Emirates NBD's Data Protection and Information Security Terms (the "Data Protection Schedule")

1. **Definitions:**

Unless otherwise defined herein, capitalized terms shall have the meanings set forth in the Agreement. For the sake of clarity, certain definitions in this Data Protection Schedule have been duplicated from the Agreement solely for ease of reference. In the event of any inconsistency or conflict between the definitions herein and those in the Agreement, the terms herein shall prevail unless expressly stated otherwise.

The following definitions shall be incorporated into this Data Protection Schedule:

"Central Bank" means the Central Bank of the United Arab Emirates;

"Data Protection Laws" means all Applicable Laws relating to data protection and privacy, the processing of Personal Data, that apply to a particular Party including without limitation, as amended or replace:

a) The Central Bank Law (Federal Law No. 14 of 2018) (United Arab Emirates).
b) Central Bank's Consumer Protection Regulation issued under Central Bank Notice No. 444 of 2021 (United Arab Emirates).
c) Central Bank Consumer Protection Standards issued under Notice No. 1158 of 2021 on Consumer Protection Standards (United Arab Emirates).
d) Federal Decree-Law No. 45/2021 On the Protection of Personal Data (PDPL) (United Arab Emirates).

"ENBD Data" means all data (including Personal Data), information, text, drawings, statistics, analysis and other materials embodied in any form relating to ENBD or any ENBD Company (and/or their respective customers) which may be supplied by Supplier, ENBD or any ENBD Company and/or which Supplier (and/or any Supplier sub-contractor) generates, collects, processes, stores or transmits in connection with this Agreement;

"Outsourcing Regulation" means the Outsourcing Regulation and Standards for Banks (Circular No. 14/2021) issued by the Central Bank of the UAE;

"Personal Data", "Personal Data Breach", "Processing", "Process", "Processed", "Processor", "Data Subject", "Data Controller" shall have the same meaning ascribed to them in the Data Protection Laws.

2. **Security Requirements;**

2.1 Supplier shall comply and shall procure that each of Supplier's personnel shall comply with the Information Security Schedule as set forth in Annex 1 to this Data Protection Schedule.

2.2 At the request of ENBD, the Supplier shall implement additional effective security measures if the security measures listed in Annex 1 of this Data Protection Schedule prove to be insufficient or if technical progress or legal changes so require. If the Supplier becomes aware that the measures implemented pursuant to clause 2.1 of this Data Protection Schedule are not sufficient or if technical progress or legal changes require further measure, the Supplier shall immediately notify ENBD in writing. All changes to security measures shall be documented by the Supplier.

2.3 Where the Supplier intends to implement alternative measure than those set out in Annex 1, ENBD shall be informed of the implementation of any alternative measures in advance. ENBD reserves the right to object to such proposed alternative measures and, where applicable, to require the Supplier to retain the existing measures and/or

implement a different set of alternative measures to ensure continued compliance with the measures set out in Annex 1.

2.4 Supplier shall co-operate with any investigation relating to security which is carried out by or on behalf of ENBD, including providing any information or material in its possession or control and implementing new security measures, to the extent reasonably requested by ENBD.

2.5 Supplier shall notify ENBD immediately in writing, and no later than 24 hours, upon becoming aware of any security breach or potential security breach. Upon the request of ENBD, Supplier shall, provide details of the security breach or potential security breach. Supplier shall notify ENBD in writing to dpo-grouplegal@emiratesnbd.com and cybersec@emiratesnbd.com.

2.6 Where Supplier is affected by a security breach or potential security breach, it shall take whatever action is necessary to minimise the impact of such event and prevent such events recurring. Supplier shall bear the cost of such action or preventative measures where the loss, damage or destruction or unauthorised access arises as a result of a breach by Supplier of its obligations under this Agreement.

2.7 Where the Supplier becomes aware of a security breach or potential security breach, it shall, without undue delay, provide ENBD with the following information:

2.7.1 Description of the nature, form, causes of the security breach, including the categories of in-scope data and approximate number of both Data Subjects and the data records concerned;

2.7.2 The likely consequences of the security breach; and

2.7.3 A description of the measures taken or proposed to be taken to address the security breach or potential security breach including measures to mitigate its possible adverse effects.

2.8 Immediately following any accidental, unathorized, or unlawful data processing or Personal Data Breach, the Parties will co-ordinate with each other to investigate the matter. Further, the Supplier will reasonably co-operate with ENBD at no additional cost to ENBD, in ENBD's handling of the matter, including but not limited to:

2.8.1 Assisting with any investigation;

2.8.2 Providing ENBD with physical access to any facilities and operations affected;

2.8.3 Facilitating interviews with the Supplier's employees, former employees and others involved in the matter including, but not limited to, its officers and directors; and

2.8.4 Making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Law or as otherwise reasonably required by ENBD.

3. **Data Protection;**

3.1 Each Party shall at all times comply with the Data Protection Laws and the Outsourcing Regulation (if applicable) in relation to the Processing of ENBD Data.

3.2 Where Supplier is Processing Personal Data as a Processor on behalf of ENBD, Supplier shall:

3.2.1 only undertake Processing of Personal Data reasonably required in connection with the Services and not for any other purpose or in a way that does not comply with this Agreement or Data Protection Laws;

3.2.2 implement appropriate technical and organisational measures to comply with Data Protection Laws;

3.2.3 only carry out the Processing on ENBD's written instructions, including in respect of any proposed international transfer of the Personal Data, and not for Supplier's own purposes or any other unauthorised purpose. ENBD reserves the right to submit to the Supplier a comprehensive list of instructions concerning the nature, extent, and method of processing. If Supplier is required to Process the Personal Data for any other purpose required by the Data Protection Laws or

any Applicable Law to which the Supplier is subject, Supplier shall inform ENBD in writing of this requirement before commencing the Processing, unless such law(s) prohibits this on grounds of public interest.

3.2.4 ensure that all instructions of ENBD are documented and that a copy of those instructions are provided on request to ENBD. Supplier shall notify ENBD immediately if the Supplier is reasonably of the opinion that an instruction of ENBD infringes any Data Protection Laws;

3.2.5 not disclose Personal Data to any Third Parties, unless such disclosure is made with prior written consent of ENBD and in accordance with the provisions of the Confidentiality clause in the Agreement;

3.2.6 limit access to Personal Data to authorised staff only and maintain logs for audit and supervisory purposes, recording the names of the staff who have accessed Personal Data databases and the timing. Such records must be provided to ENBD as and when requested;

3.2.7 ensure that all persons authorised by Supplier who have access to ENBD Data are subject to written contractual obligations concerning ENBD Data (including obligations of confidentiality) which are no less stringent than those imposed by this Agreement;

3.2.8 bring into effect and maintain reasonable technical and organisational measures to prevent unauthorised or unlawful Processing, access, copying, modification, reproduction, display, disclosure or distribution of Personal Data and accidental loss, disclosure or destruction of, or damage or alteration to, Personal Data including but not limited to taking reasonable steps to ensure the reliability of its employees having access to the Personal Data or use of encryption techniques to suitably encrypt Personal Data;

3.2.9 reasonably assist ENBD, at no additional cost to ENBD, with meeting ENBD's compliance obligations under the Data Protection Laws, (including assistance with requests from the appropriate supervisory authority) taking into account the nature of Supplier's Processing and information available to Supplier, including in relation to Data Subject rights and data protection impact assessments;

3.2.10 not sub-contract the Processing to any Third Party without the ENBD's prior written consent. In the event that ENBD (at its sole discretion) objects to the appointment of any additional or replacement sub-contractors, the Supplier shall agree any changes to the processing of ENBD Data as may be required to ensure that the objectionable sub-contractor does not process ENBD Data. Where ENBD does consent to Supplier engaging a sub-contractor to carry out any data Processing in connection with this Agreement, Supplier must enter into a written contract with such sub-contractor which shall include provisions in favour of ENBD which are the same as those in this clause 3 and as are required by applicable Data Protection Laws;

3.2.11 provide ENBD with such information as ENBD may reasonably require regarding the proposed sub-contractor including, without limitation, a copy of the contract (or draft contract, as the case may be) in place between the Supplier and the proposed sub-contractor, and information regarding the technical organizational measures implemented by the proposed sub-contractor.

3.2.12 use appropriate systems and procedures to ensure that any Personal Data which it Processes in the course of providing the Services are adequate, relevant, not excessive, accurate and, where necessary, kept up to date, and not retained for longer than is necessary;

3.2.13 immediately notify ENBD, and no later than 24 hours, as it becomes aware of any security breach, potential security breach and/or Personal Data Breach, and in any case, not later than twenty-four (24) hours after discovery of the breach relating to the Personal Data that the Supplier Processes in the course of providing the Services to ENBD. Supplier will restore such data at its own expense within 90 days;

3.2.14 provide employee training and awareness programs on the data control framework for accessing and handling Personal Data and reporting security and policy breaches. Supplier must promote the importance of protecting Personal Data as an ongoing responsibility of staff with reminders sent on an annual basis;

3.2.15 maintain, in accordance with the Data Protection Laws, a record of processing activities ('RoPA') with respect to Personal Data Processed on behalf of ENBD, which might include any ENBD Data, as well as a description of the categories of Personal Data held by Supplier, data of the persons authorised by Supplier to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and cross-border Processing of such data, as well as indicating the technical and organisational procedures related to information security and Processing operations; and

3.2.16 upon expiry or termination of this Agreement and at ENBD's instruction, securely destroy or return Personal Data to ENBD and delete existing copies at ENBD's sole option (unless any Applicable Law requires storage of the Personal Data) and provide written certification of the same to ENBD.

3.3 Supplier (or any Supplier sub-contractor) shall not transfer or otherwise Process ENBD Data, in countries outside of the UAE without obtaining ENBD's prior written consent. Where such consent is granted, Supplier may only Process, or permit the Processing involving the transfer of ENBD Data under the following conditions:

3.3.1 Supplier will not transfer or otherwise Process ENBD Data in a jurisdiction that cannot provide the same level of safeguarding that would apply if the ENBD Data was kept in the UAE. Supplier shall take all measures necessary to ensure that processing of ENBD Data will meet the requirements of Data Protection Laws and ensure the protection of the rights of all relevant Data Subjects;

3.3.2 Supplier will not store ENBD Data in any jurisdiction where bank secrecy, or other Laws, restrict or limit access to data necessary for supervisory purposes;

3.3.3 nothing alters or shall be construed as altering the ownership of the ENBD Data, which shall be retained by ENBD or its customers (as the case may be) at all times;

3.3.4 Supplier will allow ENBD and the Central Bank to access ENBD Data upon request; and

3.3.5 Supplier will permit ENBD and/or its Third-Party representatives to audit Supplier's compliance with its obligations under this Agreement, on at least one month's notice, during the term of this Agreement. If any audit or inspection reveal a material non-compliance by the Supplier with its obligations under Data Protection Laws or a breach by the Supplier of this Agreement, the Supplier shall pay the reasonable costs of ENBD or its mandated auditors of the audit or inspection.

3.4 Supplier will give ENBD and its Third-Party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

3.4.1 physical access to, remote electronic access to, and copies of records and any other information held at Supplier's premises or on systems storing the Personal Data;

3.4.2 access to and meetings with any of Supplier's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

3.4.3 inspection of all records and the infrastructure, electronic data or systems, facilities, equipment, or application software used to store or Process the Personal Data.

3.5 The subject matter of the data processing carried out by Supplier pursuant to this Agreement is the provision of the Services. The Data Processing Schedule (attached as Annex 2 to this Data Protection Schedule) sets out the nature, duration and

purposes of the Processing, the types of Personal Data that the Supplier Processes and the categories of Data Subjects whose Personal Data is Processed.

3.6 Supplier must notify ENBD immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the Processing of the Personal Data or to either party's compliance with the Data Protection Laws.

3.7 ENBD may, at reasonable intervals, request a written description of the technical and organisational methods employed by Supplier and/or the sub-contractors referred to in this clause. Within thirty (30) days of such a request, Supplier shall, at its own cost, supply written particulars of all such measures detailed to a reasonable level such that ENBD can determine whether or not in connection with the Personal Data, it is compliant with the Data Protection Laws.

3.8 Supplier shall maintain adequate policies, frameworks and controls for the protection and management of Personal Data to a similar standard of those of ENBD. Supplier shall also take reasonable steps to inform its personnel, and any other person acting under its supervision of the responsibilities of any Data Protection Laws and ensure the reliability of such persons who may come into contact with, access or Process Personal Data.

3.9 Where Personal Data is stored and retained outside of the ENBD System, Supplier agrees to use and maintain encryption techniques to suitably encrypt Personal Data for the secure transfer of Personal Data.

3.10 The Supplier shall indemnify ENBD against any loss, liability, damage, and expense incurred as a result of a Personal Data Breach or breach of Data Protection Law by the Supplier, its affiliates, sub-contractors or authorised Third Parties.

3.11 Where ENBD has obtained express consent from the Data Subject to share Personal Data with Supplier, Supplier has no further right to share the Personal Data or process it for other unauthorized purposes unless required by the Data Protection Laws or any Applicable Law.

Annex 1 – Information Security Schedule

1.1 Introduction

This Information Security Schedule (the "Information Security Schedule") sets forth the information security requirements applicable to third-party service providers, including, but not limited to, Commercial Off-The-Shelf (COTS) software providers, resellers, implementation partners, suppliers providing professional services, suppliers providing business process outsourcing services, Infrastructure as a Service(IaaS) providers ,Platform as a Service (PaaS) providers, Software-as-a-Service (SaaS) providers, and any other suppliers (collectively, the "Supplier(s)") engaged by Emirates NBD Group ("ENBD").

The intent of this Information Security Schedule is to ensure that the Supplier implements and maintains appropriate administrative, technical, and physical safeguards to protect ENBD Data and/or to ensure the confidentiality, integrity, and availability of information assets used in the delivery of Services under this Agreement. These requirements are designed to address evolving cybersecurity threats, regulatory obligations, and industry best practices, and apply regardless of the nature of the Services provided, the deployment model used.

1.2 Information Security Requirements

1. Information Security Governance

1.1 Supplier shall implement, maintain, and continuously improve an information security management system (ISMS) aligned with industry-recognized standards (e.g., ISO/IEC 27001, NIST CSF, or equivalent). Evidence of certification or compliance shall be provided by the Supplier upon ENBD's request.

1.2 Supplier shall assign a qualified individual for ensuring compliance with information security obligations outlined in this Information Security Schedule and shall notify ENBD of any change to the assignment.

1.3 Supplier shall ensure that information security governance includes oversight mechanisms and risk-based decision-making for activities related to information assets used in the delivery of the Services under this Agreement.

1.4 Supplier shall maintain communication channels and reporting mechanisms to ensure transparency and compliance with ENBD's information security governance requirements.

2. Risk Management

2.1 Supplier shall establish, maintain, and operate a documented Risk Management Framework to identify, assess, mitigate, and monitor risks associated with the delivery of Services under this Agreement or/and protection of ENBD Data.

2.2 Supplier shall implement risk governance practices that promote transparency, accountability, and communication of risk posture with respect to the Services provided to ENBD.

2.3 Supplier shall align its risk management framework with internationally recognized standards) and where relevant, comply with any applicable legal and regulatory requirements affecting the Services.

3. Security Awareness

3.1 Supplier shall implement and maintain a formal Security Awareness and Training Program to ensure all personnel involved in the delivery, support, or administration of the Services under this Agreement are aware of their information security responsibilities and can protect ENBD Data and systems from accidental or intentional compromise.

3.2 Supplier shall ensure that personnel with elevated privileges (e.g., system administrators, developers) receive additional role-specific security training, covering secure coding, system administration and secure posture management, change management, and access control best practices.

3.3 Supplier shall implement ongoing awareness initiatives, such as simulated phishing campaigns, regular bulletins, refresher content, etc. to reinforce secure behavior and reduce human risk.

4. Background Checks

4.1 Supplier shall maintain comprehensive hiring/recruitment policies/procedures for its employees, contractors, or consultants, which include, among other things, a background check for criminal convictions to the extent permitted by Applicable Law. Supplier further represents that, through its hiring/recruitment policies/procedures, it endeavour's to employ the best qualified people of appropriate character and honesty. ENBD reserves the right to audit the process used for such screening. The Supplier ensures that all personnel authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Data Usage

5.1 Supplier shall ensure ENBD Data is processed in accordance with Applicable Laws and shall not use ENBD Data for any purpose other than providing the agreed Services.

5.2 Supplier shall not use, access, retain, or repurpose any ENBD Data, whether in raw, aggregated, derived, or anonymized form for the purposes of analytics, profiling, marketing or advertising, or training, fine-tuning, testing, or developing any artificial intelligence (AI), machine learning (ML), or generative models (including large language models), or for any other purpose, unless explicitly agreed to in writing by ENBD.

5.3 Supplier shall not disclose, transmit, or otherwise make available any data, information, reports, or materials relating to ENBD, its customers, or this Agreement to any customer of ENBD or to any third party without ENBD's prior written consent. The type, scope, format, and purpose of any such disclosure must be explicitly discussed with and approved by ENBD in writing prior to any such disclosure.

5.4 Supplier shall ensure that any approved disclosures are limited to the minimum necessary information and are made in accordance with all applicable confidentiality, data protection, and regulatory requirements. Unauthorized disclosure will be considered a material breach of this Agreement.

6. Data Security

6.1 Supplier shall at all times have appropriate technical and organizational measures in place to protect Personal Data and any other ENBD Data against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to Personal Data or any other ENBD Data held or processed by it and shall take reasonable steps to ensure the reliability of any of its personnel who will have access to ENBD

Data, especially Personal Data processed in accordance with the terms prescribed in the Data Protection section of this Data Protection Schedule.

6.2 Supplier shall implement and adhere to a data classification framework that ensures all ENBD Data which gets processed, transmitted, or stored in their systems and environment is handled according to its sensitivity level.

6.3 Supplier shall implement and enforce a Clear Desk and Clear Screen Policy to protect ENBD Data or any other data in relation to the Services under this Agreement from unauthorized access, loss, or disclosure.

6.4 Supplier shall implement and maintain robust encryption and key management practices to protect ENBD Data including encryption keys, passwords, access tokens, and other authentication credentials, in accordance with best industry standards and applicable legal or regulatory requirements.

6.5 Where technically feasible or/and if a regulatory mandate is in place, ENBD may request the use of ENBD-Managed Keys (CMKs) or a Bring Your Own Key (BYOK) model. Supplier shall support integration with the ENBD's key management infrastructure and ensure full segregation and control of keys.

6.6 All ENBD Data, whether at rest or in transit, shall be protected using strong encryption (e.g., AES-256 for data at rest, TLS 1.2 and above for data in transit).

6.7 Supplier shall implement robust Data Loss Prevention (DLP) controls across all environments, including endpoints, network, email, cloud, and storage systems used to process, store, or transmit ENBD Data and provide assurance on the control effectiveness to ENBD on an annual basis or upon request.

6.8 Supplier shall implement and maintain secure data backup procedures to ensure the availability and recoverability of data or/and critical system components in relation to the Services under this Agreement.

7. Data Residency and Sovereignty

7.1 Supplier shall ensure that ENBD Data, including backups and metadata, is stored, and processed within the UAE, unless explicit written approval is provided by ENBD or relevant regulatory authority.

7.2 Supplier shall not engage any sub-processor or allow any cross-border access to ENBD Data unless the sub processor is disclosed and approved in writing by ENBD, and the Supplier has imposed terms on the sub-processor as required under this Agreement which may include equivalent terms on matters such as data protection, information security, residency, and confidentiality.

8. Data Retention and End-of-Service Data Handling

8.1 Supplier shall retain ENBD Data only for as long as necessary to fulfil the purposes of this engagement, or as required by applicable laws, regulations, or contractual obligations.

8.2 Upon termination or expiration of this Agreement, for any reason, Supplier shall make available all ENBD Data in a commonly used, machine-readable, structured format (e.g., CSV, JSON, XML, or other agreed format) to allow for seamless data portability to ENBD or an alternate service provider where relevant and as requested by ENBD.

8.3 Supplier shall ensure that the exported data is complete, usable, and accompanied by documentation sufficient to enable ENBD to interpret and import the data into another system, without reliance on proprietary tools.

8.4 Following successful transfer, Supplier shall retain ENBD Data for a period not exceeding thirty (30) days, after which the data stored in either physical or electronic form must be deleted or destroyed in a way that the ENBD Data is not recoverable.

8.5 Supplier shall provide a certificate of destruction to ENBD post completion of the above activity.

8.6 Supplier shall establish policies and procedures with supporting business processes and technical measures implemented for the secure disposal and complete removal of ENBD Data from all storage media, ensuring ENBD Data is not recoverable by any computer forensic means.

9. Malware and Threat Protection

9.1 Supplier warrants and represents that:

9.1.1 the Software will be malware free at the point of delivery and at all times during updates for usage by ENBD and will not contain any backdoors; and

9.1.2 the equipment involved in any secondary storage associated with it will be malware free at the point of delivery/return.

9.2 All software used by Supplier while providing the Services to ENBD must be properly inventoried and licensed.

9.3 Supplier shall implement automated and effective malware evaluation mechanisms to inspect all files uploaded by users, third parties, or system integrations through the platform or applications related to the Services under this Agreement.

10. Endpoint Protection

10.1 Supplier shall implement and enforce robust endpoint security controls to protect all devices (including laptops, desktops, mobile devices, virtual machines, and administrative consoles) used to access, process, store, or transmit ENBD Data or to manage systems and services related to this Agreement.

10.2 Supplier shall ensure that all endpoints used to deliver the Services under this Agreement are protected with industry-standard anti-malware, firewall, and endpoint detection and response (EDR) tools, hardened in accordance with best practices, and configured with full-disk encryption. Supplier shall further ensure that all endpoints related to the Service are regularly patched with the latest security updates and all installed applications, are monitored for compliance and security threats through centralized management and logging tools.

10.3 Supplier shall conduct periodic assurance activities to verify the effectiveness of its endpoint protection controls and provide assurance and/or evidence to ENBD on an annual basis or upon ENBD's request.

11. Access Control

11.1 Supplier shall implement strict role-based access controls to ensure that only authorized personnel have access to ENBD Data and/or systems.

11.2 Supplier shall conduct periodic access reviews for all accounts and entitlements associated with ENBD's systems, ENBD Data, and services.

11.3 Supplier shall implement a robust Privileged Access Management (PAM) framework to govern the use, monitoring, and control of privileged accounts accessing systems or data associated with ENBD.

11.4 Supplier personnel shall only be granted access to ENBD Data based on a least-privilege, time-bound, and approval-based model.

11.5 Supplier shall implement Multi-Factor Authentication (MFA) to ensure secure access to all systems, platforms, and environments where ENBD Data is stored, processed, or transmitted.

11.6 Supplier shall implement and maintain comprehensive physical access controls to protect all facilities, systems, and infrastructure involved in the processing, storage, or transmission of ENBD Data from unauthorized physical access, damage, or interference.

12. Secure Software Development and Maintenance

12.1 Supplier shall adopt secure software development lifecycle (SDLC) practices, including secure coding standards, regular code reviews, static and dynamic testing, and patch management for the development and maintenance of all applications involved in the delivery of the Services under this Agreement.

12.2 Supplier shall conduct formal threat modelling activities as part of its secure software development lifecycle (SSDLC) to identify, assess, and mitigate security threats and vulnerabilities that may impact the confidentiality, integrity, and availability of ENBD Data and/or information assets involved in the delivery of the Services under this Agreement.

12.3 Supplier shall disclose the use of all third-party, proprietary, and open-source software components and cryptographic algorithms within the product and ensure their licenses do not impose obligations or risks on ENBD. Upon request, a Software Bill of Materials (SBOM) and a Cryptographic Bill of Materials (CBOM) shall be provided to ENBD by the Supplier.

12.4 Supplier shall maintain a complete, accurate, and up-to-date Software Bill of Materials (SBOM) and a Cryptographic Bill of Materials (CBOM) for all software products, components, libraries, and dependencies used in the solution or the Service provided to ENBD.

12.5 The SBOM and CBOM shall be maintained in a machine-readable format (e.g., SPDX, CycloneDX, or SWID) aligned with industry standards such as NTIA, OWASP, or OpenSSF.

12.6 Supplier shall use the SBOM and CBOM to proactively identify and address security risks related to software components, including licensing and vulnerability exposures.

12.7 ENBD reserves the right to audit and validate the accuracy and completeness of the SBOM provided by the Supplier and require corrective actions where gaps or inconsistencies are found.

13. Vulnerability Management and Penetration Testing

13.1 ENBD reserves the right to undertake a security review of the Supplier's applications and infrastructure used for the delivery of the Service through a vulnerability assessment and/or penetration testing or source code review or any other testing method, henceforth known as "Security Assessment" either through its own resources or outsourcing via a Third Party before the system goes live and once annually thereafter or more frequently (if defined so in the Service Levels).

13.2 Supplier will cooperate with ENBD, and any Third Party contracted to undertake a Security Assessment of the Services by providing the necessary documentation, source code (where feasible & agreeable), demonstration of the application and any other means required by ENBD. Supplier will allow vulnerability assessment /penetration testing to be carried out by a supplier of ENBD's choice at periodic intervals or as required.

13.3 Supplier will fix every security issue identified and reported by ENBD and / or the Third-Party agency contracted to do the testing, at Supplier's own cost, unless otherwise agreed by ENBD.

13.4 In accordance with clause 13.5 of this Information Security Schedule, all security issues rated as Critical or High (as rated by ENBD) during assessment must be fixed before the Services go live or are rolled out to end-users and those rated as Medium and Low must be fixed as per the timelines given in clauses 13.5.2 and 13.5.3.

13.5 Any identified security vulnerabilities reported to the Supplier via responsible disclosure either by ENBD or non-ENBD, shall be fixed as per the below:

13.5.1 Vulnerabilities that are rated Critical or High (CVSS Base Score of six (6) to ten (10)) shall be remediated by Supplier within seven (7) Business Days;

13.5.2 Vulnerabilities that are rated Medium (CVSS Base Score of three (3) to five point nine (5.9) shall be remediated by Supplier within fifteen (15) Business Days; and

13.5.3 Vulnerabilities that are rated Low (CVSS Base Score of zero (0) to two point nine (2.9) for public facing assets shall be remediated by Supplier within thirty (30) Business Days. Vulnerabilities that are rated Low (CVSS Base Score of zero (0) to two point nine (2.9) for non-public facing assets shall be remediated by Supplier as per the Supplier's vulnerability assessment framework.

13.6 The ratings referred to in clauses 13.5.1, 13.5.2 and 13.5.3 are calculated based on the base scores of the Common Vulnerabilities Scoring System (CVSS).

13.7 Any costs associated with remediating the vulnerabilities referenced above shall be borne by Supplier.

13.8 Supplier confirms that its products are tested for weaknesses via methods such as vulnerability assessment, regular penetration testing, red team exercises and scans that check for compliance against the baseline security standards or best security practices, before the new product or any of its releases is delivered to ENBD.

13.9 Supplier will conduct annual Third-Party penetration tests against Internet-accessible infrastructure components and the services exposed to internet through an independent accredited security-oriented services provider. Upon ENBD's request, Supplier will provide summary reports to provide assurance on the security of its infrastructure and applications in scope.

14. Change Management

14.1 Supplier shall implement a formal, documented change management process aligned with industry standards to control all changes to the systems, applications, infrastructure, and services that may affect the security, availability, or integrity of ENBD Data.

14.2 Supplier shall perform a formal security impact assessment as part of the change evaluation process to identify potential information security risks. Changes that may affect data confidentiality, integrity, availability, or compliance obligations must include mitigation strategies and documented risk acceptance where applicable.

15. Data centre Security

15.1 Supplier shall ensure that all data centers used to host, process, or store ENBD Data or systems under this Agreement are secured with robust physical, environmental, and operational controls aligned with industry best practices and international standards.

15.2 All data centers shall implement the following minimum safeguards:

15.2.1 24x7 physical security including perimeter fencing, surveillance (CCTV), intrusion detection, and manned security presence;

15.2.2 Access control mechanisms such as biometric authentication, access cards, visitor logging, and strict authorization procedures;

15.2.3 Environmental controls including fire detection and suppression systems, temperature/humidity monitoring, and uninterruptible power supply (UPS) with generator backup to ensure high availability and business continuity;

15.2.4 Redundant systems for power, networking, and storage to ensure fault tolerance and service uptime;

15.2.5 Monitoring and alerting systems to detect physical and logical anomalies, with real-time response and escalation protocols; and

15.2.6 Logical data segregation for multi-tenant environments to ensure ENBD Data is securely isolated from other clients.

15.3 Supplier shall ensure that all data centers comply with relevant industry certifications and independent audit reports, including ISO/IEC 27001, uptime institute Tier III, SOC 2 Type II, or equivalent and ensure that these are provided to ENBD on an annual basis or upon request.

16. Network Security

16.1 Supplier shall ensure that systems processing or storing ENBD Data are logically or physically segregated from other environments. Multi-tenant architectures must implement strict access controls and isolation mechanisms to prevent data leakage or unauthorized access between tenants.

16.2 All critical network boundaries shall be protected by firewalls and intrusion detection systems (IDS) or intrusion prevention systems (IPS). These must be configured based on the principle of the least privilege and reviewed regularly to ensure only necessary traffic is permitted.

16.3 All data transmitted over public or untrusted networks shall be encrypted using robust, industry-standard protocols (e.g., TLS 1.2 or higher, SSH). Insecure protocols (e.g., FTP, Telnet) must be disabled unless justified and mitigated with compensating controls.

16.4 Supplier shall continuously monitor its network for suspicious activity, unauthorized access attempts, and performance anomalies. Network logs shall be retained for a minimum of 12 months and made available to ENBD upon request for audit, investigation, or compliance purposes.

16.5 Any access to Supplier's internal network or administrative systems must be protected using secure communication protocols with access control lists (ACL's), multi factor authentication (MFA) and role-based access control (RBAC) implemented. Access must be granted only to authorized personnel on a need-to-know basis and reviewed periodically.

16.6 Supplier agrees to implement and maintain robust email security measures to protect the confidentiality, integrity, and availability of all information exchanged via email under this Agreement. Such measures shall include, but are not limited to, the use of encryption protocols (e.g., TLS) for email transmission, implementation of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) to prevent spoofing and unauthorized use of domains.

17. Security Monitoring

17.1 Supplier shall implement and maintain continuous 24 hours per day, 7 day per week security monitoring of all systems, applications, and infrastructure used to process, store, or transmit ENBD Data.

17.2 Monitoring shall include real-time detection and alerting of unauthorized access, anomalous behaviour, and security threats.

17.3 Supplier shall ensure that all access to ENBD Data which is stored or processed in their environment shall be logged with timestamp, user identity, and action taken.

17.4 Logs and events must be retained for a minimum of 12 months and made available to ENBD upon request.

17.5 Supplier shall promptly investigate security alerts and notify ENBD of any confirmed or suspected security incidents.

17.6 Supplier shall regularly assess and update its threat intelligence practices and ensure that third parties or subcontractors involved in service delivery are held to equivalent threat monitoring standards. Upon request, Supplier shall provide ENBD with evidence of threat intelligence integration, summaries of significant threat alerts, and response actions taken.

17.7 ENBD reserves the right to review the Supplier's threat intelligence approach as part of its audit or security governance processes.

17.8 Supplier shall establish and maintain a threat intelligence capability to proactively identify, assess, and respond to emerging cyber threats relevant to the Services provided to ENBD.

17.9 Supplier shall subscribe to and monitor reputable commercial, opensource, governmental, and industry-specific threat intelligence sources to stay informed of adversary tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and threat actor activity that may impact the confidentiality, integrity, or availability of ENBD's systems or ENBD Data.

17.10 Threat intelligence shall be integrated into Supplier's security operations, including security incident and event monitoring, endpoint protection, vulnerability management, and incident response processes.

17.11 Supplier shall promptly notify ENBD within 24 hours of discovering any credible threat or campaign that may affect the ENBD's environment, including any relevant IOCs, impacted components, and recommended mitigation or containment actions.

18. Security Incidents

18.1 Supplier will inform ENBD of any security/Data Breaches or incidents or serious vulnerabilities in its environment/product as soon as possible and in any event no later than twenty-four (24) hours or sooner as required by the local regulation/s, after having become aware of the breach. Supplier should provide, at the minimum, a summary of the incident, type of information involved, and immediate steps taken to mitigate the incident.

18.2 In the event of a security incident or breach involving the Supplier and/or any of its subcontractors, agents, or/and other third parties engaged in the performance of the Supplier's obligations hereunder ("Downstream Parties"), the Supplier shall, at its own cost and within ten (10) business days of such breach (or sooner if required by the nature or urgency of the breach), provide a detailed written Root Cause Analysis ("RCA").

The RCA shall:

18.2.1 Identify the root cause(s) of the breach, including any contributing actions, omissions, or failures by the Supplier and any Downstream Parties;

18.2.2 Describe in detail the timeline of events leading to the breach;

18.2.3 Include the names and roles of all involved parties;

18.2.4 Specify immediate corrective actions taken;

18.2.5 Propose preventive measures to avoid recurrence; and

18.2.6 Be reviewed and approved by ENBD, who may request clarifications or additional information as reasonably necessary.

Supplier shall fully cooperate with ENBD in the investigation and shall ensure that all relevant Downstream Parties also provide the necessary information and access to facilitate the RCA process.

18.3 Supplier shall report any incidents or anomalies that could potentially impact ENBD Data or operations immediately to cybersec@emiratesnbd.com and dpo@emiratesnbd.com.

18.4 Failure to comply with clauses 18.1, 18.2 and 18.3 by the Supplier may be deemed as a material breach of this Agreement.

19. Cyber Insurance

19.1 In addition to the insurance requirements in the Agreement, Supplier shall, at its own cost, for the duration of this Agreement and for a period of at least twelve [12] months thereafter, maintain appropriate cyber liability insurance covering losses arising from data breaches, network interruption, unauthorized access, or disclosure of confidential or personal data, malware or ransomware attacks, cyber extortion and business interruption due to cyber incidents. Such insurance shall include coverage for third-party claims, regulatory investigations, breach response costs including legal, forensic, notification, credit monitoring, and public relations, and liability for the Supplier's subcontractors, if applicable. Supplier shall provide ENBD with a valid certificate of insurance upon request and shall ensure that the insurance policy is not cancelled or materially altered without at least thirty (30) days' prior written notice to ENBD. This insurance requirement shall not limit or reduce the Supplier's liability under this Agreement.

20. Audit Rights

20.1 The audit rights set forth in clause 25 of the Agreement shall apply in full to this Information Security Schedule. Without limiting the generality of the foregoing, any rights granted to ENBD under the Agreement to audit or inspect the Supplier's compliance with the Agreement shall extend to include the Supplier's compliance with this Information Security Schedule, including but not limited to any technical and organizational security measures implemented by the Supplier. All such audits shall be conducted in accordance with the terms, conditions, and limitations specified in the Agreement. For the avoidance of doubt, any right of audit for ENBD pursuant to the Agreement shall include but is not limited to a right to audit the Supplier on-site at its or any of its third-party subcontractor's premises.

21. Compliance

21.1 Supplier shall adhere to applicable requirements from ENBD and under Applicable Laws, Regulations, Standards and Guidelines (the "Standards"). In the event of a breach or a crime, fraud and/or corruption, ENBD reserves the right to institute an appropriate disciplinary process to take any action or legal proceeding against Supplier.

21.2 Supplier shall, notify ENBD where cloud-based systems are used as part of the provision of the Services and provide evidence that it is compliant with the requirements of the Telecommunications and Digital Government Regulatory Authority (formerly the TRA) UAE Information Assurance Regulation,

21.3 Supplier shall provide ENBD with a copy of the available infosec certifications such as ISO27001 and the latest independent security audit report SOC 2 Type 2 or equivalent on an annual basis.

21.4 Where applicable, Supplier shall collaborate with ENBD to define, document, and agree upon a shared responsibility model that clearly delineates the security, compliance, and operational responsibilities of each Party based on the specific cloud deployment model (e.g., IaaS, PaaS, SaaS) used to deliver the Services. This model shall identify the division of responsibilities across key security domains including, but not limited to, data protection, identity and access management, infrastructure security, application security, and incident response and shall align with industry standards such as ISO/IEC 27017 or applicable regulatory requirements. The shared responsibility model shall be reviewed and updated periodically, and whenever there is a material change in the Services, architecture, or underlying cloud environment.

21.5 To the extent the Supplier processes, stores, or transmits cardholder data or sensitive authentication data on behalf of ENBD, or otherwise has access to such data or systems that handle it,

21.5.1 Supplier understands and agrees that it is responsible for the security of the functions that impact the security of ENBD's cardholder data environment.

21.5.2 Supplier agrees that, as of the Effective Date, it has complied with all applicable requirements to be considered PCI DSS compliant and has performed the necessary steps to validate its compliance with the PCI DSS.

21.5.3 Supplier agrees to supply the present status of the Supplier's PCI DSS compliance status, and evidence of its most recent validation of compliance to ENBD at least annually or upon request.

21.5.4 Supplier will immediately notify ENBD if it learns that it is no longer PCI DSS compliant and will immediately provide ENBD the steps being taken to remediate the non-compliance status. In no event should the Supplier's notification to ENBD be later than seven (7) calendar days after the Supplier learns it is no longer PCI DSS complaint.

22. Downstream Parties

22.1 The Parties acknowledge and agree this clause 22 shall be subject to the terms of clause 23 in the Agreement (Assignment and Subcontracting). Supplier shall enforce the compliance of its published security controls on its Downstream Parties and maintain back-to-back service level agreements to meet the agreed Service Levels of ENBD, if and where applicable.

22.2 Supplier shall ensure that all Downstream Parties are contractually bound to comply with information security, confidentiality, and data protection obligations that are at least as equivalent to as those defined in this Agreement.

22.3 Supplier shall conduct due diligence and risk assessments on all subcontractors and Downstream Parties, including evaluations of their technical and organizational security controls, prior to engagement and at least annually thereafter.

22.4 Supplier shall implement and maintain robust supply chain risk management practices to identify, document, and continuously monitor all Downstream Parties involved in the delivery or support of Services under this Agreement.

22.5 Supplier shall ensure that all Downstream Parties notify the Supplier of any actual or suspected security incidents affecting ENBD Data or systems immediately, and that ENBD is notified within 24 hours.

22.6 ENBD reserves the right to conduct an offsite or onsite audit or require audit evidence of any Downstream Parties engaged by the Supplier, either by ENBD or through an authorized third party, to ensure compliance with this Agreement's security requirements.

22.7 Supplier shall ensure that all Downstream Parties enforce strong access control measures, including individual user IDs, role-based access, multi-factor authentication, and logging of all access to ENBD systems or ENBD Data.

22.8 Supplier shall ensure that Downstream Parties only access, store, or process ENBD Data in jurisdictions that have been explicitly approved by ENBD and are subject to applicable Data Protection Laws.

22.9 Upon termination or expiry of the Agreement, Supplier shall ensure that all Downstream Parties return or securely delete all ENBD Data in accordance with NIST SP 800-88 or equivalent standards and provide certification of destruction.

22.10 If the Supplier is acting as a reseller, the Supplier shall ensure that a formal agreement is in place between the Supplier and the Original Equipment Manufacturer or the Original Service Provider (collectively referred to as the "OEM") which governs the provision of services to ENBD. This agreement must incorporate all applicable ENBD information security requirements. ENBD reserves the right to review this agreement and to assess the OEM's information security posture and compliance with ENBD's information security requirements. Such assessments may include remote or on-site audits.

22.11 Supplier shall remain fully liable to ENBD for any actions, omissions, or breaches by its Downstream Parties in connection with this Agreement.

Annexure: Service Level Requirements

The Service Levels that should be abided by the Supplier are given below:

#	Service / Activity	Description	Trigger	Responsible	Service Level
Cyber and Information Security					
1	Security Incidents *Criticality Level 1 - Severe*	Very significant impact / threat to the organisation's reputation, financial stability, or public safety due to e.g., ransomware attacks, critical infrastructure disruptions, data breaches of large volumes of sensitive information	Upon Notification by the Supplier (Via E-mail and / or Authorised Call & Chat Channels)	Supplier	Response: **0-10 minutes** Resolution: **0-2 hours** Notification upon identification : **0-2 hours**
2	Security Incidents *Criticality Level 2 – High*	Significant impact / threat to the organisation due to e.g., significant data breaches of large-scale malware outbreaks	Upon Notification by the Supplier (Via E-mail and / or Authorised Call & Chat Channels)	Supplier	Response: **0-30 mins** Resolution: **6 hours** Notification upon identification : **6 hours**
3	Security Incidents *Criticality Level 3 – Medium*	Medium impact / threat to the organisation due to e.g., malware infections, phishing attacks, unauthorised	Upon Notification by the Supplier	Supplier	Response: **0-2 hours** Resolution: **16 hours**

#	Service / Activity	Description	Trigger	Responsible	Service Level
		access, DoS attacks or insider threats	(Via E-mail and / or Authorised Call & Chat Channels)		Notification upon identification : **12 hours**
4	Security Incidents *Criticality Level 4 – Low*	Low impact / threat to the organisation due to e.g., routine malware infections, minor policy violations, low-level phishing attacks	Upon Notification by the Supplier (Via E-mail and / or Authorised Call & Chat Channels)	Supplier	Response: **0-4 hours** Resolution: **48 hours** Notification upon identification : **24 hours**
5	Security Operations Center Monitoring	The Supplier must constantly monitor the security elements of the operational centres and to provide reports of the same to ENBD upon request.	To be performed Daily by the Supplier	Supplier	Monitoring Frequency: **24X7** Reporting: **Upon request from ENBD**
6	Periodic Vulnerability Scanning	The Supplier must scan their infrastructure and system applications on a recurring basis and to provide reports of the same to ENBD upon request.	To be performed Monthly by the Supplier	Supplier	Scanning Frequency: **Monthly** Reporting: **Upon request from ENBD**
7	Vulnerability Remediation	Any identified security vulnerabilities shall be addressed and neutralised within a reasonable timeframe by the Supplier depending on its criticality as per the CVSS base scoring. CVSS base scoring scales are as the following: Critical & High: 6-10 Medium: 3-5.9 Low:0-2.9	Upon Notification by the Supplier (Via E-mail and / or Authorised Call & Chat Channels)	Supplier	Resolution - *Critical and High:* **7 business days** Resolution- *Medium:* **15 business days** Resolution- *Low:* **30 business days**
8	Penetration Testing	The Supplier shall conduct yearly penetration testing through an independent party for the Services in	Upon Submission by the Supplier	Supplier	Reporting Period: **Yearly or upon ENBD request**

#	Service / Activity	Description	Trigger	Responsible	Service Level
		scope and share the testing report with ENBD.	(Via E-mail and / or Authorised Call & Chat Channels)		
9	External Audits & Assessments (SOC 2 type II & ISO 27001:2022)	The Supplier shall conduct yearly external audits and assessments for the Services in scope and share the audit and assessment reports with ENBD.	Upon Submission by the Supplier (Via E-mail and / or Authorised Call & Chat Channels)	Supplier	Reporting Period: **Yearly**

Annex 2 – Data Processing Schedule

1. This Annex 2 includes certain details of the Processing of the Personal Data as required by the Data Protection Laws. ENBD and the Supplier agrees and acknowledges that for the purpose of the Data Protection Laws ENBD is the Data Controller, and the Supplier is the Data Processor.

2. The subject matter of the processing is the Personal Data provided in respect of the Services under the Agreement.

3. The duration of the processing is the duration of the provision of the Services under the Agreement until disposal of the Personal Data in accordance with the Agreement.

4. The nature and purpose of the processing is in connection with the provision of the Services under the Agreement.

5. The types of Personal Data processed are those submitted to the Supplier by or at the direction of ENBD as part of the Services.

6. The categories of Data Subjects are those whose Personal Data is submitted to the Supplier by or at the direction of ENBD as part of the Services.