights *Act*
- Municipal Freedom of Information and Protection of Privacy *Act* (MFIPPA)
- Ontario Human Rights Code