TELUS' Privacy Management Program Framework

Presented by
The TELUS Data & Trust Office

We are accountable to you.

A vital part of our commitment to privacy is to be transparent with you about the ways we protect your privacy. We want you to know just how robust our framework for managing privacy is so we are pleased to share the framework for our core Privacy Management Program with you.

The TELUS Privacy Management Program and its components set out in this document reflect TELUS' desire to exceed our privacy obligations as prescribed by legislation, to be transparent with customers, and to provide further direction for TELUS team members.

While TELUS strives to meet these commitments, the Program is not intended to, and does not, impose additional legal obligations or constraints on TELUS and should not be construed as such. As privacy and technology evolve, this Program Framework will change and changes will be shared.

Last updated on June 1, 2021.

Table of Contents

Introduction 4
- Scope 4

Stakeholders in our Privacy Management Program 5

Key Drivers 6

Our Structure of Accountability 7
- The Board of Directors 7
- The Chief Executive Officer 7
- The Executive Team 7
- The Chief Data & Trust Officer 7
- Individual Team Member Accountability 8
- Privacy Partners 8
- Integration with TELUS' Data Governance Framework 8
- Key Partnerships 8
  - Our Security Teams 8
  - Our Legal Services and Regulatory Affairs Teams 9
  - The Privacy Request Centre Team 9
  - TELUS Wise® 9
  - Chief Procurement Office 9
  - Our People & Culture Team 9
  - Our Enterprise Architecture Team 9
  - Our Product Development and Management Teams 9
  - Our Enterprise Risk Team 10
  - Our Integrity Working Group 10
  - Our Emergency Management Operations Committee (EMOC) 10
  - All of our business units that handle personal information 10

Governance of Policy, Standards, Procedures and Guidance 10

Operational Controls 11
- Risk Identification Tools 11
  - Privacy Impact Assessment Process 11
- Personal Information Inventories 12
- De-identification Framework and Community of Practice 12
- Records Management (Retention and Disposal) 12
- Disclosures to Law Enforcement 13
- Training and Awareness 13
- Incident Response 13
- Inquiries and Requests for Access to Personal Information 14
- Privacy Compliance Monitoring, Audit and Enforcement 14
- Service Provider Management 15

Transparency, Education and Choice 15
- Our TELUS Privacy Centre, policies and supporting material 15
- Our Transparency Reporting 16
- Choice and Consent 16
- TELUS Learning Centres 16
- TELUS Wise® 16

Oversight and Review 17

Questions? 17

Introduction

At TELUS, we hold ourselves accountable for protecting the privacy of the personal information[1], which includes personal health information, entrusted to us by our customers and team members[2].

Specifically, we are accountable for:

- developing a governance structure that promotes and values privacy and that enables every one of our team members to make the right decisions, every day, about how to respect privacy when handling personal information;
- ensuring that we properly identify and mitigate privacy risks throughout our operations, in part by striving to apply the principles of Privacy by Design in the development and review of our products and services; and
- earning and maintaining our customers' and team members' trust by being transparent about how we handle personal information and by offering choices where it is appropriate to do so.

Every team member at TELUS has a responsibility to put privacy first when handling personal information and to understand the privacy commitments we make to both our customers and team members, set out, respectively, at telus.com/privacy.

This framework sets out core elements of TELUS' Privacy Management Program, documenting some of our key program commitments to protecting the privacy of our customers and team members in a manner consistent with the 10 Fair Information Privacy Principles outlined in our Privacy Code.

This framework also sets out some of the ways in which we have operationalized those commitments and the organizational structure we have implemented in order to do so.[3]

Scope

This Privacy Management Program framework applies to customer and team member privacy within TELUS, including TELUS Health.[4]

[1]Any information about an identifiable individual, other than the name, title or business address (including business email address) or business telephone or fax numbers of an employee of an organization. For clarity, personal information includes personal health information. Personal information does not include de-identified or aggregated information that cannot reasonably be associated with a specific individual.Information about customers who are sole proprietors or partners is considered to be "personal information" if it is information about the individuals themselves, as distinct from information about their businesses. The latter is protected by other TELUS policies and practices and through contractual business arrangements.

[2]For the purposes of this document, team members includes TELUS employees as well as independent contractors performing services for TELUS.

[3]The TELUS Privacy Management Program and its components set out in this document reflect TELUS' desire to exceed our privacy obligations as prescribed by legislation, to be transparent with customers, and to provide further direction for TELUS team members. While TELUS strives to meet these commitments, the Program is not intended to, and does not, impose additional legal obligations or constraints on TELUS and should not be construed as such. As privacy and technology evolve, this Program Framework may change and changes will be shared.

[4] In this Privacy Management Framework, the words "we" or "TELUS" refer to TELUS Communications Inc. and its subsidiary companies, as they may exist from time to time, including those subsidiaries or divisions that carry on business under the names: TELUS, TELUS Communications, TELUS Mobility, TELUS Québec, TELUS Retail Ltd., Koodo, and Public Mobile, TELUS Health, and TELUS Sourcing Solutions Inc., but do not include TELUS Friendly Future Foundation or TELUS International (Cda) Inc. The words "we" and "TELUS" do not include independent dealers and distributors of TELUS products and services.

Stakeholders in our Privacy Management Program

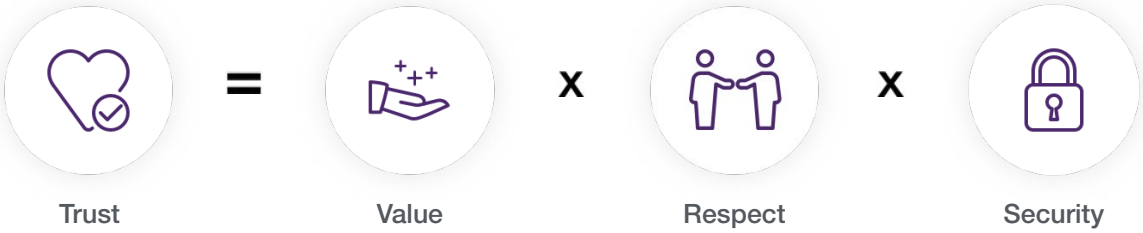
At TELUS, we recognize that there are a number of stakeholders who care about or are impacted by how we handle personal information. These stakeholders include:

- Our customers, including our business customers and their individual customers whose personal information is entrusted to us;
- Our former and prospective customers who have shared or may share their personal information with us;
- Our board of directors and our executive team, who are accountable for the development, execution and oversight of the Privacy Management Program;
- Our shareholders, who have invested in TELUS;
- Our current, former and prospective team members whose personal information we handle, our team members who are entrusted with our customers' personal information, and who participate in TELUS' success;
- Our regulators, who have oversight of our privacy management practices;
- Canadians, who as taxpayers, telecommunications users, and participants in the economy, have a stake in the success of Canadian companies such as TELUS; and
- Law enforcement, which relies on data provided by TELUS to fight crime and protect Canadians.

Key Drivers

There are numerous pieces of legislation that govern privacy in Canada. While compliance with these laws is clearly one of the drivers of TELUS' Privacy Management Program, it is only the baseline for our approach to privacy. TELUS' commitment to protecting the privacy of the personal information entrusted to us is **driven by our commitment to earn and maintain our stakeholders' trust**. Leveraging our Customers First commitments, we build trust with our stakeholders by using data in a way that generates value, promotes respect and delivers security:

The TELUS Trust Model



What do we mean by value, respect and security?

Value

We generate value for:

- Our customers
- TELUS
- Our team members
- Our other stakeholder communities

x

Respect

We demonstrate respect for our stakeholders by:

- Being transparent about our data handling practices
- Meeting their expectations about how we handle and use personal information
- Respecting the legal and regulatory framework within which we operate
- Establishing mechanisms for customer choice
- Carefully considering the risks and benefits of how we handle and use personal information before making impactful decisions
- Striving to embed Privacy by Design principles into our products and services

x

Security

We safeguard data through:

- Appropriate administrative, physical and technical security controls
- Regular security and data handling practice reviews
- Rigorous incident detection and response procedures
- Established de-identification standards
- Limiting access to data
- Striving to embed Security by Design principles into our products and services

To read more about our Trust Model and how we use our Trust Model when making decisions about data, please visit our Privacy Centre.

Our Structure of Accountability

The Board of Directors

TELUS' accountability for sound privacy management practices resides at the highest level of the organization, the TELUS Corporation board of directors. The board of directors has responsibility for approving TELUS' privacy strategy; it also has an oversight role in respect of privacy management and in ensuring that appropriate privacy policies and practices are in place and functioning effectively.

The audit committee of the board receives a written and verbal report on the Privacy Management Program from the Chief Data & Trust Officer on a quarterly basis. Summaries of the audit committee reports are provided to the entire board of directors in order to allow the full board to inquire further into any matters raised in the quarterly reporting.

The Chief Executive Officer

TELUS' Chief Executive Officer is charged by the board of directors to deliver on TELUS' overall strategy, including TELUS' commitment to customer and team member privacy. The Chief Executive Officer has ultimate accountability for establishing and overseeing execution on TELUS' privacy strategy, and for TELUS' privacy policies and practices.

The Executive Team

All members of TELUS' executive team have the responsibility to enable operational compliance with TELUS' privacy policies and standards within their own areas of responsibility, ensuring that all business units are properly aware of and resourced to meet our privacy obligations. Our executive team also take responsibility for endorsing TELUS' privacy program and controls, implementing appropriate procedures to give effect to our standards, and generally fostering a culture that respects customer and team member privacy. The senior executive leadership team receives quarterly reporting from the Data & Trust Office on privacy risks and incidents, along with any significant risk remediation programs.

The Chief Data & Trust Officer

While accountability for privacy at the operational level ultimately resides with TELUS' Chief Executive Officer, day-to-day operational functions have been formally delegated to the Chief Data & Trust Officer. The Chief Data & Trust Officer is charged with operationalizing TELUS' commitment to earn and maintain the trust of our customers and other stakeholders when it comes to how we handle personal information. The Chief Data & Trust Officer, supported by a dedicated team comprising TELUS' Data & Trust Office, is responsible for:

- managing the Privacy Management Program;
- enhancing the Privacy Management Program to ensure it continues to meet the expectations of our customers, team members, other stakeholders and regulators;
- setting privacy policies and standards to achieve our goal of earning and maintaining stakeholder trust;
- providing privacy advice and support to all areas of TELUS;
- ensuring that TELUS' suite of privacy policies and standards is comprehensive, up-to-date and compliant with applicable law;
- providing enterprise privacy training, supporting more job-specific privacy training and maintaining privacy awareness throughout the organization;
- identifying privacy risks and providing recommendations and strategies to mitigate or eliminate such risks; and
- conducting privacy reviews and monitoring compliance, as appropriate.

Finally, in recognition of the importance of privacy to TELUS' overall strategy, the Chief Data & Trust Officer is responsible for keeping the board of directors (audit committee), Chief Executive Officer, Chief Financial Officer, Chief Legal Officer, EVP Technology Strategy and Business Transformation, and Chief Technology Officer, apprised of material privacy matters and risks, reporting to them at least quarterly on a formal basis, and on an ad hoc basis as required.

Individual Team Member Accountability

As a core commitment of TELUS, all TELUS team members are accountable for protecting the privacy of our customers and other team members; all team members play a role in earning and maintaining the trust of our stakeholders. This goes beyond complying with our privacy policies and standards, our Acceptable Use Policy and our Code of Ethics and Conduct. Whether team members are developing products and services using Privacy by Design principles, on our front-line interacting directly with our customers, handling sensitive personal information of team members, marketing our products and services, supporting our technology infrastructure or designing security solutions, part of putting our Customers First is putting their privacy first. Not only is this part of our privacy commitment to our customers and team members, this is part of our commitment to acting with integrity in all that we do, every day. To that end, we have established the TELUS Trust Model to guide our decisions around data.

In addition, TELUS team members are trained on our privacy incident reporting protocol and are required to report any privacy incident, including suspected incidents.

TELUS has established an Integrity Working Group that oversees team member compliance with ethics, privacy, security and respectful workplace policies. The Integrity Working Group reviews any breach of obligations under those policies to ensure that appropriate disciplinary action is taken.

Privacy Partners

The TELUS Data & Trust Office has implemented the privacy partner model to enable the implementation of Privacy by Design principles. Each business unit has an identified Privacy Partner in the Data & Trust Officer who assists them with identifying possible privacy considerations that may arise as they execute on their strategy and, more granularly, can work collaboratively with members from the business to ensure that their initiatives are enabled at an early stage of a project in a manner that respects the privacy and security of our customers and team members.

Integration with TELUS' Data Governance Framework

TELUS has developed and continues to focus efforts on a data governance framework that applies broadly to all data, including personal information, put simply, any information that can be used to gain knowledge or drive decisions. Our evolving data governance framework reflects TELUS' commitment to respectfully treat data in a manner that fosters innovation and, at the same time, mitigates privacy, security and ethical risks associated with innovative uses of data. This Privacy Management Program framework, and the governance structure that supports it, are part of the backbone of TELUS' overall data governance framework and ground accountable decision-making around data.

Key Partnerships

TELUS' Privacy Management Program relies upon several key internal partnerships. The Data & Trust Office works closely with:

Our Security Teams

- To help safeguard the personal information under our control;
- To control access to personal information, limiting access to those who have a need;
- To identify and remediate security risks to personal information;
- To monitor, investigate and contain suspected security breaches;
- To promote privacy and security awareness throughout TELUS; and
- To respond promptly and effectively to valid court orders and other requests for assistance from law enforcement where it is appropriate and consistent with our privacy commitments to do so.

Our Legal Services and Regulatory Affairs Teams

- To ensure our Privacy Management Program is compliant with the law and that we stay up-to-date on new legal requirements and regulatory guidance;
- To respond in a prompt and appropriate manner to our regulators in respect of matters relating to our handling of personal information; and
- To protect our customer and team member privacy through established contract reviews and controls wherever appropriate.

The Privacy Request Centre Team[5]

- To assist in providing specialized coaching and subject matter support to our PRC team members;
- To resolve customer inquiries, concerns and complaints in respect of how their personal information is used;
- To identify ways we can be more transparent with our customers about how we handle their personal information.

TELUS Wise®

- To offer free-of-charge, interactive and informative workshops and content to help Canadians of all ages have a positive experience as digital citizens. Topics include protecting your online security, privacy, and reputation, rising above cyberbullying, and using technology responsibly.

Chief Procurement Office

- To collaborate on the review, selection, and monitoring of partners and other organizations who handle or have access to personal information of our customers or team members;
- To ensure that appropriate contractual controls around the privacy and security of data are in place with such organizations;
- To ensure that our Supplier Code of Conduct contains appropriate privacy commitments.

[5]Our Privacy Request Centre (PRC) is made up of agents who are specially trained to be able to respond to customer inquiries and concerns regarding privacy-related matters.

Our People & Culture Team

- To promote privacy training and awareness for all of our team members;
- To ensure that our people & culture practices reflect our commitments to team member privacy;
- To support the enforcement of our rules and standards put in place to protect customer and team member privacy, providing appropriate coaching and discipline where appropriate.

Our Enterprise Architecture Team

- To assist in the development of architectural standards and guidance to enable Privacy by Design;
- To achieve consistency between our data management systems and standards and to ensure our systems are architected to support data quality.

Our Product Development and Management Teams

- To ensure, by embracing the principles of Privacy by Design, that our products and services support our commitment to protect privacy and to be transparent about our personal information handling practices.

Our Enterprise Risk Team

- To identify, manage, monitor and report on privacy related risk at the enterprise level;
- To assist in the identification of privacy-related compliance risk and support recommendations from our internal audit process.

Our Integrity Working Group

- To review team member compliance with ethics, privacy, security and respectful workplace policies including the review of any breach of obligations under those policies to ensure that appropriate disciplinary action is taken, up to and including dismissal;
- To design and deliver annual integrity training to our team members which reinforces the fundamental importance of our commitment to integrity and how our commitment to privacy is part of acting with integrity.

Our Emergency Management Operations Committee (EMOC)

- To ensure that privacy considerations relating to the personal information of our customers and team members are appropriately addressed when managing emergencies and disasters.

All of our business units that handle personal information

- To maintain awareness about privacy to ensure that every team member understands that they have personal responsibility for meeting TELUS' privacy commitments every day in everything they do;
- To appoint data stewards to be advocates for data governance and data management processes within the business unit to ensure data governance principles and standards are successfully operationalized.

Governance of Policy, Standards, Procedures and Guidance

The Data & Trust Office is responsible for setting policies and standards to give effect to our commitment to protect the privacy of personal information entrusted to us. These policies and standards are developed in accordance with best practices and in coordination with stakeholder business groups; and they are ultimately reviewed by the audit committee of TELUS' board of directors.

Privacy policies and standards are reviewed at least annually by the Chief Data & Trust Officer, and may also be reviewed by external privacy specialists from time to time. The reviews are focused on ensuring that the policies and standards remain compliant with the law, evolving industry standards, and our privacy commitments to our customers and team members. They may be revised more frequently to reflect changes in privacy legislation and regulations, and updated to reflect any impending changes to our personal information-handling practices.

Changes to our Privacy Commitments or Privacy Code are communicated to our customers and/or team members, as applicable, in accordance with a documented process designed not only to comply with applicable law, but also to ensure timely notice in a manner that preserves individual choice wherever appropriate.

TELUS' Privacy Commitments and Privacy Code are accessible online to all team members at telus.com/privacy. Every team member is required to confirm annually that they have read them and understand that they are expected to adhere to the standards described through our integrity online course.

The development of procedures to enable compliance with these policies is the responsibility of the applicable business unit, supported and guided by members of the Data & Trust Office.

To support the development of procedures and to enable business areas of TELUS to implement Privacy by Design principles, the Data & Trust Office also issues guidance on certain key privacy-related topics, often partnering with the Corporate Security Office in the development of the guidance.

Any exceptions to privacy policies or security standards where personal information is involved, must be reviewed by the Data & Trust Office and will be escalated up to and including the Chief Executive Officer and the board of directors in situations where our commitment to protect customer and team member privacy is at stake.

Operational Controls

Risk Identification Tools

Vital to TELUS' commitment to protecting the privacy of our customers and team members is the ongoing, systematic identification of privacy risks so that those risks can be mitigated or avoided.

To that end, TELUS has developed a Data Risk Management Policy, in conjunction with a Data Risk Management Framework, designed to provide a comprehensive process to evaluate and manage risks associated with our collection, handling, use and safeguarding of data.

We identify potential risks, through a variety of tools, including:

- Privacy Impact Assessments / Data Impact Assessments / Algorithmic Impact Assessments;
- Security Risk Assessments / Threat Risk Assessments / Data Risk Assessments;
- Audits by our Internal Audit team;
- Privacy risk reviews of a business process;
- Data Governance Forums, Councils or Executive Committee Reviews;
- Investigation made pursuant to TELUS' Data Incident Readiness and Response Playbook and / or the associated post-incident review;
- Investigation of a privacy complaint or inquiry;
- Compliance Monitoring Reviews;
- Scans and monitoring of external trends and practices, new technology, incidents, events, articles and regulator guidance;
- Annual Privacy and Information Security policy review against legislative and regulatory requirements and best practices.

Privacy risks may also be identified to us through an investigation or inquiry made by a regulator (for example, the Office of the Privacy Commissioner of Canada), or we may become aware of a privacy risk as a result of a vulnerability or breach at another organization.

Privacy Impact Assessment Process

TELUS' primary tool for the identification and mitigation of privacy risk is the Privacy Impact Assessment (PIA) process.

We recognize that new privacy risks are most often created through changes to existing products, services, processes or systems, or the introduction of new, products, services, processes and systems that involve access to or the collection, use, or disclosure of personal information. Through a PIA, new or changed collections, transfers, handling practices or uses are rigorously reviewed for consistency with our commitments to privacy, applicable customer contracts, applicable law and industry standards, as well as our TELUS Trust Model.

The PIA process has been operationalized through an online PIA tool available to all business units throughout TELUS. The PIA tool enables every business unit to submit a PIA for review by a privacy professional that is certified by a recognized privacy association[6], and an accredited security consultant in the TELUS Corporate Security Office. The Data & Trust Office identifies privacy risks and makes recommendations and/or sets conditions for the acceptance

6 For example, the International Association of Privacy Professionals (IAPP).

of a PIA. The completed PIA must be approved by the business unit, which is then responsible for implementing the agreed upon risk mitigation or avoidance steps and for accepting and managing any residual risk.

All business units are required to submit PIAs for the design of, or changes to, products, services, initiatives, processes and systems that involve access to, collection, storage, use or disclosure of data. PIAs will be reviewed and amended as necessary during the design and implementation stage.

In some cases, the Data & Trust Office, together with the applicable business unit, may determine that a different method of risk assessment and mitigation is better suited to a particular initiative. In this case, the privacy risks will be identified and addressed through another agreed upon mechanism. For example, as TELUS explores the transformative potential of artificial intelligence, we have developed a Data and Algorithmic Impact Assessment to consider new risks that are unique to machine learning.

In addition, PIAs may be conducted for any existing products, services, initiatives, processes and systems with privacy implications, as recommended by the Chief Data & Trust Officer in consultation with the executive for the applicable business unit.

Personal Information Inventories

TELUS is currently implementing a network of data stewards across the organization. The requirement is for each business unit to designate one or more data stewards, depending on the volume and sensitivity of the data within the business unit.

Data stewards are accountable for maintaining an inventory of the data under their business unit's control, and for assisting in monitoring adherence to privacy and other data standards within their business unit.

De-identification Framework and Community of Practice

TELUS has developed a de-identification framework to guide our team members to make effective decisions on initiatives that involve de-identified data. Our framework incorporates strategies for team members to use data in a responsible, ethical, and privacy protective manner and elevates data de-identification beyond most current techniques to also cover planning, implementation, and governance of de-identification initiatives.

We have also established a de-identified community of practice that allows select team members across the organization to share their de-identification expertise and explore new and innovative de-identification techniques that protect privacy while still allowing the possibility of conducting meaningful and valuable analytics.

Records Management (Retention and Disposal)

TELUS has a Records Retention Policy that incorporates a Records Retention Schedule. The policy applies to all TELUS records in any form or medium. All team members are advised of the policy and its importance. Its effective operationalization is supported by a records retention prime (team member) appointed by each executive leadership member, and for each business unit.

The Records Retention Policy also provides guidance to team members on the efficient and consistent management, retention and secure disposal of TELUS records.The Records Retention Schedule is accessible online to all team members. The Schedule sets out the retention period (a maximum and minimum) for each category of records at TELUS based on business needs and legal requirements.

Once records are at the end of their retention period, they are disposed of in a secure manner, in accordance with specific security standards set out by the TELUS Corporate Security Office and updated from time to time, as required.

The Chief Data & Trust Officer reviews the Records Retention Policy every other year and on an ad hoc basis, as required and, where appropriate, makes changes to the Policy.

Disclosures to Law Enforcement

TELUS has a designated Court Order Liaison Team (COLT) within our TELUS Corporate Security Office team that is specifically charged with working with Law Enforcement to fulfil valid court orders for the disclosure of customer or team member information. All requests from law enforcement are referred to COLT. COLT follows a strict procedure for ensuring that we meet our commitment to protect customer privacy when assisting law enforcement's lawful efforts to fight crime and terrorism. This is a delicate balance that we take seriously, which is why the COLT procedure is regularly reviewed by the Data & Trust Office and our legal department. Disclosures made to law enforcement are tracked and reported in our Transparency Reporting, described below.

Training and Awareness

An integral part of meeting our privacy commitments is our focus on raising team member awareness and understanding of privacy in a meaningful and measurable way and to maintain a privacy respectful culture at TELUS.

We develop an annual privacy and training awareness strategy that sets out a specific team member training and awareness plan for the year. In the development of that annual strategy, we are committed to the following attributes of our privacy training and awareness program:

- Privacy training content is updated on a yearly basis;
- As part of our on-boarding and orientation program, all new team members, including contractors, must take, and successfully pass, privacy training;
- On an annual basis, all team members, including contractors, must take, and successfully pass, privacy training, which is monitored and tracked;
- When a team member transitions to a new role, they may be asked to retake privacy training;
- Supplementary job-specific privacy training will be provided as appropriate and incorporated in standard job training to the extent practical;
- Responsive ad hoc training and awareness will be delivered in a timely fashion where it will have the greatest impact on mitigating privacy risk at TELUS;
- We make appropriate adjustments to our privacy training and awareness activities in order to make them effective and applicable to both our TELUS stores and our TELUS dealers;
- We provide health privacy specific training for our team members who manage personal health information that takes into consideration the special nature of health information as well as the specific requirements of the various applicable health privacy regulations;
- We embrace and incorporate the seven principles of Privacy by Design in our training as an effective way to minimize privacy risk for TELUS, our team members and our customers;
- We collaborate with our business partners and team members to ensure the training is relevant, interesting, and that we deliver it in an effective manner, maximizing the value of the training while minimizing any negative impacts to operations;
- We take a multi-media approach to raising awareness;
- We focus on high impact, repeatable/reusable/updatable training and awareness activities.

Incident Response

TELUS is committed to safeguarding personal information in order to maintain customers and team member trust. This trust, along with our brand and reputation, may be directly impacted by our ability to respond effectively in the event that our safeguards or policies are compromised. Accordingly, TELUS has systems and methods in place to regularly monitor for breaches of safeguards and policies and has a clear incident reporting process easily accessible to all team members; all team members are required to report any privacy incident (including suspected incidents).

TELUS has developed, uses, regularly tests and continuously improves our Data Incident Readiness and Response Playbook designed to facilitate a coordinated and timely response to the detection, management and remediation of privacy incidents. The playbook sets out clear roles and responsibilities, along with reporting, escalation and decision-making criteria, all designed to give effect to the TELUS Trust Model. We recognize that it is important to respond with a sense of urgency to any incidents involving personal information and to take decisive action to contain them and, where appropriate, to notify those who are impacted, or our regulators, in a timely manner.

When an incident impacts our customers we are committed to fully investigating it, mitigating risks arising from it, implementing safeguards designed to prevent it from happening again and, more generally, making it right with our customers and team members. If and when an incident occurs that could impact our customers or team members, putting them at risk of harm, we will contact them via phone, text or email, and depending on the type of incident, we will post information on a web page to keep our customers informed of any relevant updates as we work to remedy the incident.

The Chief Data & Trust Officer reviews the playbook at least annually and on an ad hoc basis as legal requirements or best practices change or to incorporate improvements identified in testing or in post-incident reviews of any privacy incidents.

Inquiries and Requests for Access to Personal Information

Our customers and our team members have a right, under applicable privacy legislation, to make inquiries about how we handle their personal information, to make certain corrections to their personal information and to request access to their personal information. To respond to such inquiries and requests (other than health or team member related), TELUS maintains a toll-free-number at **1-800-567-0000**, and an email address for customers to contact us[7]. The calls and emails are received by our Privacy Request Centre made up of agents who are specially trained to be able to respond to customer inquiries and complaints regarding privacy-related matters, and who can correct any personal information inaccuracies or respond to requests from customers for access to their personal information.

Customers of our health-related services should refer to the privacy policy for that specific service (which can be found here) for information about how to make inquiries or request access to their information.

The Team Member Privacy Office (TMPO) is a dedicated team within the Data & Trust Office that is specially trained to respond to team member privacy inquiries and complaints as well as requests from team members to access their personal information. A toll-free number and email address are maintained for team members to contact the TMPO and are posted for team members internally online on the Team Member Privacy Page.

We regularly review our responses and processes to reply to both inquiries and requests for access to personal information to determine if improvements can be made, taking into consideration customer and team member feedback, technological developments, as well as the timeliness, efficiency and comprehensiveness of our responses.

Privacy Compliance Monitoring, Audit and Enforcement

The Data & Trust Office is responsible for regular monitoring and reporting on TELUS' compliance with its privacy policies, standards and procedures.

TELUS has a Compliance Monitoring Program to measure business units on a regular basis against a set of key compliance indicators established by the Data & Trust Office. Summary reports of the results are prepared for the appropriate executive to enable a clear line of sight into the efficacy of existing policies, standards and procedures and include suggested remediation actions to address any gaps.

Our Internal Audit team also conducts privacy audits from time to time, as part of their rotating audit schedule, including audits of compliance with our privacy policies and with this framework. Opportunities for improvement are identified and assigned to the responsible executive for remediation within a specified timeframe.

7 Koodo customers can contact the Koodo Privacy Request Centre at 1-855-525-6636 or send an email to privacy@koodomobile.com. Public Mobile customers can contact the Public Mobile Privacy Request Centre by email at privacy@publicmobile.ca.

Service Provider Management

TELUS has a dedicated Chief Procurement Office team and a process that incorporates rigorous privacy requirements into the contracting process. To facilitate ongoing monitoring, our standard privacy contractual provisions also include training, incident reporting requirements and audit rights.

TELUS requires organizations with whom we share personal information to adhere to our Supplier Code of Conduct which sets out various commitments to integrity, including respect for our customers' and team members' privacy and strict controls to protect it.

More importantly, our agreements are designed to ensure that these organizations can only use the information for the purposes for which we provide it to them and must agree to abide by the confidentiality terms in our contracts, including the requirement to respect your privacy. In addition, we have a policy requiring that TELUS will only retain or partner with third parties that will appropriately protect the privacy, confidentiality and security of personal information, as well as the confidentiality and security of confidential information, TELUS intellectual property (IP) and other TELUS assets. Our Supplier Code of Conduct also sets the expectation that the organizations we share data with will be demonstrably accountable with regard to the personal information entrusted to them by TELUS.

TELUS retains accountability for customer and team member personal information it transfers to our service providers or partners for processing (including storage). Personal information collected by TELUS will be stored and processed in Canada or other countries. In either case, the information is protected with appropriate security safeguards, but may be available to foreign government agencies under applicable law. In particular, your personal information may be stored in the cloud, which may include transfers of data outside of Canada. Where appropriate, we use de-identification and other means to protect and minimize the amount of personal information we transfer.

Transparency, Education and Choice

Transparency about our privacy practices through simple explanations in clear language is a cornerstone of our Trust Model. It is only one of the ways we demonstrate respect for our customers and team members and their privacy.

Our TELUS Privacy Centre, policies and supporting material

Our TELUS Privacy Centre (publicly available privacy pages) is a home for our customers and team members to learn more about our privacy practices.

At TELUS, we know your privacy matters to you; earning and maintaining your trust matters to us. We understand that in today's technologically complex, data-driven world, it can be difficult to stay up-to-date on how personal information is being used. An important part of our commitment to respecting your privacy is our promise to be transparent with you about our privacy practices and to clearly explain how we protect your privacy.

We have created the TELUS Privacy Centre to provide you with information to help you understand TELUS' privacy practices and how we use data at TELUS. The Privacy Centre includes our TELUS Privacy Commitment and Privacy Code, our Cookies Notice, Frequently Asked Questions, and this Privacy Management Program. It also includes more detailed information about some of our privacy protective practices, such as our responsible use of artificial intelligence, how we conduct data analytics and our use of de-identification and aggregation, how Canadians can protect their privacy, and so much more.

Our TELUS Health Business Customer Privacy Policy describes how we manage personal information provided by or about business customers of TELUS Health. For individuals who are consumers of TELUS Health consumer products and services, our commitments governing the collection,

use and disclosure of such individuals' personal information are included in the TELUS Health Privacy Commitment. Our Policy and Commitment are publicly available on our TELUS Health web pages.

We are constantly looking for additional ways to be more transparent with our customers and team members about how we handle personal information. We value the feedback we receive in this regard.

Our Transparency Reporting

We also provide transparency reporting within our annual Sustainability Report. Our transparency reporting provides TELUS customers and the general public with information regarding the numbers and types of information requests we receive each year from law enforcement agencies and government organizations and provides insight into our internal practices and overall approach to complying with or, where appropriate, challenging these requests. The transparency reporting covers TELUS' telecommunications businesses, including wireline and wireless.

Choice and Consent

At TELUS, we believe in providing our customers and team members with appropriate choices about how their personal information is used or not used, particularly where sensitive personal information is involved. We regularly review our personal information-handling practices and the choices we offer against customer feedback, best practices, evolving sensitivities around privacy, and our ongoing commitment to respect our customers' and team members' privacy.

Educating our customers and team members about the implications of their choices is a vital part of demonstrating respect and facilitating truly informed choices. We strive to deliver information in a manner that is clear and concise, while still being comprehensive.

Through our PIA process and other program controls, TELUS ensures that the consent of a customer or team member, be it express or implied, is obtained for the collection, use, or disclosure of personal information, except where not required by applicable privacy legislation. Relevant team members receive specific on-the-job training to ensure they are aware of the importance of, and how to obtain, timely consent, what information should be provided to the individual to make their consent informed, as appropriate, and where to direct customers or team members who have questions.

TELUS Learning Centres

TELUS Learning Centres are accessible through TELUS retail locations across the country. At our Learning Centres customers are offered one-on-one sessions on how to get the most out of their smartphone, including setting up safety features, and how to securely set up their connected home.

TELUS Wise®

As a leading provider of smartphones and Internet services, we are dedicated to ensuring the digital space is a safe space. This, combined with TELUS' commitment to protecting privacy make TELUS Wise® an important priority for TELUS. Free-of-charge, TELUS Wise® is a bilingual digital literacy education program that offers interactive and informative workshops and content to help Canadians of all ages have a positive experience as digital citizens. Topics include protecting your online security, privacy, and reputation, rising above cyberbullying, and using technology responsibly. Visit TELUS Wise to learn more.

Oversight and Review

The Chief Data & Trust Officer develops an annual plan for the review, monitoring and continuous improvement of the Privacy Management Program. The key elements of the annual plan are reviewed by the audit committee of the board of directors, Chief Executive Officer, Chief Financial Officer, Chief Legal Officer, EVP Technology Strategy and Business Transformation, and Chief Technology Officer.

Questions?

We look forward to answering any questions you may have on our Privacy Management Program.
Please write to us at the Data & Trust Office.