INFORMATION MANAGEMENT AND SECURITY STANDARD

Electronic Communications

Approved By: **Information Management and Security Governance Committee**
Effective Date: **2018/06/18**
Next Revision Due: **2021/06/18**
Department / BU: **Information Technology, Corporate Security**

GENERAL

This standard is an extension of the Information Management and Security Policy. Consequences of non-compliance with this standard are outlined in the Policy.

PURPOSE

The City encourages the use of electronic communication and recognizes these communication tools are vital to day-to-day business activity. The purpose of this standard is to:

- Ensure that City electronic communications are used appropriately to reduce the risk of loss, corruption and mismanagement of information stored in The City's electronic communication systems;
- Prevent disruptions to and misuse of the City's electronic communication resources and systems.

SCOPE

The electronic communication systems are the property of The City of Calgary and may only be used by authorized users.

This standard applies to:

- All electronic communication resources owned or managed by The City;
- All users and uses of the electronic communication systems and resources.

This standard applies to all electronic communications, including attachments and transactional information associated with those communications. These records are considered information assets and authorized users must comply with the Information Management and Security Policy and Standards as well as the Records Management Program.

ELECTRONIC COMMUNICATION

Electronic communication is vital in conducting business at The City and must be used appropriately and securely. An electronic communication system includes, but is not limited to:

- Email;
- Text, instant messages, Skype for Business;
- Voicemail

APPROPRIATE USE

At all times, authorized users have a responsibility to use these systems in a professional, ethical and lawful manner. Users are expected to abide by all City Administration Policies and ensure that they conduct themselves professionally and appropriately at all times.

Users represent The City and therefore should not use City systems to distribute:

- any material that may damage the reputation of The City, its operations or its employees;
- material that would infringe copyright or intellectual property rights;
- junk mail, chain letters, jokes, promotions, commercial or political advertising material or other messages that would be considered unsolicited “spam”;
- offensive, obscene or indecent images or data;
- defamatory material;
- material that would, by intent or otherwise, harass the recipient;
- messages that are intended to disrupt or harm others, including viruses or other self-replicating code.

TEXT / INSTANT MESSAGES AND SKYPE FOR BUSINESS

Text / instant messages and Skype are not to be used to create official City records. If a message is received that is evidence of a business transaction, decision or activity, create an official record by either:

- Copying and pasting or taking a screen shot and storing it in an official repository and managing it according to the Corporate Records Management Program;
- Creating a record which captures the transaction, decision or activity and managing it according to the Corporate Records Management program.

EMAILS

Email messages (including attachments) created, received or transmitted by all users are considered a record and must be managed in accordance with all applicable City policies, standards, guidelines and practices with respect to Information Management, Information Security and the Corporate Records Management Program.

Authorized users will routinely identify and delete transitory email (immediate or short-term usefulness, personal mail or junk mail) within 90 days of the received or creation date. Email that serves a temporary business use (transitory record) may be retained for up to 24 months. The authorized user is responsible for moving it, with attachments, to an alternative location (shared drive, home drive, SharePoint Site, Livelink / Content Server, email subfolder) and clearly labeling it as transitory.

Where deemed appropriate and necessary, The City may employ electronic culling and / or automatic deletion of transitory email (such as *All Employee Notices*).

Email, with attachments, that has been identified as an official record (provides evidence of a business transaction, decision or activity and has legal, operational, fiscal or archival value) must be stored and managed in accordance with The City's Corporate Records Management Program requirements. The authorized user is responsible for moving it, with attachments, to one of the following:

- The City's document and records management system (Livelink / Content Server)
- A folder in a network location that is labeled with the records management requirements (meaningful title, Records Management Classification Code and Date), where the file format is maintained
- A subfolder in the email system that is labeled with the records management requirements (meaningful title, Records Management Classification Code and Date)

Authorized users will not use personal e-mail accounts to conduct City business. Authorized users will not forward or store City records in personal e-mail accounts or unauthorized cloud storage systems.

COMMERCIAL ELECTRONIC MESSAGES

Users who create and send commerical electronic messages (CEMs) are required to comply with Canadian Anti-Spam Legislation (CASL). A CEM is any electronic communication (email or text) that promotes a commercial activity. The term "commercial" is defined broadly to include the provision of any business or gaming opportunity or promotion of the barter or sale of a product, goods, services or land, even with no expectation of a profit. Some examples that may be captured are: promotion of events where commercial activities will be present, recreation activities or rentals or transit.

If a user is sending CEMs, they must be able to document that the recipient has already consented to receiving this information. Requests for consent must be managed in the way prescribed by the regulations and must include all required information. Each CEM must also contain required information and an opt-out feature as set out in CASL. Proof of consent and all other compliance evidence must be kept and managed in accordance with the Corporate Records Management Program.

VOICEMAIL

All voicemail is considered transitory. The City does not retain audio records of voicemail for City phones (mobile or landline).

Users who utilize Voice to Text should refer to the instructions above on managing text / instant messaging.

PRIVACY

As per the *Acceptable Use of City Technology Resources Policy,* users should understand they have no expectation of privacy with respect to their use of The City's electronic communications.

The City may be required to examine or disclose business communication held within The City's electronic communication system and / or logs for the following purposes:

- as part of an authorized investigation into a breach of City policy, procedure or violation of The Code of Conduct;
- to investigate an allegation of fraud or other illegal behaviors;
- as part of an ongoing or pending claim or litigation;
- as part of an ongoing or pending access to information request filed under the Freedom of Information and Protection of Privacy (FOIP) Act.

Examination and collection of information contained in The City's electronic communication system and / or logs will only be done in accordance with proper procedures and practices. The account holder may or may not be notified that The City, or a designated individual, will be examining or collecting their business communication.

A user who accesses an authorized user's account in bad faith or beyond the scope of his / her duties may be subject to disciplinary action.

Users are prohibited from seeking out, using or disclosing personal information in electronic communications without authorization. Authorized users are required under the FOIP Act to take necessary precautions to protect the confidentiality of personal information encountered either in the performance of their duties or otherwise, including within electronic communications.

SECURITY

The City makes reasonable efforts to provide secure and reliable electronic communication services. Authorized users should use reasonable care to ensure that their use of the electronic communication system does not compromise the security of the City network. User should exercise caution when opening unsolicited or suspect messages.

Authorized users shall not attempt to breach or undermine any security mechanism that protects electronic communication services or any records or messages associated with these services.

The City and its authorized individuals may monitor equipment, systems and electronic message traffic at any time for security and network maintenance purposes and to ensure the effective operation of the system.

Electronic communication should not be considered a secure form of communication. All authorized users will ensure that any information sent via electronic communication complies with the *Information Classification Standard*. Authorized users will only use encryption techniques approved by the Chief Security Officer.

BACK-UP

The City maintains back-ups of email, but not all of the other communication systems, these back-ups are created to assure system integrity and reliability, not to provide for future retrieval.

ACCOUNT MANAGEMENT

An authorized user's access to electronic communication systems will be terminated when the employment or contract ends. Access will be granted to the appropriate leader to review that user's accounts to prevent loss of official records.

Once a review has been completed and the appropriate leader authorizes it, the account can be terminated. Once an account has been deleted, it is no longer available and cannot be restored.

In the event of an unexpected or extended absence, access will be granted to the appropriate leader to e-mail or voicemail systems as required to maintain normal business operations.

RESOURCES

Refer to the Administration Policy Library for the following:

Information Management and Security Policy

Corporate Records Management Policies and Program

REVISION HISTORY

Review Date	Description
< 2018 / 06 / 18 >	New Electronic Communications Standard reviewed and approved by Information Management and Security Governance Committee.