Cyber Security and Data Protection Terms and Conditions
Effective Date: 1 January 2023

1. Definitions

In these Cyber Security and Data Protection Terms and Conditions, the following expressions shall, unless the context otherwise requires, have the meanings assigned to them below:

"**Affiliate**" means in relation to a party, a corporation owned or Controlled by the party, or which owns or Controls the party or which is owned or Controlled by a parent corporation which also owns that party;

"**Agreement**" means the contract between Axiata and the Company which incorporates by reference these Cyber Security and Data Protection Terms and Conditions;

"**Axiata**" means the Axiata Group entity which is a party to the Agreement;

"**Axiata Data**" includes, but is not limited to, the data, text, drawings, diagrams, plans, statistics or images (together with any database made up of any of these) which are embodied in any electronic, magnetic, electromagnetic, optical, tangible or other media:

(a) which are supplied to the Company by or on behalf of Axiata or any other member(s) of the Axiata Group; or

(b) which the Company accesses, Processes, stores, transmits or replicates using or on the Company's systems or equipment pursuant to the Agreement; or

(c) which the Company has custody or control of for purposes connected to the Agreement,

including any Personal Data which Axiata or any other member(s) of the Axiata Group controls the Processing of, or which comes into the knowledge, possession or control of the Company pursuant to the Agreement;

"**Axiata Group**" means Axiata and its Affiliates and associated companies;

"**Axiata Systems**" means the hardware (including computer hardware), software and telecommunications or information technology equipment, systems and networks used or owned by Axiata or any other member(s) of the Axiata Group or licensed to Axiata or any other member(s) of the Axiata Group by a third party;

"**Best Industry Practice**" means, in relation to any undertaking and any circumstances, the exercise of the degree of skill, care, diligence, prudence, foresight and judgement which could reasonably be expected from highly skilled, experienced persons, entities and world leading suppliers and contractors engaged in comparable types of undertaking under similar circumstances, applying equivalent or better standards currently applied in the industry relevant to the Goods and any other products, works and services that may become available to ensure, without limitation, the objectives and obligations identified in the Agreement are achieved and performed that include best practices and value in respect of price, performance and time to market;

"Company" means each of the entities or parties (excluding Axiata) who or which is party to the Agreement;

"Confidential Information" means all information, reports or data such as diagrams, plans, statistics, drawings and supporting records or materials (whether in writing, orally, or by any

electronic or other means), which has come into the possession of the Company before, on or after the effective date of the Agreement which relate to member(s) of the Axiata Group, its customers (including its customers' customers) or suppliers and shall include but is not limited to:

(a) data on the network, formulae, photographs, drawings, specifications, software programs, samples and any technical, business plans, financial or commercial information relating to member(s) of the Axiata Group; or

(b) any information relating to its business, operations, processes, plans, intentions, product information, know-how, design rights, trade secrets, market strategy and opportunities, customer and supplier details and business affairs and any other material bearing or incorporating any information and documentation relating to member(s) of the Axiata Group; and

(c) any Personal Data which Axiata or any other member(s) of the Axiata Group controls the Processing of or which comes into the knowledge, possession or control of the Company pursuant to the Agreement;

"Control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person or entity, whether through the ownership of voting securities, by contract or otherwise;

"**Data Subject**" means an individual who is the subject of the Personal Data;

"**Goods**" means the tangible or intangible goods (which may be hardware, equipment, services or software) specified in the Agreement, including components thereof, all deliverables or work products arising therefrom and all related or ancillary documentation (including training, educational and supporting manuals and materials) which are or are to be provided by the Company under the Agreement;

"**Malware**" means any thing, software or device which may impair or otherwise adversely affect the operation of any computer or system, prevent or hinder access to any program or data (whether by rearranging within the computer or any storage medium or device, altering or erasing, the program or data in whole or in part, or otherwise), gain unauthorised access to any program, equipment, system or data or collect data or surveillance without authorisation, including worms, Trojan horses, computer viruses, ransomware, spyware or similar things;

"**Personal Data**" means personal data, personal information or data relating to individuals;

"**Personnel**" means in relation to a party, the employees, directors, officers, agents, advisers, contractors and subcontractors of that party or of its Affiliates or associates, and the employees, directors and personnel of any such agents, advisers, contractors and subcontractors. The Company's Personnel shall, in addition to the foregoing, include Sub-Processors;

"**Process**", "**Processes**" or "**Processing**" means the processing of any data or information, which shall include the collecting, recording, holding or storing Personal Data or carrying out any operation or set of operations on Personal Data, including:

(a) the organization, adaptation or alteration of Personal Data;
(b) the retrieval, consultation or use of Personal Data;
(c) the disclosure of Personal Data by transmission, transfer, dissemination or otherwise making available; or
(d) the alignment, combination, correction, erasure or destruction of Personal Data;

"Sub-Processor" means any party appointed by, or on behalf of, the Company to Process Personal Data of Axiata or any other member(s) of the Axiata Group in connection with the Agreement.

Interpretation and Construction

1.1 In these Cyber Security and Data Protection Terms and Conditions, unless the context otherwise requires or indicated otherwise:

(a) words denoting the singular number include the plural and vice-versa;

(b) words denoting a gender include every gender;

(c) "person" and words denoting natural persons include bodies corporate and unincorporated, governments, government officials, government departments, agencies or instrumentalities, officials of government departments, agencies, or instrumentalities, public international organisations, official of public international organisations, political party, political party officials, candidates for political office, or their respective representatives or proxies;

(d) words denoting bodies corporate or unincorporated include natural persons;

(e) references to any legislation or law shall include any modification, amendment, re-enactment or substitution of that legislation or law and all regulations, directives, guidelines, by-laws, circulars, guidances, notices, codes, rules and statutory instruments issued under such legislation or law that has the force of law; and

(f) reference to a Clause is a reference to a clause in these Cyber Security and Data Protection Terms and Conditions.

1.2 A rule of construction does not apply to the disadvantage of a party because the party was responsible for the preparation of these Cyber Security and Data Protection Terms and Conditions or any part of it.

1.3 in respect of or in connection with cyber security or data protection, in the event of any conflict or inconsistency between any provision (including the definitions) in these Cyber Security and Data Protection Terms and Conditions and any provision in any other part of the Agreement, the former shall prevail.

2. Cyber Security and Data Protection

2.1 In supplying the Goods, and in carrying out any other tasks allocated to the Company in the Agreement, the Company shall in accordance with Best Industry Practice:

(a) take all necessary steps to ensure that all Axiata Data are protected at all times from accidental, unauthorized or unlawful access, Processing, use or transfer, or loss, misuse, damage, destruction, corruption, or alteration and this includes the following:

(i) having the necessary protective policies, processes, technical and organisations measures and controls for Axiata Data;

(ii) If the Company does not have the necessary protective policies, processes, technical and organisations measures and controls for Axiata Data or when the Company's Personnel is in any member of Axiata Group's premises and/or has access to Axiata Systems (on-site and/or off-site), the Company shall comply with the relevant member of Axiata Group's data privacy, information technology, security, access and usage policies, procedures and directions set out in the Agreement or notified to it from time to time;

(iii) take all necessary steps to prevent any Malware being introduced into any software or onto any of the Axiata Systems or any other systems and/or networks used by the Company to access, Process, store, transmit or generate Axiata Data or supply the Goods to Axiata;

(iv) ensure that there is no unauthorised access to any of the Axiata Data or Axiata Systems without the prior written consent of Axiata and other relevant member(s) of the Axiata Group and/or by any unauthorised third party;

(v) ensure that there is no unauthorised disclosure of passwords, authentication tokens or credentials supplied by Axiata or other member(s) of the Axiata Group to access the Axiata Systems and in the event of an unauthorised disclosure, to remove such access immediately, and revoke or remove such access immediately upon any personnel of the Company no longer having the need to know or leaving the Company; and

(vi) ensure that access to Axiata Data shall be solely for the purpose of performing the Agreement.

(b) immediately notify Axiata of any breach of Clause 2.1**(a) (i)** to **(vi)** above.

3. Security Incident

3.1 If the Company becomes aware of any actual or suspected:

(a) action taken through the use of computer networks that attempts to access the Company's information system or Axiata Data residing on that system or that results in any actual or potential adverse effect on the Company's information system or the Axiata Data residing on that system; or

(b) any other unauthorized access or use by a third party or misuse, damage or destruction by any person; or

(c) breach of any breach of any Personal Data Laws or any applicable law in relation to cyber security by the Company; or

(d) occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies of any member of the Axiata Group or the Company (respectively or collectively shall be referred to as a "**Security Incident**"), the Company shall:

(i) notify Axiata and other relevant member(s) of the Axiata Group in writing immediately (and no longer than 24 hours after becoming aware of the Security Incident and to provide full details of the Security Incident and keep

Axiata and other relevant member(s) of the Axiata Group updated of the Security Incident; and

(ii) provide sufficient information and assistance to allow Axiata and other relevant member(s) of the Axiata Group to meet their respective obligations to report the Security Incident to the relevant authorities or inform the Data Subjects under the applicable privacy or data protection and other laws. The Company shall co-operate with Axiata, other relevant member(s) of the Axiata Group and the relevant authorities to take all reasonable steps to assist in the investigation, mitigation and remediation of the Security Incident.

3.2 The Company shall ensure that:

(a) all subcontracts, other supply chain arrangements and contracts with Sub-Processors, which may allow or cause access to Axiata Data, contain provisions that are at least as stringent as those in Clause 3.1 and this Clause 3.2 and do not contain any provisions that are inconsistent with these Cyber Security and Data Protection Terms and Conditions; and

(b) all the Company's Personnel who have access, directly or indirectly, to Axiata Data or Axiata Systems comply with Clause 3.1 and this Clause 3.2 as if the Personnel were the Company.

3.2 The Company shall store all Axiata Data and Confidential Information as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution.

3.3 In the event Company is dealing with Axiata Data and Confidential Information, the Company shall ensure that any and all electronic transmission or exchange of system and application data with Axiata and other member(s) of the Axiata Group and any other parties designated by Axiata shall take place via secure means (e.g. using S/MIME, HTTPS or SFTP or equivalent).

3.4 The Company shall at all times maintain network security that conforms to Best Industry Practice. At a minimum, network protection shall include:

(a) network firewall provisioning;
(b) strong user authentication;
(c) encrypted transmissions and storage;
(d) anti-malware programs;
(e) intrusion detection;
(f) controlled access to the physical location of computer hardware; and
(g) regular (two or more in each calendar year) third party vulnerability assessments.

4. Obligations relating to Data Protection

The Company shall:

(a) at all times comply with the Malaysian Personal Data Protection Act 2010 and legislation in other jurisdictions (collectively "**Personal Data Laws**") in respect of the Processing of Personal Data of Axiata and other members of the Axiata Group, including but not limited to Personal Data of the customers or employees of Axiata or other members of the Axiata Group;

(b) not do or omit to do anything that would cause Axiata or other members of the Axiata Group to contravene, or that would result in Axiata or other members of the Axiata Group contravening, any Personal Data Laws;

(c) only Process Personal Data of Axiata and other members of the Axiata Group for the sole purpose of supplying the Goods or to carry out the other tasks allocated to the Company in the Agreement, in accordance with the Agreement. The Company shall immediately notify Axiata and other relevant member(s) of the Axiata Group if the data Processing instruction infringes the applicable Personal Data Laws;

(d) not transfer, access or remotely access Personal Data of Axiata or other members of the Axiata Group without the prior written consent of Axiata and other relevant member(s) of the Axiata Group. The Company shall ensure that any transfer of, or remote access to, Personal Data of Axiata or other members of the Axiata Group does not contravene any provisions of the Agreement or any applicable Personal Data Laws and that the transfer of such Personal Data shall be encrypted over public and wireless network;

(e) not engage a Sub-Processor to Process any Personal Data of Axiata and other members of the Axiata Group or change any Sub-Processor without the prior written consent of Axiata and other relevant member(s) of the Axiata Group. Where the Company engages any such Sub-Processor, the Company shall ensure that the Sub-Processor adheres to the same obligations as the Company's obligations with respect to Axiata Data and Confidential Information in the Agreement. The Company shall be responsible for verifying the Sub-Processor's compliance and responsible to Axiata and other relevant member(s) of the Axiata Group for any non-compliance by any Sub-Processor with the aforesaid obligations or any applicable laws;

(f) ensure that if the Company or its Sub-Processor (where applicable) receives a complaint or any request (including any request for access to Personal Data) from any Data Subject or his/her agents, or from any authority, the Company must, without undue delay, inform Axiata and other relevant member(s) of the Axiata Group of the complaint or request. Upon request by Axiata or other relevant member(s) of the Axiata Group, the Company shall, without undue delay, supply the information to Axiata and other relevant member(s) of the Axiata Group to enable them to respond to such complaint or request. The Company shall not respond to these complaints or requests unless instructed in writing by Axiata;

(g) establish and maintain a record of Personal Data Processing activities in electronic form and shall furnish a copy of the up-to-date record to Axiata and other relevant member(s) of the Axiata Group upon request. Such record shall, at the minimum, contain the following information:

(i) types/categories of Personal Data Processed;

(ii) transfer details, including countries transferred to and the safeguards for the transfer;

(iii) information of the Sub-Processor and details of the Processing activity;

(iv) specific data security requirements;

(v) information of the Company and its Data Protection Officer or appointed officer responsible for the Processing of Personal Data; and

(vi) technical and organizational security measures employed by the Company to safeguard Personal Data.

(h) provide reasonable assistance to Axiata and other relevant member(s) of the Axiata Group with any data protection impact assessment and consultation with supervisory authority, when required by Axiata or other relevant member(s) of the Axiata Group; and

(i) assist Axiata and other relevant member(s) of the Axiata Group in any investigations, mitigation and remediation related to Personal Data Processed and in meeting any obligations to report any breach, outcome of investigations and any queries relating to the provision of the Goods or to carry out any other tasks allocated to the Company in the Agreement, to the relevant authorities.

5. Audit & Vulnerability Scans

5.1 Axiata and other relevant member(s) of the Axiata Group may conduct, or require a third party nominated by them to conduct, a security audit of the Company's facilities, safeguards, policies, procedures and security measures in place to protect the Axiata Data and Confidential Information at any time and from time to time during the Term, including if directed by the data protection authority or if necessary due to any accidental, unauthorized or unlawful access to, Processing, use or transfer of, or loss, misuse, damage or destruction of, any Axiata Data. The Company shall make available all information necessary to demonstrate compliance with the provisions of t the Agreement and Personal Data Laws and this includes access to the books, records, correspondence, accounts, and non-confidential supporting documentation such as Company's most current information security statement and digital forensic evidence.

.

5.2 Further to Clause 5.1 above, the Company may engage its own auditor, provided such auditor is acceptable to Axiata and other relevant member(s) of the Axiata Group, and shall furnish the auditor's report to Axiata and other relevant member(s) of the Axiata Group for their review. Subject to Clause 5.3, each Party will bear its own cost of audit pursuant to Clause 5.1 and Clause 5.2.

5.3 If the results of the security audits demonstrate that the Company has breached any of its obligations, or that the Company's safeguards and security measures in place to protect the Axiata Data or Confidential Information do not meet Best Industry Practice, or there is a reasonable risk of material security breaches, the Company shall (without limiting Axiata's rights and remedies):

(a) pay Axiata's and other relevant member(s) of the Axiata Group's costs associated with the security audit; and

(b) promptly take such steps as are necessary to remediate the issues identified in respect of the safeguards and security measures to the Best Industry Practice identified as adequate in the security audit and will provide to Axiata and other relevant member(s) of the Axiata Group regular status updates of such remediation. The frequency of such status updates will be agreed upon by the Company and Axiata and other relevant member(s) of the Axiata Group but in any event will be at least once every seven (7) days.

5.4 In addition, Axiata and other relevant member(s) of the Axiata Group may conduct periodic vulnerability scans of any network or site maintained by the Company that stores Axiata Data or Confidential Information. The Company shall take all reasonable steps to facilitate such scans by Axiata and other relevant member(s) of the Axiata Group and shall promptly remediate any vulnerability identified by Axiata and other relevant member(s) of the Axiata Group in the course of such scans.

6. Variation

Notwithstanding any other provision in the Agreement, Axiata may vary (including add to) these Cyber Security and Data Protection Terms and Conditions at any time or from time to time without any notice to the Company. The latest version of the Cyber Security and Data Protection Terms and Conditions: (a) will be published on https://www.axiata.com/our-business/suppliers (or such other website/webpage as may be determined by Axiata from time to time); and (b) shall supersede the immediately preceding version of the Cyber Security and Data Protection Terms and Conditions and be binding on the Company with effect from the date stated as the Effective Date set out at the top of the Cyber Security and Data Protection Terms and Conditions. In the event of any conflict or inconsistency between this Clause 6 and any provision in any other part of the Agreement, the former shall prevail.