BRAMPTON

Report
Staff Report
The Corporation of the City of Brampton
2021-01-14

Date: 2021-01-14

Subject: **Email, Files and Meeting Platforms**

Contact: Kumanan Gopalasamy, CIO Digital Innovation & Information Technology Division, Corporate Service (905) 874-2018

Report Number: Corporate Support Services-2021-111

Recommendations:
That the City email and electronic files security and electronic meeting platforms report dated January 14th 2021 be received to provide Council information on these systems.

Overview:

- Exchange Online is the City email system which provides a secure environment for emails. There is the ability for individuals to securely grant delegate access to their email and calendar.
- The City has provided secure storage of electronic documents for both Political Records and Constituent Records. There is functionality to allow documents to be safely shared with other individuals both within and external to the City.
- Electronic meeting platforms of Microsoft Teams and Cisco WebEx have been licensed and configured to enable both Internal and External collaboration. Other meeting platforms exist, but are not officially supported by City staff.

Background:

There are two fundamental aspects which impact the security of email, files and meeting communication.

1. Unauthorized access to information
    a. Communication intercepted
    b. Incorrect delegated authority
    c. Privileged administrative access

2. Loss of information
    a. Equipment (laptop, mobile device, USB drive) lost or stolen
    b. Malicious damage (e.g. Ransomware encryption) of files
    c. Document inadvertently overwritten or deleted

Current Situation:

Email

To mitigate communication being intercepted, Microsoft Exchange Online (email platform) provides encryption.

- All data is encrypted at rest. “Data at rest” refers to data that is not actively in transit and Exchange Online encrypts emails stored in secure data centers.
- Exchange Online encrypts communication going to and coming from the client.
- Email to other organizations is less straightforward. The email protocol does not require encryption but supports it. Exchange Online will always try to send and receive email over encrypted channels. If another organization does not allow encryption, the email will be sent in plain text.

Council and staff should not send sensitive information via email particularly with external parties, as there is the potential for this communication to be intercepted.

Council and staff have the ability to delegate access to their Email and Calendars to other staff without IT involvement. To ensure only authorized persons have delegated rights, this list should be reviewed on a regular basis. There are three types of access:

1. Reviewer (Can read items);
2. Author (Can read and create items); and
3. Editor (Can read, create and modify items).

Each of these levels of access can be applied to the Calendar, Tasks, Inbox, Contacts and Notes. Detailed instructions on managing Outlook Delegate Access can be found in the IT Service Catalog for Email and Calendar.

IT administrators have elevated access for enterprise email support. There are a number of controls in place to mitigate unauthorized access.

1. Administrative Accounts are restricted to a limited number of administrators.
2. Any administrator granting permissions is recorded in audit logs and appropriate notifications are sent to other designated staff to review and monitor.
3. Processes are in place requiring written authorization for any activities such as Freedom of Information (FOI) or Legal review.

An advantage of using Exchange Online is that email can be accessed anywhere with access to the Internet. Council and staff should refrain from extracting and saving emails to local or portable drives as this increases the risk of unauthorized access to their content.

The City of Brampton has implemented mitigating controls against the risk of emails being lost due to corruption, ransomware or accidental deletion by having appropriate backups. Nightly backups have the ability to reduce the loss of information to within 24 hours.

Electronic Files

While it is possible to save documents to numerous places, Council and staff should adhere to best practices detailed by Records and Information Management to ensure the security, integrity and retention of records.

Political Records and Constituent Records should be saved into the appropriate SharePoint Team Site in alignment with guidelines detailed in the Access to Information Service Card. This ensures that records are backed up and access is restricted to only authorized individuals.

If files need to be shared with internal / external parties, OneDrive has additional features and protections over local drives or portable drives. Council and staff should be cognizant that files stored on local drives or portable drives are at a higher risk of being lost through file corruption, theft or damaged by malware.

Electronic file access between the client computer and SharePoint Team Sites or OneDrive uses encryption to protect the contents of these documents from being intercepted.

Documents within SharePoint and OneDrive can be shared with others and this should be reviewed on a regular basis to ensure only authorized staff have access. Any file access, (including administrative accounts) is logged and can be audited.

Files saved on City of Brampton issued computers are encrypted and cannot be accessed without a valid City of Brampton network account, even in the event a device was stolen and the hard drive removed from the computer.

Training for SharePoint Team Sites and OneDrive is available by request.

Electronic Meeting Platforms

There are two City of Brampton supported online meeting platforms.

1. Teams
   The standard platform for all internal meetings (up to 250 participants)

2. WebEx
   Training (up to 1000 participants) with breakout rooms
   Events (up to 3000 participants)

Both of these meeting platforms have a number of security related features that staff should use to manage how meetings are run.

- Meeting lobby – ability to restrict access into the meeting.
- Meeting participants – ability to view who is in the meeting.
- Video – ability to see the participants if they enable their video.

- Backgrounds – the ability to blur or change the background so other participants cannot see the room of the participant.
- Recording of the Session – The session can have recording enabled, all other participants will be notified if this is enabled.
- End-to-end encryption – the meeting is encrypted and unauthorized 3rd parties have no ability to intercept any information within these platforms.

WebEx also has the following additional features:

- Live streaming with social media
- Managed participant registration

Features and functionality continue to be added to these meeting platforms to increase their capabilities and the number of participants.

Corporate Implications:

Whilst the City of Brampton has the necessary tools and technology to provide a safe and secure environment for email and electronic files, some improvements have been identified around process and documentation to ensure consistency and compliance in the configuration and management of these systems.

Whilst the City of Brampton has settled on Microsoft Teams and Cisco WebEx as supported electronic meeting platforms, there are numerous other vendors and products available. Adoption of multiple platforms incurs additional expenses and requires upskilling of staff which adds further overheads. DI&IT can provide some assistance with other platforms such as Zoom, but do not have the experience or skills in place to provide full support.

Term of Council Priorities:

Management and support of these platforms enables Council and staff to work and collaborate efficiently as part of a well-run City.

Conclusion:

Email and Electronic Files

- There are multiple controls in place to secure and protect email and electronic files from unauthorized access.
- Emails and electronic files can be shared with others by the owner. Access to these repositories is managed and reviewed by the owner to ensure only authorized individuals have access.
- Administrative accounts can grant access to email and electronic files. Controls are in place to ensure that these rights are restricted to only authorized staff, and any changes are logged for audit purposes and notifications are sent.

Electronic Meeting Platforms

- Teams should be used for all internal meetings (unless more than 250 participants).
- WebEx should be used for external large events or where specific functionality is required that Teams does not have.
- The functionality and number of participants on both platforms continues to be enhanced.

Authored by: Douglas Elsmore	Reviewed by: Kumanan Gopalasamy
[Author/Principal Writer]	[Manager/Director]
Approved by: Michael Davidson	Submitted by: David Barrick
[Commissioner/Department Head]	[Chief Administrative Officer]

Attachments: