PBC COMMUNICATIONS INC. PRIVACY POLICY AND COMPLIANCE GUIDE

Note: This document complies with changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) and the proposed Consumer Privacy Protection Act (CPPA).

1. INTENT

The Personal Information Protection and Electronic Documents Act (PIPEDA) establishes rules to govern the collection, use, and disclosure of personal information in a manner that recognizes the right to privacy of individuals' personal information and the need for organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PBC Communications Inc. is committed to protecting and respecting the personal information of its customers, employees, business partners, and all other entities it interacts with in accordance with PIPEDA. This policy provides guidelines to ensure that PBC Communications Inc. remains compliant with PIPEDA requirements.

2. DEFINITIONS

- Breach of security safeguards: The loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.
- Personal information: Information about an identifiable individual.
- Security safeguards: Measures to protect personal information, including:
  - Physical measures: For example, locking filing cabinets and restricting access to offices.
  - Organizational measures: For example, security clearances and limiting access on a "need-to-know" basis.
- - Technological measures: For example, the use of passwords and encryption.
- Significant harm: Includes bodily harm; humiliation; damage to reputation or relationships; loss of employment, business, or professional opportunities; financial loss; identity theft; negative effects on a credit record; and damage to or loss of property.

3. GUIDELINES

COMPLIANCE

- Protecting personal information appropriately: Implementing robust security measures.
- Informing individuals why personal information is being collected: Providing clear and accessible privacy notices.
- Obtaining clear and explicit consent for collection and use: Using straightforward language and processes for consent.
- Allowing individuals to withdraw consent: Providing simple mechanisms for consent withdrawal.
- Using personal information only for its collected purposes: Ensuring data use aligns with stated purposes.
- Retaining personal information only as long as necessary: Establishing data retention schedules.
- Destroying personal information securely when no longer needed: Using methods like shredding and secure digital deletion.

- Ensuring personal information accuracy: Regularly updating and verifying information.
- Providing individuals access to their personal information and allowing corrections: Facilitating access and correction requests.
- Limiting access to authorized personnel: Restricting data access based on role necessity.
- Requiring consent before releasing personal information to third parties, except as legally permitted: Ensuring third-party disclosures are consented or legally justified.

BREACHES OF SECURITY SAFEGUARDS REPORTING

- The CEO coordinates the response and notifies the Privacy Commissioner of Canada and affected individuals promptly.
- PBC Communications Inc. maintains records of all breaches, documenting the incident, response, and mitigation steps.

NOTIFYING AFFECTED INDIVIDUALS

Factors determining significant harm include:

- Sensitivity of the personal information.
- Probability of misuse.

NOTIFICATIONS

- Description of the breach.
- Period of occurrence.
- Types of information involved.
- Steps taken to mitigate harm.
- Actions individuals can take to protect themselves.
- Contact information for further inquiries.

ADDITIONAL NOTIFICATIONS

PBC Communications Inc. may notify other organizations or government institutions to mitigate harm from a breach.

ACCOUNTABILITY AND TRAINING

Accountability: Designating a Privacy Officer (CEO) responsible for compliance and overseeing privacy practices.

Training: Regularly training employees on privacy policies, procedures, and their responsibilities.

POLICY REVIEW AND UPDATES

Review: Conducting annual reviews of privacy policies and practices.

Updates: Updating the policy as needed to reflect changes in regulations or business practices.