Avaya Privacy Laws Compliance Guide:
Freedom of Information and Protection of Privacy Act and the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario)

At Avaya, security and privacy are of primary importance. Avaya is committed to building on its experience through leading edge technology solutions that enhance privacy, as well as cloud solutions that aim to deliver both security and privacy. This includes complying with local and regional privacy and security regulations and giving Avaya's customers the tools they need to be compliant with Canadian data protection regulations, including Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Avaya's commitment to privacy and security extends to implementing organization-wide policies and practices as well as physical and technical security measures aimed at promoting security and privacy of customer data, including personal information. As part of Avaya's Trust Center, Avaya publishes additional information about our security practices, including information about Avaya's certifications and accreditations. While Avaya prohibits the use of its services to breach privacy laws, Avaya cannot prevent all abuses of its services. Customers are responsible for their compliance with privacy laws and for ensuring their staff comply with privacy laws.

This document describes Avaya's privacy and security practices as they relate to personal information and how Avaya can help its public sector customers in Ontario with personal information under their control, comply with Ontario's public sector privacy laws. For information on Avaya's practices as they relate public sector organization's collection, use or disclose of personal health information, see Avaya's *Personal Health Information Protection Act* (Ontario) compliance guide.

1. What are FIPPA and MFIPPA?

FIPPA is Ontario's provincial public-sector privacy legislation. It regulates the collection, use, disclosure, retention and disposal of individuals' personal information in the custody or control of public provincial bodies and institutions. MFIPPA applies to all Ontario municipal corporations, local boards and commissions and regulates records in their custody or control. Both FIPPA and MFIPPA also address individuals' rights of access to information under the control of public institutions. Under these laws, personal information includes any recorded information about an identifiable individual.

2. How Avaya Helps Public Sector Customers Meet Their Obligations

Avaya has implemented privacy practices and technical and physical security measures to protect customer data, including personal information.

(a) Avaya's Privacy Practices to Help Public Sector Customers Meet Their Obligations

Avaya's privacy practices include:

- ensuring that Avaya complies with applicable laws, including FIPPA and MFIPPA when it collects, uses and discloses personal information on behalf of public bodies.

- assisting customers in complying with requirements to inform and explain to individuals how their personal information is collected, used or disclosed.

- enabling customers to respond to requests from individuals for access to or correction of personal information.

- only using and disclosing the personal information to which it has access in the course of providing services to the customer in accordance applicable laws, including FIPPA and MFIPPA, and the instructions of the customer, and informing customers of when it cannot comply with this practice.

- ensuring its employees or any person acting on its behalf are unable to access personal information unless they agree to comply with the same restrictions Avaya is subject to under FIPPA and MFIPPA.

- following instructions of customers to store, return or dispose of personal information in a secure manner (including, through transfer to the Archives of Ontario, where applicable), when the services are terminated.

- complying with data security breach notification requirements, notifying customers of any security breach of personal information (including in the event that personal information is stolen, lost or accessed by an unauthorized person) at the first reasonable opportunity and as required under its contracts with customers and assisting customers in complying with data breach notification obligations.

- assisting customers in taking reasonable steps to ensure personal information is accurate and up-to-date.

- assisting customers in complying with requests for access to a record or personal information.

- assisting customers in complying with their data retention/destruction requirements.

- committing to help customers meet their compliance audit requirements, including under FIPPA and MFIPPA.

- storing personal information in jurisdictions outside of Ontario only as permitted by applicable legislation, including FIPPA and MFIPPA. Upon request, Avaya can provide product-specific information regarding storage location.

(b) Avaya's Physical and Technical Measures to Help Public Sector Customers Meet Their Obligations

Avaya will protect personal information by employing procedures to meet the privacy and security requirements of FIPPA, MFIPPA and their respective regulations. Avaya's administrative, physical and technical measures to promote data privacy and security include:

- restricting physical access to customer data processing equipment, including by:
    - an electronic access control system,
    - 24/7 video recording of physical facilities,
    - intrusion detection or engaging on-premises security officers, and

- restricting access to various zones at its premises based on roles and periodically revalidating access.

- restricting logical access to customer data and processing equipment, including through:
  - unique user IDs for access with formal authorization processes and unique complex passwords,
  - role-based access, least-privileged access and need-to-know only access,
  - access logs,
  - multi-factor authentication of Avaya's VPN for remote access,
  - encrypted endpoints,
  - centrally monitored and updated anti-virus programs and regular anti-virus scans,
  - secure deletion and/or disposal of data, and
  - secure storage of backup media and testing backups.
- using secure communication channels and logging, including:
  - using VPN with a multi-factor authentication for remote access,
  - using firewalls with stateful inspection, default denial access rules, role-based and least-privileged access on a "need to know" basis, logging and alerting of access, an annual review, and
  - using encrypted email if this has been enabled by the customer, using TLS.

(c) Avaya's Data Breach Incident Response Team and Privacy Law Advisors

Avaya also has a Data Breach Incident Response Team (DBIRT) that provides leadership in the event of a data breach. This is a cross-functional team established with the specific purpose of responding to actual and suspected data breaches. The DBIRT operates according to Avaya's Data Breach Incident Response Plan, which provides a well-defined, organized, repeatable and documentable approach to efficiently and effectively respond to data breaches to minimize their impact on Avaya or third parties, including Avaya's customers.

Avaya also receives advice from a leading Canadian law firm on privacy law compliance.

3. Who to Contact about Avaya's Security and Privacy Practices

For any questions about Avaya's security and privacy practices, please contact:

Avaya Global Privacy Office
Email: dataprivacy@avaya.com