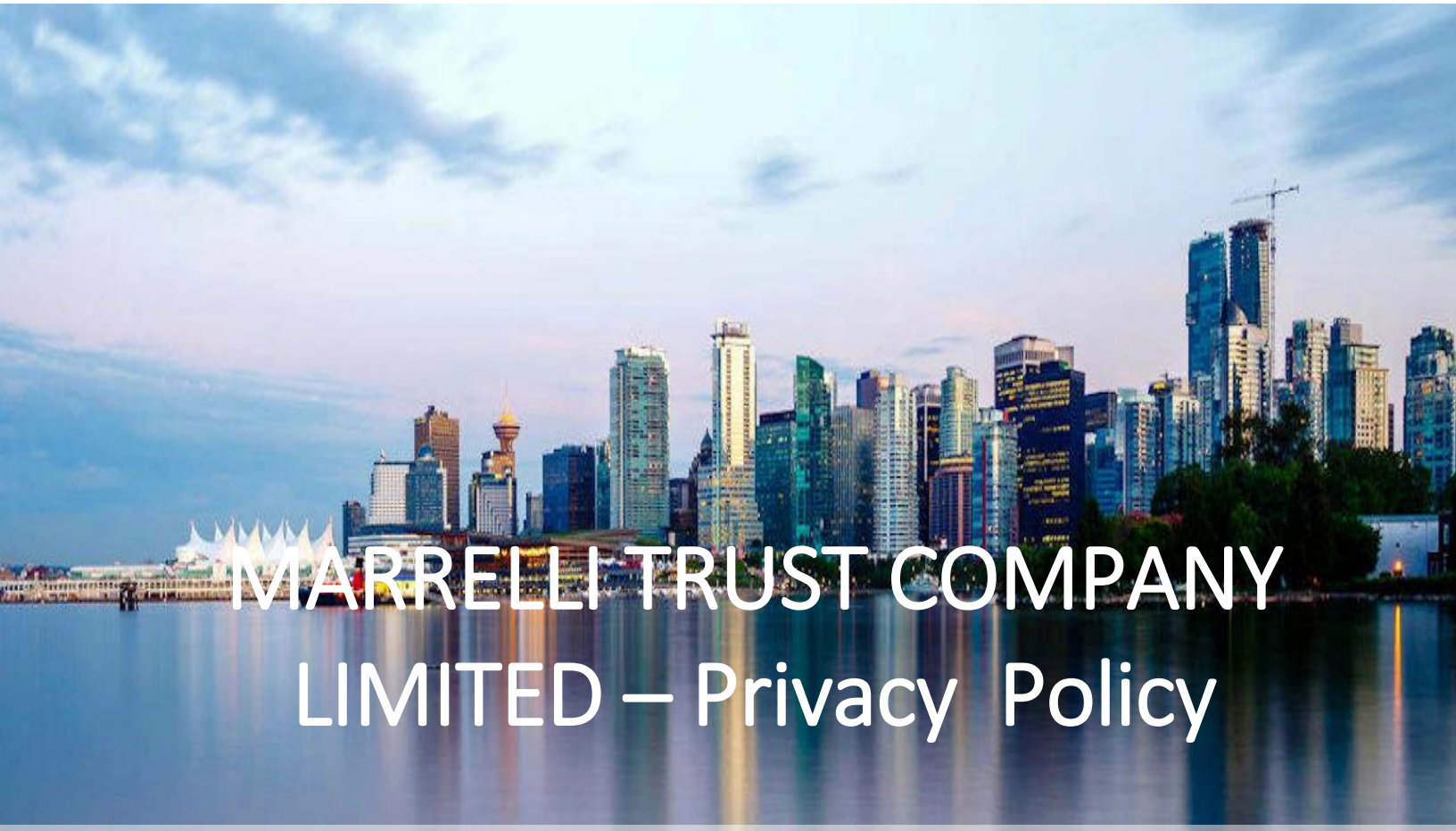

# MARRELLI TRUST COMPANY LIMITED – Privacy Policy

Version 3 – March 14, 2023

| | |
|---|---|
| **DOCUMENT CLASSIFICATION** | MTCL Confidential |
| **DOCUMENT REF** | PRIVACY POLICY |
| **VERSION** | 3 |
| **DATED** | 14 March 2023 |
| **DOCUMENT AUTHOR** | Lisa Cripps |
| **DOCUMENT OWNER** | Harvey Tan, Compliance Officer |

Revision history

| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
|---|---|---|---|
| 1 | December 19, 2019 | Lisa Cripps | Initial publication |
| 2 | March 18, 2022 | Lisa Cripps | Minor edits/ no significant changes |
| 3 | March 14, 2023 | Lisa Cripps | Minor edits/ no significant changes |

Distribution

| NAME | TITLE |
|---|---|
| | |
| | |

Approval

| NAME | POSITION | DATE |
|---|---|---|
| Harvey Tan | Compliance Officer | March 18, 2022 |
| Harvey Tan | Compliance Officer | March 14, 2023 |

# Contents

# What Is Privacy?

## Privacy Definition

Privacy is defined in Generally Accepted Privacy Principles as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information."

## Personal Information

Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom MTCL has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as nonpersonal information. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

## Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organization to organization and, in most cases, are driven by contractual arrangements.

## Generally Accepted Privacy Principles ("GAPP")

GAPP is designed to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities.

The privacy principles and criteria are founded on key concepts from significant local, national, and international privacy laws, regulations, guidelines, and good business practices. By using GAPP, MTCL can proactively address the significant challenges that they face in establishing and managing their privacy programs and risks from a business perspective. GAPP also facilitates the management of privacy risk on a multijurisdictional basis.

The privacy principles and criteria are founded on the following privacy objective.

- Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in *Generally Accepted Privacy Principles* issued by the AICPA and CICA.

The privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

The following are the 10 generally accepted privacy principles:

1. **Management.** MTCL defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** MTCL provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** MTCL describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** MTCL collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** MTCL limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. MTCL retains personal information for only as long as necessary to fulfill thestated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** MTCL provides individuals with access to their personal information for review and update.

7. **Disclosure to third parties.** MTCL discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** MTCL protects personal information against unauthorized access (both physical and logical).
9. **Quality.** MTCL maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** MTCL monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

# Management Criteria

## 1.0 The Marrelli Trust Company Limited ("MTCL") defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

### 1.1 Policies and Communications

#### 1.1.0 Privacy Policies

MTCL defines and documents its privacy policies with respect to the following:

- Notice (See 2.1.0)
- Choice and consent (See 3.1.0)
- Collection (See 4.1.0)
- Use, retention, and disposal (See 5.1.0)
- Access (See 6.1.0)
- Disclosure to third parties (See 7.1.0)
- Security for privacy (See 8.1.0)
- Quality (See 9.1.0)
- Monitoring and enforcement (See 10.1.0)

Privacy policies are documented in writing and made readily available to internal personnel and third parties who need them.

#### 1.1.1 Communication to Internal Personnel

Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to MTCL'S internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.

- MTCL periodically communicates to internal personnel relevant information about MTCL's privacy policies. Changes to its privacy policies are communicated shortly after approval.
- MTCL requires internal personnel to confirm (initially and periodically) their understanding of MTCL's privacy policies and their agreement to comply with them

#### 1.1.2 MTCL has assigned responsibility for privacy policies to the compliance officer.

The responsibility, authority, and accountability of compliance officer is clearly documented.

Responsibilities include the following:

- Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required
- Formulating and maintaining MTCL's privacy policies
- Monitoring and updating MTCL's privacy policies
- Delegating authority for enforcing MTCL's privacy policies
- Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices

Nominating & Corporate Governance Committee includes privacy periodically in its regular review of overall corporate governance.

## 1.2 Procedures and Controls

### 1.2.1 Review and Approval

Privacy policies and procedures, and changes thereto, are reviewed and approved by management.

Privacy policies and procedures are

- Reviewed and approved by senior management.
- Reviewed at least annually and updated as needed.

### 1.2.2 Consistency of Privacy Policies and Procedures with Laws and Regulations

Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.

Corporate Counsel

- Determines which privacy laws and regulations are applicable in the jurisdictions in which MTCL operates.
- Identifies other standards applicable to MTCL.
- Reviews MTCL’s privacy policies and procedures to ensure they are consistent with the applicable laws, regulations, and appropriate standards.

### 1.2.3 Personal Information Identification and Classification

The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by MTCL’s privacy and related security policies and procedures.

MTCL has both an information classification policy and process, which include the following:

- A classification process, which identifies and classifies information into one or more of the following categories:
    - Business confidential
    - Personal information (sensitive and other personal information)
    - Business general
    - Public
- Identifying processes, systems, and third parties that handle personal information

- Specific security and privacy policies and procedures that apply to each category of information

### 1.2.4 Risk Assessment

A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.

A process is in place to periodically identify the risks to MTCL's personal information. Such risks may be external (such as loss of information by vendors or failure to comply with regulatory requirements) or internal (such as e-mailing unprotected sensitive information).

When new or changed risks are identified, the privacy risk assessment and the response strategies are updated.

The process considers factors such as experience with privacy incident management, the complaint and dispute resolution process, and monitoring activities.

### 1.2.5 Consistency of Commitments with Privacy Policies and Procedures

Management reviews contracts for consistency with privacy policies and procedures and address any inconsistencies.

- Both management and the legal counsel review all contracts and service-level agreements for consistency with MTCL's privacy policies and procedures.

### 1.2.6 Infrastructure and Systems Management

The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:

- Infrastructure
- Systems
- Applications
- Websites
- Procedures
- Products and services
- Data bases and information repositories
- Mobile computing and other similar electronic devices

The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with MTCL's privacy policies and procedures.

The following are used for addressing privacy impact:

- Management assesses the privacy impact of new and significantly changed products, services, business processes, and infrastructure.
- MTCL uses a documented systems development and change management process for all information systems and related technology (including manual procedures, application programs, technology infrastructure, organizational structure, and the responsibilities of users and systems personnel), used to collect, use, retain, disclose, and destroy personal information.
- MTCL assesses planned new systems and changes for their potential effect on privacy.

- Changes to system components are tested to minimize the risk of any adverse effect on the protection of personal information. All test data are anonymized. A controlled test database is maintained for full regression testing to ensure that changes to one program do not adversely affect other programs that process personal information.
- Procedures ensure the maintenance of integrity and protection of personal information during migration from old to new or changed systems.
- Documentation and approval by the compliance officer, CEO, and IT management are required before implementing the changes to systems and procedures that handle personal information, including those that may affect security.
- Emergency changes are required to maintain the same level of protection of personal information; however, they may be documented and approved on an after-the-fact basis.
- The IT function maintains a listing of all software that processes personal information and the respective level, version, and patches that have been applied.
- Procedures exist to provide that only authorized, tested, and documented changes are made to the system.
- Where computerized systems are involved, appropriate procedures are followed, such as the use of separate development, test, and production libraries to ensure that access to personal information is appropriately restricted.
- Personnel responsible for initiating or implementing new systems and changes, and users of new or revised processes and applications, are provided training and awareness sessions related to privacy. Specific roles and responsibilities are assigned related to privacy.

### 1.2.7 Privacy Incident and Breach Management

A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:

- Procedures for the identification, management, and resolution of privacy incidents and breaches
- Defined responsibilities
- A process to identify incident severity and determine required actions and escalation procedures
- A process for complying with breach laws and regulations, including stakeholders breach notification, if required
- An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate
- A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following:
    - Incident patterns and root cause
    - Changes in the internal control environment or external requirements (regulation or legislation)
- Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed

A formal, comprehensive privacy incident and breach management program has been implemented, which specifies the following:

- Incidents and breaches are reported to a member of the breach team, who assesses if it is privacy or security related, or both, classifies the severity of the incident, initiates required actions, and determines the required involvement by individuals who are responsible for privacy and security.
- The Compliance Officer has the overall accountability for the program and is supported by the privacy and security steering committees and assisted by the breach team. Incidents and breaches that do not involve personal information are the responsibility of Bluemore Consulting.
- MTCL has a privacy breach notification policy, supported by

(a) a process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach,
(b) a process for assessing the need for stakeholders breach notification, if required by law, regulation, or policy, and (*c*) a process for delivering the notice in a timely manner. MTCL has agreements in place with a third party to manage the notification process and provide credit monitoring services for individuals, if needed.

- The program includes a clear escalation path, based on the type or severity, or both, of the incident, up to executive management, legal counsel, and the board.
- The program sets forth a process for contacting law enforcement, regulatory, or other authorities when necessary.
- Program training for new hires and team members, and awareness training for general staff, is conducted annually, when a significant change in the program is implemented, and after any major incident.

The privacy incident and breach management program also specifies the following:

After any major privacy incident, a formal incident evaluation is conducted by internal audit or outside consultants.

A quarterly review of actual incidents is conducted and required program updates are identified based on the following:

- Incident root cause
- Incident patterns
- Changes in the internal control environment and legislation
- Results of the quarterly review are reported to the Nominating & Corporate Governance Committee and annually to the Audit Committee.
- Key metrics are defined, tracked and reported to senior management on a quarterly basis.
- The program is tested at least every six months and shortly after the implementation of significant system or procedural changes.

### 1.2.8 Supporting Resources

- Resources are provided by MTCL to implement and support its privacy policies.
- Management annually reviews the assignment of personnel, budgets, and allocation of other resources to its privacy program.

### 1.2.9 Qualifications of Internal Personnel

MTCL establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.

The qualifications of internal personnel responsible for protecting the privacy and security of personal information are ensured by procedures such as the following:

- Formal job descriptions (including responsibilities, educational and professional requirements, and organizational reporting for key privacy management positions)
- Hiring procedures (including the comprehensive screening of credentials, background checks, and reference checking) and formal employment and confidentiality agreements
- Performance appraisals (performed by supervisors, including assessments of professional development activities)

### 1.2.10 Privacy Awareness and Training

A privacy awareness program about MTCL's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.

An interactive online privacy and security awareness course is required annually for all employees. New employees, contractors, and others are required to complete this course within the first month following employment in order to retain their access privileges.

In-depth training is provided which covers privacy and relevant security policies and procedures, legal and regulatory considerations, incident response, and related topics. Such training is

- required annually for all employees who have access to personal information or are responsible for protection of personal information.
- tailored to the employee's job responsibilities.
- supplemented by external training

Attendance at MTCL's privacy training and awareness courses is monitored.

Training and awareness courses are reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements.

### 1.2.11 Changes in Regulatory and Business Requirements

For each jurisdiction in which MTCL operates, the effect on privacy requirements from changes in the following factors is identified and addressed:

- Legal and regulatory
- Contracts, including service-level agreements
- Industry requirements
- Business operations and processes
- People, roles, and responsibilities
- Technology

Privacy policies and procedures are updated to reflect changes in requirements.

MTCL has an ongoing process in place to monitor, assess, and address the effect on privacy requirements from changes in the following:

- Legal and regulatory environments
- Industry requirements
- Contracts, including service-level agreements with third parties (changes that alter the privacy and security related clauses in contracts are reviewed and approved by the compliance officer or legal counsel before they are executed)
- Business operations and processes
- People assigned responsibility for privacy and security matters
- Technology (prior to implementation)

# Notice Criteria

## 2.0 MTCL provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

## 2.1 Policies and Communications

### 2.1.0 Privacy Policies

MTCL's privacy policies address providing notice to individuals.

### 2.1.1 Communication to Individuals

Notice is provided to individuals regarding the following privacy policies:

(a) Purpose for collecting personal information
(b) Choice and consent (See 3.1.1)
(c) Collection (See 4.1.1)
(d) Use, retention, and disposal (See 5.1.1)
(e) Access (See 6.1.1)
(f) Disclosure to third parties (See 7.1.1)
(g) Security for privacy (See 8.1.1)
(h) Quality (See 9.1.1)
(i) Monitoring and enforcement (See 10.1.1)

If personal information is collected from sources other than the individual, such sources are described in the notice.

MTCL's privacy notice

- describes the personal information collected, the sources of such information, and purposes for which it is collected.
- indicates the purpose for collecting sensitive personal information and whether such purpose is part of a legal requirement.
- describes the consequences, if any, of not providing the requested information.
- indicates that certain information may be developed about individuals, such as buying patterns.
- may be provided in various ways (for example, in a face-to-face conversation, on a telephone interview, on an application form or questionnaire, or electronically). However, written notice is the preferred method.

## 2.2 Procedures and Controls

### 2.2.1 Provision of Notice

Notice is provided to the individual about MTCL's privacy policies and procedures (*a*) at or before the time personal information is collected, or as soon as practical thereafter, (*b*) at or before MTCL changes its privacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.

- readily accessible and available when personal information is first collected from the individual.
- provided in a timely manner (that is, at or before the time personal information is collected, or as soon as practical thereafter) to enable individuals to decide whether or not to submit personal information to MTCL.
- clearly dated to allow individuals to determine whether the notice has changed since the last time they read it or since the last time they submitted personal information to MTCL

In addition, MTCL

- tracks previous iterations of MTCL's privacy policies and procedures.
- informs individuals of a change to a previously communicated privacy notice, for example, by posting the notification on MTCL's Web site, by sending written notice via postal mail, or by sending an e-mail.
- documents that changes to privacy policies and procedures were communicated to individuals.

### 2.2.2 Entities and Activities Covered

An objective description of the entities and activities covered by the privacy policies and procedures is included in MTCL's privacy notice. The privacy notice describes the particular entities, business segments, locations, and types of information covered, such as:

- Operating jurisdictions (British Columbia & Ontario)
- Business segments and affiliates
- Lines of business
- Types of third parties
- Types of information (for example, information about clients and shareholders)
- Sources of information

MTCL informs individuals when they might assume they ae covered by MTCL's privacy policies but, in fact, are no longer covered (for example, linking to another Web site that is similar to MTCL's, or using services on MTCL's premises provided by third parties).

### 2.2.3 Clear and Conspicuous

MTCL's privacy notice is conspicuous and uses clear language.

The privacy notice is

- in plain and simple language.
- appropriately labeled, easy to see, and not in unusually small print.
- linked to or displayed on the Web site at points of data collection.
- available in the national languages used on the site or in languages required by law

# Choice and Consent Criteria

## 3.0 MTCL describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

## 3.1 Policies and Communications

### 3.1.0 Privacy Policies

MTCL's privacy policies address the choices available to individuals and the consent to be obtained.

### 3.1.1 Communication to Individuals

Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.

MTCL's privacy notice describes, in a clear and concise manner, the following:

- The choices available to the individual regarding the collection, use, and disclosure of personal information
- The process an individual should follow to exercise these choices (for example, checking an opt out box to decline receiving marketing materials)
- The ability of, and process for, an individual to change contact preferences
- The consequences of failing to provide personal information required for a transaction or service

Individuals are advised of the following:

- Personal information not essential to the purposes identified in the privacy notice need not be provided.
- Preferences may be changed, and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice.

The type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from MTCL).

### 3.1.2 Consequences of Denying or Withdrawing Consent

When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.

At the time of collection, MTCL informs individuals of the following:

- About the consequences of refusing to provide personal information (for example, transactions may not be processed)
- About the consequences of denying or withdrawing consent (for example, opting out of receiving information about products and services may result in not being made aware of sales promotions)
- About how they will or will not be affected by failing to provide more than the minimum required personal information (for example, services will still be provided)

## 3.2 Procedures and Controls

### 3.2.1 Implicit or Explicit Consent

MTCL Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.

- obtains and documents an individual's consent in a timely manner (that is, at or before the time personal information is collected or soon after).
- confirms an individual's preferences (in writing or electronically).
- documents and manages changes to an individual's preferences.
- ensures that an individual's preferences are implemented in a timely fashion.

- addresses conflicts in the records about an individual's preferences by providing a process for users to notify and challenge a vendor's interpretation of their contact preferences.
- ensures that the use of personal information, throughout MTCL and by third parties, is in accordance with an individual's preferences.

### 3.2.2 Consent for New Purposes and Uses

If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.

When personal information is to be used for a purpose not previously specified, MTCL

- notifies the individual and documents the new purpose.
- obtains and documents consent or withdrawal of consent to use the personal information for the new purpose.
- ensures that personal information is being used in
- accordance with the new purpose or, if consent was withdrawn, not so used.

### 3.2.3 Explicit Consent for Sensitive Information

Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.

MTCL collects sensitive information only if the individual provides explicit consent. Explicit consent requires that the individual affirmatively agree, through some action, to the use or disclosure of the sensitive information. Explicit consent is obtained directly from the individual and documented, for example, by requiring the individual to check a box or sign a form. This is sometimes referred to as opt in.

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Schedule 1, clause 4.3.6, states that an organization should generally seek explicit consent when the information is likely to be considered sensitive.

Some jurisdictions consider government-issued personal identifiers, for example, Social Security numbers or Social Insurance numbers, to be sensitive information.

### 3.2.4 Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices

Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.

MTCL requests customer permission to store, alter, or copy personal information (other than cookies) in the customer's computer or other similar electronic device.

If the customer has indicated to MTCL that it does not want cookies, MTCL has controls to ensure that cookies are not stored on the customer's computer or other similar electronic device.

Entities will not download software that will transfer personal information without obtaining permission.

## Collection Criteria

# 4.0 MTCL collects personal information only for the purposes identified in the notice.

## 4.1 Policies and Communications

### 4.1.0 Privacy Policies

MTCL's privacy policies address the collection of personal information.

### 4.1.1 Communication to Individuals

Individuals are informed that personal information is collected only for the purposes identified in the notice.

MTCL's privacy notice discloses the types of personal information collected, the sources and methods used to collect personal information, and whether information is developed or acquired about individuals, such as buying patterns.

### 4.1.2Types of Personal Information Collected and Methods of Collection

The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.

Types of personal information collected include the following:

- Financial (for example, financial account information and share data)
- Social Insurance Numbers

Methods of collecting and third-party sources of personal information include the following:

- Credit reporting agencies
- Over the telephone
- Via the Internet using forms, cookies, or Web beacons

MTCL's privacy notice discloses whether it uses cookies and Web beacons and how they are used. The notice also describes the consequences if the cookie is refused.

## 4.2 Procedures and Controls

### 4.2.1 Collection Limited to Identified Purpose

The collection of personal information is limited to that necessary for the purposes identified in the notice.

Systems and procedures are in place to

- specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information.
- periodically review MTCL's program or service needs for personal information (for example, once every five years or when changes to the program or service are made).
- obtain explicit consent when sensitive personal information is collected (see 3.2.3, "Explicit Consent for Sensitive Information").
- monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice and that all optional data is identified as such.

#### 4.2.2 Collection by Fair and Lawful Means

Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained

(a) fairly, without intimidation or deception, and

(b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.

MTCL's management, privacy officer, and legal counsel, review the methods of collection and any changes thereto.

#### 4.2.3 Collection From Third Parties

Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.

MTCL

- performs due diligence before establishing a relationship with a third-party data provider.
- reviews the privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources.

Contracts include provisions requiring personal information to be collected fairly and lawfully and from reliable sources.

### 4.2.4 Information Developed about Individuals

Individuals are informed if MTCL develops or acquires additional information about them for its use.

MTCL's privacy notice indicates that, if applicable, it may develop and acquire information about the individual using third-party sources, browsing, credit and purchasing history, and so on.

# Use, Retention, and Disposal Criteria

## 5.0 MTCL limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. MTCL retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

## 5.1 Policies and Communications

#### 5.1.0 Privacy Policies

MTCL's privacy policies address the use, retention, and disposal of personal information.

5.1.1

Communication to Individuals Individuals are informed that personal information is (a) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (b) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.

MTCL's privacy notice describes the following uses of personal information, for example:

- Processing business transactions such as claims and warranties, payroll, taxes, benefits, stock options, bonuses, or other compensation schemes
- Addressing inquiries or complaints about products or services, or interacting during the promotion of products or services
- Product design and development, or purchasing of products or services
- Participation in scientific or medical research activities, marketing, surveys, or market analysis
- Personalization of Web sites or downloading software
- Legal requirements
- Direct marketing

MTCL's privacy notice explains that personal information will be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and thereafter will be disposed of securely or made anonymous so that it cannot be identified to any individual.

## 5.2 Procedures and Controls

### 5.2.1 Use of Personal Information

Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.

Systems and procedures are in place to ensure that personal information is used

- in conformity with the purposes identified in MTCL's privacy notice.
- in agreement with the consent received from the individual.
- in compliance with applicable laws and regulations.

### 5.2.2 Retention of Personal Information

Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.

MTCL

- documents its retention policies and disposal procedures.
- retains, stores, and disposes of archived and backup copies of records in accordance with its retention policies.
- ensures personal information is not kept beyond the standard retention time unless a justified business or legal reason for doing so exists.

Contractual requirements are considered when establishing retention practices when they may be exceptions to normal policies.

#### 5.2.3 Disposal, Destruction and Redaction of Personal Information

Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.

MTCL

- erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based).
- disposes of original, archived, backup and ad hoc or personal copies of records in accordance with its destruction policies.
- documents the disposal of personal information.
- within the limits of technology, locates and removes or redacts specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete.
- regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or as required by laws and regulations.

Contractual requirements are considered when establishing disposal, destruction, and redaction practices if they may result in exception to MTCL's normal policies.

# Access Criteria

## 6.0 MTCL provides individuals with access to their personal information for review and update.

### 6.1 Policies and Communications

#### 6.1.0 Privacy Policies

MTCL's privacy policies address providing individuals with access to their personal information.

#### 6.1.1 Communication to Individuals

Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.

MTCL's privacy notice

- explains how individuals may gain access to their personal information and any costs associated with obtaining such access.
- outlines the means by which individuals may update and correct their personal information (for example, in writing, by phone, by e-mail, or by using MTCL's Web site).
- explains how disagreements related to personal information may be resolved.

## 6.2 Procedures and Controls

### 6.2.1 Access by Individuals to Their Personal Information

Individuals are able to determine whether MTCL maintains personal information about them and, upon request, may obtain access to their personal information.

Procedures are in place to

- determine whether MTCL holds or controls personal information about an individual.
- communicate the steps to be taken to gain access to the personal information.
- respond to an individual's request on a timely basis.provide a copy of personal information, upon request, in printed or electronic form that is convenient to both the individual and MTCL.
- record requests for access and actions taken, including denial of access and unresolved complaints and disputes.

### 6.2.2 Confirmation of an Individual's Identity

The identity of individuals who request access to their personal information is authenticated before they are given access to that information.

Employees are adequately trained to authenticate the identity of individuals before granting the following:

- Access to their personal information
- Requests to change sensitive or other personal information (for example, to update information such as address or bank details)

MTCL

- mails information about a change request only to the address of record or, in the case of a change of address, to both the old and new addresses.
- requires that a unique user identification and password (or equivalent) be used to access user account information online.

### 6.2.3 Understandable Personal Information, Time Frame, and Cost

Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any. MTCL

- makes a reasonable effort to locate the personal information requested and, if personal information cannot be found, keeps sufficient records to demonstrate that a reasonable search was made.
- takes reasonable precautions to ensure that personal information released does not identify another person, directly or indirectly.
- provides access to personal information in a timeframe that is similar to MTCL's normal response times for other business transactions, or as permitted or required by law.
- provides access to personal information in archived or backup systems and media.
- informs individuals of the cost of access at the time the access request is made or as soon as practicable thereafter.
- charges the individual for access to personal information at an amount, if any, which is not excessive in relation to MTCL's cost of providing access.
- provides an appropriate physical space to inspect personal information.

### 6.2.4 Denial of Access

Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of MTCL's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.

MTCL

- outlines the reasons why access to personal information may be denied.
- records all denials of access and unresolved complaints and disputes.
- provides the individual with partial access in situations in which access to some of his or her personal information is justifiably denied.
- provides the individual with a written explanation about why access to personal information is denied.
- provides a formal escalation (appeal) process if access to personal information is denied.
- conveys MTCL's legal rights and the individual's right to challenge, if applicable.

### 6.2.5 Updating or Correcting Personal Information

Individuals are able to update or correct personal information held by MTCL. If practical and economically feasible to do so, MTCL provides such updated or corrected information to third parties that previously were provided with the individual's personal information.

MTCL

- describes the process an individual must follow to update or correct personal information records (for example, in writing, by phone, by e-mail, or by using MTCL's Web site).
- verifies the accuracy and completeness of personal information that an individual updates or changes (for example, by edit and validation controls, and forced completion of mandatory fields
- records the date, time, and identification of the person making the change if MTCL's employee is making a change on behalf of an individual.
- notifies third parties to whom personal information has been disclosed of amendments, erasures, or blocking of personal information, if it is possible and reasonable to do so.

### 6.2.6 Statement of Disagreement

Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.

If an individual and an entity disagree about whether personal information is complete and accurate, the individual may ask MTCL to accept a statement claiming that the personal information is not complete and accurate.

MTCL

- documents instances where an individual and MTCL disagree about whether personal information is complete and accurate.
- informs the individual, in writing, of the reason a request for correction of personal information is denied, citing the individual's right to appeal.
- informs the individual, when access to personal information is requested or when access is actually provided, that the statement of disagreement may include information about the nature of the change sought by
- the individual and the reason for its refusal by MTCL. if appropriate, notifies third parties who have previously been provided with personal information that there is a disagreement and the nature of the disagreement.

# Disclosure to Third Parties Criteria

## 7.0 MTCL discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

## 7.1 Policies and Communications

### 7.1.0 Privacy Policies

MTCL's privacy policies address the disclosure of personal information to third parties.

#### 7.1.1 Communication to Individuals

Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.

MTCL's privacy notice

- describes the practices related to the sharing of personal information (if any) with third parties and the reasons for information sharing.
- identifies third parties or classes of third parties to whom personal information is disclosed.
- informs individuals that personal information is disclosed to third parties only for the purposes (a) identified in the notice, and (b) for which the individual has provided implicit or explicit consent, or as specifically allowed or required by law or regulation.

MTCL's privacy notice may disclose the following:

- The process used to assure the privacy and security of personal information that has been disclosed to a third party
- How personal information shared with a third party will be kept up to date, so that outdated or incorrect information shared with a third party will be changed if the individual has changed his or her information

#### 7.1.2 Communication to Third Parties

Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.

Prior to sharing personal information with a third party, MTCL communicates its privacy policies or other specific instructions or requirements for handling personal information to, and obtains a written agreement from the third party that its privacy practices over the disclosed personal information adhere to those policies or requirements.

## 7.2 Procedures and Controls

#### 7.2.1 Disclosure of Personal Information

Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.

Systems and procedures are in place to

- prevent the disclosure of personal information to third parties unless an individual has given implicit or explicit consent for the disclosure.

- document the nature and extent of personal information disclosed to third parties.
- test whether disclosure to third parties is in compliance with MTCL's privacy policies and procedures, or as specifically allowed or required by law or regulation.
- document any third-party disclosures for legal reasons.

### 7.2.2 Protection of Personal Information

Personal information is disclosed only to third parties who have agreements with MTCL to protect personal information in a manner consistent with the relevant aspects of MTCL's privacy policies or other specific instructions or requirements. MTCL has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.

When providing personal information to third parties, MTCL enters into contracts that require a level of protection of personal information equivalent to that of MTCL's. In doing so, MTCL

- limits the third party's use of personal information to purposes necessary to fulfill the contract.
- communicates the individual's preferences to the third party.
- refers any requests for access or complaints about the personal information transferred by the
- entity to a designated privacy executive, such as a corporate privacy officer.
- specifies how and when third parties are to dispose of or return any personal information provided by MTCL.

MTCL evaluates compliance with such contract using one or more of the following approaches to obtain an increasing level of assurance depending on its risk assessment:

- The third party responds to a questionnaire about their practices.
- The third party self-certifies that its practices meet MTCL's requirements based on internal audit reports or other procedures.
- MTCL performs an onsite evaluation of the third party.
- MTCL receives an audit or similar report provided by an independent auditor.

### 7.2.3 New Purposes and Uses

Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.

Systems and procedures are in place to

- notify individuals and obtain their consent prior to disclosing personal information to a third party for purposes not identified in the privacy notice.
- document whether MTCL has notified the individual and received the individual's consent.
- monitor that personal information is being provided to third party specified in the privacy notice.

### 7.2.4 Misuse of Personal Information by a Third Party

MTCL takes remedial action in response to misuse of personal information by a third party to whom MTCL has transferred such information.

MTCL

- reviews complaints to identify indications of any misuse of personal information by third parties.
- responds to any knowledge of a third party using or disclosing personal information in variance with MTCL's privacy policies and procedures or contractual arrangements.

- mitigates, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of MTCL's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void affected numbers and reissue new numbers).
- takes remedial action in the event that a third party misuses personal information (for example, contractual clauses address the ramification of misuse of personal information).

# Security for Privacy Criteria

## 8.0 MTCL protects personal information against unauthorized access (both physical and logical).

## 8.1 Policies and Communications

### 8.1.0 Privacy Policies

MTCL's privacy policies (including any relevant security policies), address the security of personal information.

Privacy policies adequately address security measures to safeguard the privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal informationbe protected.

### 8.1.1 Communication to Individuals

Individuals are informed that precautions are taken to protect personal information.

MTCL's privacy notice describes the general types of security measures used to protect the individual's personal information, for example:

- Employees are authorized to access personal information based on job responsibilities.
- Authentication is used to prevent unauthorized access to personal information stored electronically.
- Physical security is maintained over personal information stored in hard copy form, and encryption is used to prevent unauthorized access to personal information sent over the Internet.
- Additional security safeguards are applied to sensitive information.

## 8.2 Procedures and Controls

### 8.2.1 Information Security Program

A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas3 insofar as they relate to the security of personal information:

(a) Risk assessment and treatment [1.2.4]
(b) Security policy [8.1.0]
(c) Organization of information security [sections 1, 7, and 10]
(d) Asset management [section 1]
(e) Human resources security [section 1]
(f) Physical and environmental security [8.2.3 and 8.2.4]

(g) Communications and operations management [sections 1, 7, and 10]
(h) Access control [sections 1, 8.2, and 10]
(i) Information systems acquisition, development, and maintenance [1.2.6]
(j) Information security incident management [1.2.7]
(k) Business continuity management [section 8.2]
(l) Compliance [sections 1 and 10]

MTCL's security program addresses the following matters related to protection of personal information:

- Periodic risk assessments
- Identification of all types of personal information and the related processes, systems, and third parties that are involved in the handling of such information
- Identification and documentation of the security requirements of authorized users
- Allowing access, the nature of that access, and who authorizes such access
- Preventing unauthorized access by using effective physical and logical access controls
- The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access
- Assignment of responsibility and accountability for security
- Assignment of responsibility and accountability for system changes and maintenance
- Protecting operating system and network software and system files

- Protecting cryptographic tools and information
- Implementing system software upgrades and patches
- Testing, evaluating, and authorizing system components before implementation
- Addressing how complaints and requests relating to security issues are resolved
- Handling errors and omissions, security breaches, and other incidents
- Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing)
- Allocating training and other resources to support its security policies
- Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies
- Business continuity management and disaster recovery plans and related testing
- Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts
- A requirement that users, management, and third parties confirm (initially and annually) their understanding of and agreement to comply with MTCL's privacy policies and procedures related to the security of personal information
- Procedures to cancel access privileges and ensure return of computers and other devices used to access or store personal information when personnel are terminated

MTCL's security program prevents access to personal information in computers, media, and paper based information that are no longer in active use by the organization (for example, computers, media, and paper-based information in storage, sold, or otherwise disposed of).

### 8.2.2 Logical Access Controls

Logical access to personal information is restricted by procedures that address the following matters:

(a) Authorizing and registering internal personnel and individuals

(b) Identifying and authenticating internal personnel and individuals
(c) Making changes and updating access profiles
(d) Preventing individuals from accessing anything other than their own personal or sensitive information
(e) Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities
(f) Distributing output only to authorized internal personnel
(g) Restricting logical access to offline storage, backup data, systems, and media
(h) Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
(i) Preventing the introduction of viruses, malicious code, and unauthorized software measures for remote access, such as additional or dynamic passwords, callback procedures, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls.

Granting privileges and permissions for access to IT Systems and procedures are in place to

- establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information.
- authenticate users, for example, by user name and password, certificate, external token, or biometrics before access is granted to systems handling personal information.
- require enhanced security infrastructure components and personal information
- implement intrusion detection and monitoring systems.

### 8.2.3 Physical Access Controls

Physical access is restricted to personal information in any form (including the components of MTCL's system(s) that contain or protect personal information).

Systems and procedures are in place to

- manage logical and physical access to personal information, including hard copy, archival, and backup copies.
- log and monitor access to personal information.
- prevent the unauthorized or accidental destruction or loss of personal information.
- investigate breaches and

- attempts to gain unauthorized access.
- communicate investigation results to the appropriate designated privacy executive.
- maintain physical control over the distribution of reports containing personal information.
- securely dispose of waste containing confidential information (for example, shredding).

### 8.2.4 Environmental Safeguards

Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.

Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. MTCL's controlled areas are protected against fire using both smoke detectors and a fire suppression system.

In addition, MTCL maintains physical and other safeguards to prevent accidental disclosure of personal information in the event of an environmental incident.

### 8.2.5 Transmitted Personal Information

Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying Systems and procedures are in place to

- define minimum levels of encryption and controls.
- employ industry standard encryption technology, for example, 128-bit Transport Layer Security (TLS), over VPNs, industry standard encryption technology for transferring and receiving personal information.
- approve external network connections.
- protect personal information in both hardcopy and electronic forms sent by mail, courier, or other physical means.
- encrypt personal information collected and transmitted wirelessly and protect wireless networks from unauthorized access.

### 8.2.6 Personal Information on Portable Media

Personal information stored on portable media or devices is protected from unauthorized access.

Policies and procedures prohibit the storage of personal information on portable media or devices unless a business need exists and such storage is approved by management.

Policies, systems, and procedures are in place to protect personal information accessed or stored in manners such as using the following:

- Laptop computers, PDAs, smart- phones and similar devices
- Computers and other devices used by employees while, for example, traveling and working at home
- USB drives, CDs and DVDs, magnetic tape, or other portable
- media

Such information is encrypted, password protected, physically protected, and subject to MTCL's access, retention, and destruction policies.

Controls exist over creation, transfer, storage, and disposal of media containing personal information used for backup and recovery.

Procedures exist to report loss or potential misuse of media containing personal information.

Upon termination of employees or contractors, procedures provide for the return or destruction of portable media and devices used to access and store personal information, and of printed and other copies of such information.

### 8.2.7 Testing Security Safeguards

Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.

Systems and procedures are in place to

- regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information.
- periodically undertake independent audits of security controls using either internal or external auditors.
- test fob access systems and other physical security devices at least annually.
- periodically undertake threat and vulnerability testing, including security penetration and Web vulnerability and resilience.

- make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities.
- periodically report the results of security testing to management.

# Quality Criteria

## 9.0 MTCL maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

## 9.1 Policies and Communications

### 9.1.0 Privacy Policies

MTCL's privacy policies address the quality of personal information.

### 9.1.1 Communication to Individuals

Individuals are informed that they are responsible for providing MTCL with accurate and complete personal information, and for contacting MTCL if correction of such information is required.

MTCL's privacy notice explains that personal information needs to be kept accurate and complete only when the individual has an ongoing relationship with MTCL.

## 9.2 Procedures and Controls

### 9.2.1 Accuracy and Completeness of Personal Information

Personal information is accurate and complete for the purposes for which it is to be used.

Systems and procedures are in place to

- edit and validate personal information as it is collected, created, maintained, and updated.
- record the date when the personal information is obtained or updated.
- specify when the personal information is no longer valid.
- specify when and how the personal information is to be updated and the source for the update (for example, annual reconfirmation of information held and methods for individuals
- to proactively update personal information).
- indicate how to verify the accuracy and completeness of personal information obtained directly from an individual, received from a third party (see 4.2.3, "Collection From Third Parties"), or disclosed to a third party (see 7.2.2, "Protection of Personal Information").
- ensure personal information used on an ongoing basis is sufficiently accurate and complete to make decisions, unless clear limits exist for the need for accuracy.
- ensure personal information is not routinely updated unless such a process is necessary to fulfill the purposes for which it is to be used.
- MTCL undertakes periodic assessments to check the accuracy of personal information records and to correct them, as necessary, to fulfill the stated purpose.
- periodically assess the relevance of personal information records and to correct them, as necessary, to minimize the use of inappropriate data for decision making

# Monitoring and Enforcement

## 10.0 MTCL monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.

## 10.1 Policies and Communications

### 10.1.0 Privacy Policies

MTCL's privacy policies address the monitoring and enforcement of privacy policies and procedures.

### 10.1.1 Communication to Individuals

Individuals are informed about how to contact MTCL with inquiries, complaints and disputes.

MTCL's privacy notice

- describes how individuals can contact MTCL with complaints (for example, via an e-mail link to MTCL's Web site or a telephone number).
- provides relevant contact information to which the individual can direct complaints (for example, name, telephone number, mailing address, and e- mail address of the individual or office responsible for handling complaints).

## 10.2 Procedures and Controls

### 10.2.1 Inquiry, Complaint, and Dispute Process

A process is in place to address inquiries, complaints, and disputes.

The corporate privacy officer or other designated individual is authorized to address privacy related complaints, disputes, and other problems.

Systems and procedures are in place that allow for

- procedures to be followed in communicating and resolving complaints about MTCL.
- action that will be taken with respect to the disputed information until the complaint is satisfactorily resolved.
- remedies to be available in case of a breach of personal information and how to communicate this information to an individual.
- recourse and a formal escalation process to be in place to review and approve any recourse offered to individuals.
- contact information and procedures to be followed with any designated third party dispute resolution or similar service (if offered).

### 10.2.2 Dispute Resolution and Recourse

Each complaint is addressed, and the resolution is documented and communicated to the individual.

MTCL has a formally documented process in place to

- train employees responsible for handling individuals' complaints and disputes about the resolution and escalation processes.

- document and respond to all complaints in a timely manner.
- periodically review unresolved disputes and complaints to ensure they are resolved in a timely manner.
- escalate unresolved complaints and disputes for review by management.
- identify trends and the potential need to change MTCL's privacy policies and procedures.
- use specified independent third party dispute resolution services or other processes mandated by regulatory bodies in the event the individual is not satisfied with MTCL's proposed resolution, together with a commitment from such third parties to handle such recourses.

If MTCL offers a third-party dispute resolution process for complaints that cannot be resolved directly with MTCL, an explanation is provided about how an individual can use that process.

### 10.2.3 Compliance Review

Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service- level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.

Systems and procedures are in place to

- annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, standards adopted by MTCL, and other contracts.
- document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign offs.
- report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan.
- monitor the resolution of issues and vulnerabilities noted in the compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary).

In addition to legal, regulatory and contractual requirements, some entities may elect to comply with certain standards, such as those published by ISO, or may be required to comply with certain standards, such as those published by the payment card industry, as a condition of doing business.

### 10.2.4 Instances of Noncompliance

Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.

Systems and procedures are in place to

- notify employees of the need to report privacy breaches and security vulnerabilities in a timely manner.
- inform employees of the appropriate channels to report security vulnerabilities and privacy breaches.
- document instances of noncompliance with privacy policies and procedures.
- monitor the resolution of security vulnerabilities and privacy breaches to ensure appropriate corrective measures are taken on a timely basis.
- discipline employees and others, as appropriate, who cause privacy incidents or breaches.
- mitigate, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of MTCL's privacy policies and procedures (for example, notify individuals affected, attempt to recover information disclosed to others, void affected account numbers and reissue new numbers).
- identify trends that may require revisions to privacy policies and procedures.

### 10.2.5, Ongoing Monitoring

Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary., MTCL uses the following:

- Control reports
- Trend analysis
- Training attendance and evaluations
- Complaint resolutions
- Regular internal reviews
- Internal audit reports
- Independent audit reports covering controls at service organizations
- Other evidence of control effectiveness

The selection of controls to be monitored, and the frequency with which they are monitored are based on the sensitivity of the information and the risks of possible exposure of the information.

Examples of such controls are as follows:

- Policies require that all employees take initial privacy training within 30 days of employment. Ongoing monitoring activities would include a review of human resource files of selected employees to determine that they contain the appropriate evidence of course completion.
- Policies require that whenever an employee changes job responsibilities or is terminated, such employee's access to personal information be reviewed and appropriately modified or terminated within 24 hours (or immediately in the case of employee termination). This is controlled by an automated process within the human resource system which produces a report of employee status changes, which requires supervisor action to avoid automatic termination of access. This is monitored by the security group which receives copies of these reports and the related supervisor actions.
- Policies state that confirmation of a privacy-related complaint is provided to the complainant within 72 hours, and if not resolved within 10 working days, then the issue is escalated to the CEO. The control is a log used to record privacy complaints, including complaint date, and subsequent activities through to resolution. The monitoring activity is the monthly review of such logs for consistency with this policy.

## Appendix A—Glossary

**affiliate.** An entity that controls, is controlled by, or is under common control with another entity.

**anonymize.** The removal of any person-related information that could be used to identify a specific individual.

**confidentiality.** The protection of nonpersonal information and data from unauthorized disclosure.

**consent.** Agreement by the individual for MTCL to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. *Explicit consent* is given orally, electronically,

or in writing, is unequivocal and does not require any inference on the part of MTCL seeking consent. *Implicit consent* may reasonably be inferred from the action or inaction of the individual such as not having *opted out*, or providing credit card information to complete a transaction. (see opt in and opt out).

**cookies.** Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. The information can then be used to identify the user when returning to the Web site, to personalize Web content, and suggest items of potential interest based on previous buying habits. Certain advertisers use tracking methods, including cookies, to analyze the patterns and paths through a site.

**encryption.** The process of transforming information to make it unreadable to anyone except those possessing special key (to decrypt).

**entity.** An organization that collects, uses, retains, and discloses personal information.

**individual.** The person about whom the personal information is being collected (sometimes referred to as the *data subject*).

**internal personnel.** Employees, contractors, agents, and others acting on behalf of MTCL and its affiliates.

**opt in.** Personal information may not be collected, used, retained and disclosed by MTCL without the explicit consent of the individual.

**opt out.** Implied consent exists for MTCL to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

**outsourcing.** The use and handling of personal information by a third party that performs a business function for MTCL.

**personal information.** Information that is or can be about or related to an identifiable individual.

**personal information cycle.** The collection, use, retention, disclosure, disposal, or anonymization of personal information.

**policy.** A written statement that communicates management’s intent, objectives, requirements, responsibilities, and standards.

**privacy.** The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.

**privacy breach**. A privacy breach occurs when personal information is collected, retained, accessed, used, or disclosed in ways that are not in accordance with the provisions of the enterprise's policies, applicable privacy laws, or regulations.

**privacy program.** The policies, communications, procedures, and controls in place to manage and protect personal information in accordance with business and compliance risks and requirements.

**purpose.** The reason personal information is collected by MTCL.

**redact.** To delete or black out personal information from a document or file.

**sensitive personal information.** Personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

**third party.** An entity that is not affiliated with MTCL that collects personal information or any affiliated entity not covered by MTCL's privacy notice.

**Web beacon.** Web beacons, also known as Web bugs, are small strings of code that provide a method for delivering a graphic image on a Web page or in an e-mail message for the purpose of transferring data. Businesses use Web beacons for many purposes, including site traffic reporting, unique visitor counts, advertising and e-mail auditing and reporting, and personalization. For example, a Web beacon can gather a user's IP address, collect the referrer, and track the sites visited by users.