Information Data Security Standards

Effective Date:	March 14, 2022
Authority:	Hydro One Ombudsman
Next review date:	August 2022
Document Type:	Public

1. OVERVIEW STATEMENT

1.1 The Hydro One Ombudsman ("the Ombudsman") is committed to protecting the privacy of complainants who contact the Ombudsman's Office, including those who access the Ombudsman's website.

1.2 The Ombudsman's Office takes seriously the protection of confidential data and the safeguarding of complainant information. The protection of data from data loss or data leakage is a business requirement.

1.3 The Ombudsman's Office follows the industry standard for security management and to that extent, the Ombudsman may consult with and/or consider Hydro One's data governance policies or procedures that may inform the Ombudsman's data security standards and practices.

2. PURPOSE

2.1 The purpose of these Standards is to set out the process for maintaining the security and confidentiality of Ombudsman records and complainant data (electronic and hard copy).

3. SCOPE

3.1 These Standards apply to the Ombudsman's Office and anyone engaged by the Ombudsman to perform services.

4. DEFINITIONS

4.1 **"Data"** means any information regardless of the storage medium (e.g. paper, digital file, portable USB hard drive, recording device, CD, etc.) and regardless

of format (e.g. audio, video, text, etc.) that is the property of the Ombudsman. Data includes information on the Ombudsman Case Management System.

4.2 **"Hydro One"** means Hydro One Inc. and its subsidiaries (together referred to as "Hydro One")

4.3 **"OCMS"** means the Ombudsman Case Management System where complainant information is stored.

4.4 **"Ombudsman"** means the Hydro One Ombudsman.

4.5 **"Ombudsman's Office"** means the Hydro One Ombudsman and staff of the Ombudsman.

5. RESPONSIBILITIES

5.1 The Ombudsman's Office

5.1.1 The Ombudsman's Office is expected to comply with these Standards and ensure that it meets the confidentiality and data security obligations in all aspects of its work.

5.1.2 The Ombudsman's Office shall not send any confidential or sensitive complainant information via any computer system that is not controlled by the office.

5.1.3 The transmission of confidential information can only occur from an Ombudsman's Office authorized email account.

5.1.4 Confidential data contained on Ombudsman issued portable devices (e.g. laptops or cell phones) will remain in the care and custody of the Ombudsman's Office and not be left unattended in unsecure areas.

5.1.5 When not in use, the Ombudsman's Office's devices, paper documents or records, must be securely stored.

5.1.6 When transferring information on a portable device such as USB stick, information must be encrypted.

5.1.7 Confidential information should remain on the premises of the Ombudsman's Office unless authorized by the Ombudsman.

5.1.8 Anyone conducting work outside of the office using Ombudsman owned devices, must immediately upon returning to the office or as soon as possible thereafter, upload any data files to the OCMS or shared office drive and ensure the original data is deleted from the portable business device.

5.1.9 Personal devices should not be used to carry out the Ombudsman's Office's business.

5.1.10 Computers used by the Ombudsman's Office must have automatic screen locking after a short period of inactivity.

5.1.11 When any member of the Ombudsman's Office is working outside of the office, including working remotely, they are expected to:

5.1.11.1 Follow security protocols for ensuring that any data on Ombudsman owned property is kept secure;

5.1.11.2 Ensure conversations are held in a private and confidential manner;

5.1.11.3 Safely retain and maintain all data in a secure and confidential manner; and

5.1.11.4 Dispose of any transient records in a way that preserves confidentiality.

5.2 Other Parties Contracted by the Ombudsman

5.2.1 The Ombudsman will require that those who are hired to provide goods and services will comply with confidentiality and data security requirements as set out in these Standards.

6. ACCESS CONTROLS

6.1 The Ombudsman's Office uses computers that have been configured with the appropriate software and safeguards to protect data and confidentiality of information.

6.2 Portable business devices must be Ombudsman issued encrypted devices that cannot be copied or used by someone in the event of theft or accidental loss.

6.3 The Ombudsman's Office does not utilize cloud-based platforms (i.e. a network of remote servers hosted on the internet rather than on local servers or Ombudsman computers) for the sharing of information.

6.4 Strict access controls are in place requiring sign in on the Ombudsman's Office's devices, which are password protected.

6.4.1 Each member of the Ombudsman's Office has a unique user account and a complex passcode for accessing any complainant information on the OCMS or shared office drive.

6.4.2 A secure and unique password must be used and must not be used on other external systems or servers.

6.5 Any access to information marked as 'Confidential' will be limited to authorized personnel only whose role requires access to the information as determined by the Ombudsman.

6.6 Any visitors to the office will be escorted and accompanied at all times by a member of the Ombudsman's Office, and shall be restricted to the appropriate areas of the office.

6.7 Any member of the Ombudsman's Office who no longer works for the Ombudsman will be required to return all Ombudsman owned devices immediately.

7. SECURITY TRAINING

7.1. Periodically and as needed, the Ombudsman's Office will participate in data security training, compliance monitoring and/or auditing activities as may be required.

8. INCIDENT REPORTS

8.1. Suspected data security concerns or non-compliance with security requirements as outlined in these Standards should be immediately reported to the Ombudsman.

8.2. The Ombudsman must be promptly notified in the event that any Ombudsman owned device containing sensitive or confidential data is lost or misplaced (e.g. mobiles, laptops, etc.).

9. DISPOSAL OF CONFIDENTIAL DATA

9.1. The Ombudsman's Office shall comply with the Document Retention Standards. Documents or records that have met the required retention period and are identified for destruction, must be disposed of in accordance with standard business practice that ensures confidentiality of the data being disposed of.

9.2. The Ombudsman may determine the best method to be used for the destruction of any storage media (such as CDs, DVDs) as may be appropriate in the circumstances.

10. REVIEW OF STANDARDS AND PROCEDURES

10.1. These Standards will be reviewed and amended as may be required by the Ombudsman's Office. The Ombudsman's Office shall also update the procedures that accompany these Standards as needed.

11. RELATED DOCUMENTS

11.1. Other documents related to these Standards are noted below.

Related Document	Effective Date of Document	Applicable Sections
Security Code of Practice (Hydro One)	2019/11/06	ss. 5.6, 5.7 and 6.0
Security Policy (Hydro One)	July 31, 2019	ss. 1.1, 1.2.3 to 1.2.5
Document Retention Standards	March 14, 2022	ss. 5, 8, 9 and 10
Record Keeping Standards	March 14, 2022	ss. 5, 6, and 8-12.

Approval Date: March 3, 2022