COMMITMENT TO CUSTOMER PRIVACY AND DATA PROTECTION

As Axiata embarks on its journey towards becoming a New Generation Digital Champion, we remain committed to respecting and protecting the data and privacy of approximately 320 million customers throughout our regional footprint of ten countries across Asia, with a high level of cybersecurity standards.

We are cognisant of the sensitivity of our customers' information, which includes their personal information and communications, locations and their use of the Internet and digital applications.

As the world becomes increasingly digitalised, with mobile technologies a crucial communications enabler in our lives and businesses emphasis on data privacy and security measures is becoming increasingly more significant. Primary concerns centre on the complexity of advanced technologies, threats from hackers and the potential for human error, all of which can lead to the loss, deletion or misappropriation of information.

We intend to inspire digital trust and confidence in our customers through robust data privacy and security policies, frameworks and management, which will be based on our values of Uncompromising Integrity and Exceptional Performance (UI.EP). Our aim is to enhance our customer experience by ensuring the confidentiality of our customers' personal and business communications by respecting their choice and preferences, whilst keeping their information secure through various controls.

To maintain the digital confidence of our customers we will be implementing initiatives which will broadly cover a number of areas within the Group. These include how we process and protect personal data; maintain a cross-functional Privacy Team; detect and report non-conformities; and create an organisational and employee culture founded on a clear understanding of the importance of protecting and respecting our customers' information.

In 2016, we acknowledged privacy and security issues as an important element in our business processes. Understanding the need to maintain a very high level of compliance in this area, we identified a cross-functional privacy taskforce and identified several action items to reinforce our commitment to upholding privacy and security across the Group. Among these actions are to ascertain consumers' expectations for privacy and security in the markets we operate in, and draft a Group Privacy Framework that will conform to international best practices.

A new Group Privacy Framework will encapsulate Axiata's beliefs on Data Privacy and Cybersecurity and will have the key overarching objective of encouraging business practices and standards that enable innovation while respecting and protecting privacy through providing meaningful transparency, notice, choice and control for customers over the use of their personal information. These actions will be developed and initiated across our Operating Companies (OpCos) and the Group between 2017 and 2018.

We implemented the Axiata Regulatory Compliance Framework in 2015 as an integral part of our Corporate Governance Framework which provides the Board of Directors oversight of Axiata's regulatory compliance performance. Its objective is to set baseline expectations in all OpCos in relation to Regulatory Compliance, placing Axiata and our OpCos in the best position of compliance with regards to regulatory obligations. It also assists the Group to manage exposure to unacceptable compliance risks, and ensure compliance with regulatory authorities.

Within each of our OpCos, compliance with national laws and regulations are a vital core of our OpCos' Data and Privacy Policies. In Malaysia, we have set our commitment to privacy and security based on the Personal Data Protection Act (PDPA) 2010 and the information security standard ISO 27000.

Axiata Group's implementation and execution of our Group wide data privacy actions and measures will be based on four fundamental pillars:

1. **Personal Data Security**

   To protect our customers from the threat of hackers and potential human error, we will utilise a mix of IT system security and periodic data security audits to secure the personal data of our customers. We will also adopt a formal Data Retention Policy to determine when data is to be deleted, once the data is no longer required for its original purpose.

   Where the data processing function is subcontracted to a vendor or supplier for third party processing and/or cross border transfers, we will explain our processes to our customers to ensure they clearly understand our actions and intentions. For third parties with access to Axiata systems or the personal data of our customers, we will ensure that they are contractually bound to maintain Axiata's data security and privacy protocols, where subcontractors will be expected to provide data security levels which are on par with, if not higher than, Axiata's standards.

2. **Personal Data Privacy**

   To ensure that our customers are aware of how and why we intend to process their personal data, we will provide all our customers with choice and control over the use of their personal data in accordance to prevailing laws and obligations as described in our operating licenses and approvals.

   In creating new value through innovative services for today's digital-savvy consumer, we will do so by using techniques to process data where it is not possible to identify specific customers; and/or provide notice or ask for our customers' consent if otherwise. This is essential for the purpose of meeting legitimate business purposes to deliver, provision, maintain or develop new innovative apps and services.

3. **Support for Law Enforcement**

   Mobile telecommunications information is playing an increasingly important role in activities related to national surveillance and support for law enforcement.

   As a responsible Group, we will comply with local law enforcement and national security requirements and will respond to requests from authorities as stipulated within laws and regulations.

4. **Information Technology (IT)**

   A key strategy employed by our OpCos is IT modernisation and digital enablement to give rise to a superior customer experience for our 320 million customers throughout Asia. In line within this, all our OpCos across the region are focusing on implementing various related initiatives to meet evolving business requirements and achieving competitive positioning for our Group. These include developing and inducting the Digital IT Stack to digitize business processes, application rationalisation, enhancing the Application Programme Interface (API) strategy, and modernising Business Support Systems (BSS) and Operations Support Systems (OSS).

   Cybersecurity is an essential component of our digital strategy and risk mitigation. In 2016, Axiata's Cyber Security Operations Center (CSOC) was established across the majority of our OpCos to improve incident monitoring capability. In addition, we continue to relentlessly focus on strengthening our cybersecurity resilience through various initiatives such as periodic cybersecurity posture assessments (CSPA). Another critical area is business continuity and we are sustaining our focus and investments to ensure in effective disaster recovery for key IT systems.