DATA PRIVACY & SECURITY POLICY

Management Consultant Consortium of North America

1. PURPOSE

The purpose of this Data Privacy & Security Policy is to establish clear guidelines for the secure disposal, retention, and management of personal identifiable information (PII) in compliance with Canadian privacy and security regulations, including but not limited to the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial privacy laws. This policy seeks to protect the privacy of individuals and businesses, prevent unauthorized access to sensitive information, and uphold our commitment to data security.

2. SCOPE

This policy applies to all employees, contractors, and third-party agents handling:

- Individual names
- Company names
- Physical addresses
- Email addresses
- Phone numbers
- IP addresses

It covers all forms of data, including physical documents, digital files, databases, and any media containing the aforementioned information.

3. Key Stakeholders

The stakeholders responsible for the implementation and compliance of this policy include:

- General Canadian Public whose personal information is collected and managed.
- Canadian Business Entities engaged in handling or processing personal data directly tied to citizens.

4. Compliance Requirements

This policy is designed to align and conform with:

- Personal Information Protection and Electronic Documents Act (PIPEDA).
- Provincial Privacy Laws, such as Quebec's Bill 64 and Alberta's Personal Information Protection Act (PIPA).
- Industry best practices related to secure information management to ensure data governance and confidentiality.

5. Roles and Responsibilities

a. Employees and Contractors

- Ensure compliance with this policy and proper handling of personal and business information.
- Follow the defined procedures for secure data disposal and adhere to training programs on data privacy.

b. Data Privacy Officers

- Enforce the guidelines established in this policy.
- Conduct audits to verify adherence to proper information disposition standards.
- Update the policy as needed to reflect changes in regulations or organizational needs

c. Third-Party Vendors

- Comply with all provisions of this policy.
- Provide documented proof of compliance and proper disposal practices when handling data on behalf of the organization.

6. Information Retention and Storage

- Minimum Retention Period:

PII should only be retained for the duration necessary to fulfill its intended purpose or as required by law.

- Secure Storage:

All PII must be stored in secured environments—this includes encrypted databases for electronic information and locked cabinets for physical records.

- Retention Schedule:

A formal retention schedule will clearly delineate the duration specific types of information are retained.

7. Information Disposal

All forms of PII must be securely disposed of once they have reached the end of their retention period or are deemed no longer relevant. Proper methods of disposal include:

a. Digital Data

- Use permanently destructive methods such as data wiping software compliant with ISO 27040 standards.
- Ensure that decommissioned hardware (e.g., desktops, laptops, servers) is securely wiped or physically destroyed.

b. Physical Documents

- Utilize shredding machines certified for cross-cut or micro-cut methods.
- Partner only with certified shredding vendors for large-scale disposal, ensuring they provide documentation of destruction.

c. Third-Party Disposal Services

- Third-party services must comply with all relevant Canadian laws and provide certificates of destruction.

8. Breach Response Protocol

If there is suspected or confirmed unauthorized access, improper disposal, or exposure of personal data, the organization will:

1. Immediately notify the Data Privacy Officer.
2. Investigate and assess the scope of the incident.
3. Inform affected individuals as required under PIPEDA.
4. Report the breach to the Office of the Privacy Commissioner of Canada within the mandated timeframes.
5. Implement remediation measures and update policies if the breach was caused by procedural gaps.

9. Training and Awareness

All employees and contractors must complete mandatory training on PII management, including retention and disposal best practices. Training modules will include PIPEDA compliance standards and the consequences of non-adherence.

10. Policy Review

The Information Disposition Policy will be reviewed and updated annually or as required by changes in federal or provincial regulations. Revisions to the policy must be approved by the Data Privacy Officer and circulated across stakeholders.

11. Penalties for Non-Compliance

Employees, contractors, or third-party vendors found in violation of this policy may face:

- Disciplinary action, up to and including termination of employment or the service contract.
- Reporting to regulatory authorities as required by Canadian privacy laws.
- Legal action to recover damages caused by non-compliance.

12. Contact for Questions

For any questions or concerns regarding this policy:

Data Privacy Officer
Email: jriley@apm.today
Phone: 587.899.6826

This policy is designed to protect both individuals and businesses while ensuring the secure and responsible handling of information in compliance with Canadian security and privacy regulations.

Jason Riley
MCCNA Chair

Date: 01/28/25

Management Consultant Consortium of North America