SUPPLIER PRIVACY AND SECURITY TERMS

These Supplier Privacy and Security Terms establish Kyndryl's and Supplier's rights and obligations on data governance, security and related matters (the "**Terms**"). The Terms are incorporated into, and made a part of, the Supplier Relationship Agreement (or equivalent agreement) between the parties, including Statements of Work, Work Authorizations, or other documents between our companies that refer to them (the "**Transaction Documents**").

These Terms consist of:

- This document,
- The Processing Details Exhibit attached to this document outlines the Supplier's data processing activities as of the execution of these Terms (for any Transaction Documents entered into after these Terms are executed, a separate Processing Details Exhibit will be attached to each Transaction Document, documenting the Supplier's processing activities specific to that document), and
- The EU Standard Contractual Clauses, UK International Data Transfer Addendum, and Supplier Transfer Impact Assessment found at https://www.kyndryl.com/procurement/terms/privacy-and-security-terms.

In case of conflict between the provisions of these Terms, the Supplier Relationship Agreement, an equivalent agreement, or Transaction Document, including any data processing agreement, these Terms will prevail. If the conflict is between these Terms and provisions mutually agreed between Supplier and Kyndryl for a Kyndryl Customer, the provisions mutually agreed for a Kyndryl Customer will prevail.

Capitalized words have the meanings given in Article V to these Terms, otherwise within these Terms, or in the Transaction Document or associated base agreement between the parties.

Article I. DATA GOVERNANCE AND AI

1.1. **Compliance with Laws**. Supplier will comply with all laws applicable to the Services and Deliverables, including laws relating to data protection, cybersecurity and AI Systems. Supplier will promptly notify Kyndryl (and in any event within time frames required by law and affording Kyndryl the opportunity to meet its own legal obligations), if Supplier determines it can no longer fulfill its legal obligations.

1.2. **Data Use.** Supplier will not:

(a) use Kyndryl Data in any form, including aggregated, anonymized or otherwise, for any purpose other than providing the Services and Deliverables (by way of example, Supplier is not permitted to use or reuse Kyndryl Data to evaluate the effectiveness or means of improving Supplier's offerings other than the Services or Deliverables, for research and development to create new offerings, or to generate reports regarding Supplier's offerings)

(b) Sell or Share Kyndryl Data; or

(c) attempt to re-identify any information that can reasonably be used to infer information about, or otherwise be linked to, a Data Subject.

1.3. **Web Tracking Technologies**. If Supplier or its Subcontractors, in the delivery of the Services or the Deliverables, collect any data using web tracking technologies (including HTML5, local storage, third party tags or tokens, and web beacons), such data is considered to be Kyndryl Data and Supplier will comply with its obligations regarding Kyndryl Data under these Terms.

1.4. **Non-disclosure**. Supplier will not disclose Kyndryl Data to any third party, other than to Subprocessors approved in accordance with Section 3.5 or Subcontractors approved in accordance with the Agreement.

1.5. **Government Access**. If a government, including any regulator, demands access to Kyndryl Data (e.g., if the U.S. government serves a national security order on Supplier to obtain Kyndryl Data), or if a disclosure of Kyndryl Data is otherwise required by law, Supplier will promptly notify Kyndryl in writing of such demand or requirement and afford Kyndryl a reasonable opportunity to challenge any disclosure, unless prohibited by law. If notification is prohibited by law, Supplier will take the steps that it reasonably believes are appropriate to challenge the prohibition and disclosure of Kyndryl Data through judicial action or other means.

1.6. **Confidentiality**. Supplier assures Kyndryl that: (a) only those of its employees who need access to Kyndryl Data to provide Services or Deliverables will have that access, and only to the extent necessary; and (b) it has bound its employees to confidentiality obligations that require those employees to only use and disclose Kyndryl Data as these Terms permit.

1.7. **Return or Deletion of Kyndryl Data**. Supplier will, at Kyndryl's choice, either delete or return Kyndryl Data to Kyndryl at its own cost upon termination or expiration of the Transaction Document, or earlier upon request from Kyndryl. If Kyndryl requires deletion, then Supplier will, consistent with NIST SP 800-88 rev.1, render the data unreadable and unable to be reassembled or reconstructed, and will certify the deletion to Kyndryl upon request. If Kyndryl requires the return of Kyndryl Data, then Supplier will do so in a commonly used format on Kyndryl's reasonable schedule and instructions.

1.8. **AI Systems**

(a) Supplier shall not use AI Systems in the delivery of the Services or a Deliverable or include AI Systems in a Deliverable, without Kyndryl's prior authorization in a Transaction Document or the Agreement. In seeking Kyndryl's authorization, Supplier will provide Kyndryl in writing with all necessary information to assess Supplier's use of AI Systems (e.g., data flows, language models used, data separation).

(b) Supplier represents and warrants that: (i) the input provided by Kyndryl (including input provided by the employees or any other third party under a Transaction Document) and output will be classified as Kyndryl Materials, (ii) Supplier will not use Kyndryl Materials to train or fine-tune the foundation model or other elements of the AI Systems, (iii) Supplier will not store Kyndryl Materials longer than necessary to provide the Services, (iv) the AI Systems (including the outputs and the training data) will be classified as part of the Services, and (v) to the extent permitted by applicable law, Supplier hereby assigns all of its right, title and interest in and to the outputs of the AI Systems to Kyndryl.

(c) Supplier shall implement and maintain a documented governance and risk management program for the AI Systems that identifies, tests for, monitors, and reasonably and appropriately mitigates known and foreseeable risks, including, without limitation, risks relating to ethics, bias, security, and safety associated with, or arising from, the AI Systems. On request, Supplier will share a copy of its governance and risk management program for AI Systems. Supplier will promptly notify Kyndryl in writing of any risks that occurred or any material risk that has been identified in accordance with notification provision agreed in the Transaction Document with a copy to ailegalteam@kyndryl.com.

Article II. PRIVACY

2.1. **Business Contact Information**. Kyndryl and Supplier may Process each other's BCI in accordance with applicable data protection laws as independent Controllers wherever they do business to deliver and receive the Deliverables and the Services. The parties are not acting as joint Controllers regarding each other's BCI. If either party informs the other of any requests from a Data Subject in respect of the other's BCI, the other party will be responsible for addressing such requests directly with the Data Subject. Each of the parties has implemented appropriate technical and organizational measures to protect the other's BCI. For clarity, Section 3.12 (Security Incidents) applies to BCI.

2.2. **Supplier as Processor**. Kyndryl appoints Supplier as a Processor of Kyndryl Personal Data for the sole purpose of providing the Deliverables and Services in accordance with Kyndryl's instructions, including those contained in these Terms, the Agreement and any related Transaction Document. Supplier is a Processor of Kyndryl Personal Data. If Supplier does not act in accordance with Kyndryl's instruction in order for Kyndryl to comply with applicable data protection law, Kyndryl may terminate the affected part of the Services on written notice. If Supplier believes an instruction violates a data protection law, Supplier will inform Kyndryl promptly and within any time frame required by law.

2.3. **Technical and Organizational Measures**. Supplier will implement and maintain appropriate technical and organizational measures, including the security measures in Article III below, to ensure a level of security appropriate to the risk associated with delivery of the Services and Deliverables.

2.4. **Data Subject Rights and Requests**

(a) Supplier will inform Kyndryl promptly (on a schedule that allows Kyndryl and any Other Controllers to fulfill their legal obligations) of any request from a Data Subject to exercise any Data Subject rights (e.g., rectification, deletion or blocking of data) regarding Kyndryl Personal Data. Supplier may also promptly direct a Data Subject making such a request to Kyndryl. Supplier will not answer any requests from Data Subjects unless it is legally required or instructed by Kyndryl in writing to do so.

(b) If Kyndryl is obliged to provide information regarding Kyndryl Personal Data to Other Controllers or other third parties (e.g., Data Subjects or regulators), Supplier will assist Kyndryl by providing information and taking other reasonable actions that Kyndryl requests, on a schedule that allows Kyndryl to timely respond to such Other Controllers or third parties.

2.5. **Subprocessors**

(a) Kyndryl authorizes Supplier to engage the Subprocessors listed in the respective Processing Details Exhibits. Kyndryl further authorizes Supplier to engage additional or replacement Subprocessors or expand the scope of Processing by an existing Subprocessor subject to the following conditions:

(i) Supplier will provide Kyndryl with advance written notice before adding a new Subprocessor or replacing an existing Subprocessor or expanding the scope of Processing by an existing Subprocessor.

(ii) Kyndryl may object to any such new or replacement Subprocessor or expanded scope on reasonable grounds at any time, and if it does so, the parties will work together in good faith to address Kyndryl's objection.

(iii) Supplier may engage the new or replacing Subprocessor or expand the scope of Processing of the existing Subprocessor if Kyndryl has not raised an objection within 30 days of receipt of Supplier's written notice.

(b) Supplier will impose the data protection, security and certification obligations set out in these Terms on each approved Subprocessor prior to a Subprocessor Processing any Kyndryl Personal Data. Supplier is fully liable to Kyndryl for performance of each Subprocessor's obligations.

2.6. **Transborder Data Processing**

(a) Supplier will not transfer or disclose (including by remote access) any Kyndryl Personal Data across borders except to approved Subprocessors in accordance with Section 3.5. If Kyndryl approves transborder transfer of Kyndryl Personal Data, the parties will cooperate to comply with applicable data protection laws. If SCCs are required by those laws, Supplier will promptly enter into SCCs as defined below.

(b) **European Economic Area**

(i) If Kyndryl transfers Personal Data subject to the General Data Protection Regulation (2016/679) outside of the European Economic Area to Supplier not established in an Adequate Country, Supplier hereby enters into the EU Standard Contractual Clauses (Commission Decision 2021/914), pre-signed by Kyndryl and located at https://www.kyndryl.com/procurement/terms/privacy-and-security-terms ("**EU SCCs**").

(ii) In the event Kyndryl has factually disappeared, ceased to exist in law, or has become insolvent, the Other Controllers shall have the right to terminate the Agreement and to instruct Supplier to erase or return the Kyndryl Personal Data.

(iii) Kyndryl's assessment on Personal Data transfers to Suppliers as required by the EU SCCs is published for Supplier's review at https://www.kyndryl.com/ procurement/terms/privacy-and-security-terms.

(iv) Supplier will provide sufficient details of each Subprocessor in the Processing Details Exhibits and notices to satisfy its obligations as a data importer under clause 14(c) of the EU Standard Contractual Clauses, including the Subprocessor's name, processing locations, and processing activities.

(v) Supplier will act as the Data Exporter and enter into EU SCCs or other appropriate transfer mechanism with each approved Subprocessor not established in an Adequate Country.

(c) **United Kingdom.** If Kyndryl Personal Data subject to the UK Data Protection Act (2018) are transferred outside of the United Kingdom to a Non-Adequate Country, Supplier hereby enters into the UK International Data Transfer Addendum, pre-signed by Kyndryl and located at [https://www.kyndryl.com/procurement/terms/privacy-and-security-terms].

(d) **Switzerland**. If Kyndryl Personal Data subject to the Swiss Federal Act on Data Protection ("**FADP**") are transferred outside of Switzerland to a Non-Adequate Country, Supplier hereby enters into the EU SCCs, subject to the following amendments:

(i) references to the GDPR shall also include the reference to the equivalent provisions of the FADP;

(ii) the Swiss Federal Data Protection Information Commission is the exclusive supervisory authority in accordance with Clause 13 and Annex I.C of EU SCCs;
(iii) the governing law in accordance with Clause 17 of the EU SCCs shall be Swiss law in case the data transfer is exclusively subject to FADP; and
(iv) the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCCs.

(e) **Other Countries**. If a transfer of Kyndryl Personal Data is subject to the data protection laws of a country where either the local SCCs have not been published by the Supervisory Authority (e.g., Brazil Data Protection Law, Peru Data Protection Act, South African Data Protection Act) or the Supervisory Authority has approved the use of EU standard contractual clauses as a sufficient safeguard for transborder transfer (e.g., Argentina Data Protection Law), the EU SCCs shall govern such transfer subject to the following amendments:
(i) references to the GDPR shall also include the reference to the equivalent provisions of the local data protection law;
(ii) the local Supervisory Authority is the exclusive supervisory authority in accordance with Clause 13 and Annex I.C of EU SCCs;
(iii) the governing law in accordance with Clause 17 of the EU SCCs shall be the local data protection law; and
(iv) the term "member state" must not be interpreted in such a way as to exclude data subjects in the country from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18 of the EU SCCs.

2.7. **Assistance and Records**

(a) Taking into account the nature of Processing, Supplier will assist Kyndryl by having appropriate Technical and Organizational Measures ("**TOMs**") to fulfil obligations associated with Data Subject requests and rights. Supplier will also assist Kyndryl in ensuring compliance with obligations relating to the security of Processing, the notification and communication of any Security Incident, and the creation of data protection impact assessments, including prior consultation with the responsible regulator, if required, taking into account the information available to Supplier.

(b) Supplier will maintain an up-to-date record of the name and contact details of each Subprocessor, including each Subprocessor's representative and data protection officer. Upon request, Supplier will provide this record to Kyndryl on a schedule that allows Kyndryl to timely respond to any demand from a Customer or other third-party.

2.8. **Country-Required Terms**

(a) **Japan**
i) For BCI of Data Subjects located in Japan, Supplier will comply with the provisions of these Terms, applicable to Supplier as a Processor.
ii) The definition of "Security Incident" in these Terms are hereby amended to include reasonably suspected breaches of Kyndryl Personal Data related to Data Subjects located in Japan.
iii) Supplier warrants that it has no reason to believe that the laws and practices of any country where Supplier or its Subprocessors will process Kyndryl Personal Data prevent Supplier from fulfilling its obligations under these Terms. Supplier will notify Kyndryl if, after having agreed to the Terms and for the duration of the Terms, Supplier has reason to believe that it cannot comply with its obligation under the Terms. In which case, the parties will cooperate in good faith to identify appropriate measures to be adopted to address the situation. If no appropriate measures can be implemented, Kyndryl will evaluate whether to suspend the transfer of Kyndryl Personal Data.

(b) **California**. Where Supplier, as a Processor, Processes Kyndryl Personal Data of Data Subjects located in the State of California, (i) Kyndryl discloses the Kyndryl Personal Data to Supplier only for the limited and specified business purposes selected in the applicable Processing Details Exhibit, (ii) Kyndryl may, upon notice, take reasonable and appropriate measures to stop unauthorized Processing or to ensure that Supplier's Processing is consistent with Kyndryl's obligations under applicable data protection laws, and (iii) Supplier will not retain, use, or disclose Kyndryl Personal Data outside of the direct business relationship between Kyndryl and Supplier.

Article III. GENERAL SECURITY

3.1. Security Policies

(a) **Policies.** Supplier's information security policies will be documented, approved by Supplier's senior management, and consistent with Industry Standard Practices. Supplier's information security policies will be reviewed and assessed by Supplier at least annually, and promptly after any material changes are made to the policies, to confirm their continuing applicability and effectiveness. Supplier will not make changes to the policies that would degrade Supplier's security relative to the Kyndryl Materials, the Deliverables or the Services.

(b) **Testing.** Supplier will maintain a process for regularly testing the effectiveness of its technical and organizational measures to ensure the security of the Kyndryl Materials, the Deliverables and the Services.

(c) **Risk Management**. Supplier will perform appropriate information security risk assessments as part of an ongoing risk governance program with the following objectives: (i) identify information security risk relating to the Kyndryl Materials, the Deliverables and the Services; (ii) assess the impact of any such risk; and (iii) where risk reduction or mitigation strategies are identified or warranted, implement measures to mitigate and effectively manage such risk recognizing that the threat landscape constantly changes.

3.2. Personnel Security

(a) **Security Training**. Supplier will provide appropriate security and privacy awareness, education, and training at least annually to all Supplier Personnel having access to, or the ability to access, Kyndryl Materials, Deliverables or Services.

(b) **Background Screening**. Supplier will maintain and follow standard, mandatory employment verification requirements for all new employee hires, and extend such requirements to all Supplier Personnel and Personnel of Supplier-controlled subsidiaries. Those requirements will include criminal background checks to the extent permitted by local laws, proof of identity validation, and additional checks that Supplier deems necessary. Supplier will periodically repeat and revalidate these requirements, as it deems necessary.

3.3. Asset Management

(a) **Asset Inventory**. Supplier will maintain an asset inventory of all equipment on which Kyndryl Materials are stored. Supplier will restrict access to such equipment only to authorized Supplier Personnel. Supplier will prevent unauthorized access to and copying, modification or removal of Kyndryl Materials. Supplier will maintain measures to prevent the unauthorized access, copying, modification or deletion of Kyndryl Materials.

(b) **Security of Software Components**. Supplier agrees to appropriately inventory all software components (including open-source software) used in the provision of the Services and the development and provision of the Deliverables. Supplier will assess whether any such software components have security defects and/or vulnerabilities that could lead to the unauthorized disclosure of or access to Kyndryl Materials, the Deliverables or Services. Supplier will perform such assessment prior to delivery of, or providing Kyndryl access to, the Services and Deliverables and on an on-going basis thereafter during the term of the Transaction Document. Supplier agrees to timely remediate any security defect or vulnerability in any such software component of which Supplier becomes aware. Supplier will promptly respond to any inquiries by Kyndryl relating to whether any security defect or vulnerability in any such software component is known by Supplier and/or has been remediated by Supplier.

3.4. Access Control Policy

. Supplier will maintain an appropriate role-based access control policy and appropriate access control technical measures consistent with Industry Standard Practices to restrict access to Kyndryl Materials and Supplier assets used to provide the Services only to authorized Supplier Personnel and limit such access to the least level required to provide and support the Services and Deliverables.

3.5. Authorization

(a) Supplier will maintain user account creation and deletion procedures for granting and promptly (and in any event within twenty-four (24) hours) revoking access to all Kyndryl Materials and all Supplier internal applications and assets used in the provision of the Services and Deliverables. Supplier will assign an appropriate authority to approve creation and revocation of user accounts or elevated or reduced levels of access for existing accounts including for termination of a Personnel's employment, contract, engagement or other agreement with Supplier or a change in role if such Personnel no longer require such access rights.

(b) Supplier will maintain and update records of Supplier Personnel who are authorized to access systems and assets on which are stored, or from which may be accessed Kyndryl Materials and the Deliverables or that are used to provide the Services and review such records at least quarterly. Administrative and technical support Personnel will only be permitted to have access to such systems, Kyndryl Materials and Deliverables only when required and provided that such Personnel comply with applicable Supplier technical and organizational measures.
(c) Supplier will ensure that user accounts having access to such systems and assets are unique and restricted by passwords and that user accounts are not shared.

3.6. Authentication

(a) Supplier will monitor for repeated access attempts to information systems and assets.
(b) Supplier will maintain password protection practices that are consistent with Industry Standard Practices and designed to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form. Supplier will generate or require the user to create and use a strong randomly generated complex password or passphrase or suitable alternatives, such as digital certificates, cards/hardware tokens or biometrics.
(c) Supplier will use multi-factor authentication, including for domain and cloud portal administrative access. Multi-factor authentication may include techniques such as the use of cryptographic certificates, one-time-password (OTP) tokens, or biometrics.

3.7. Cryptography

(a) **Policy**. Supplier will implement and maintain cryptographic policies and standards consistent with Industry Standard Practices to protect Kyndryl Materials, including, where appropriate, pseudonymization and encryption.
(b) **Encryption**. Supplier shall encrypt Kyndryl Materials in transit and at rest. Encryption algorithms will protect data to security levels consistent with Industry Standard Practices (such as NIST SP 800-131a) and will utilize industry recognized hashing functions, which will be at least as protective as 256-bit Advanced Encryption Standard encryption (AES 256) at rest and TLS v1.2 in transit. Supplier will maintain and follow key management policies and practices consistent with Industry Standard Practices that define encryption key requirements, security, rotation, and lifecycle, including creation, distribution, revocation, archival, and destruction.

3.8. Physical and Environmental Security

(a) **Access to Facilities**. Supplier will limit access of Facilities to its authorized Personnel.
(b) **Protection from Disruptions**. Supplier will use reasonable efforts to protect such systems and assets from power failures and other disruptions caused by failures in supporting utilities.
(c) **Secure Disposal or Reuse of Equipment**. Supplier will ensure that all Kyndryl Materials have been securely deleted or overwritten from equipment containing storage media using processes consistent with Industry Standard Practices prior to disposal or re-use of such equipment.

3.9. Operations Security

(a) **Operations Policy**. Supplier will maintain appropriate operational and security operating procedures and such procedures will be made available to all Personnel who require them.
(b) **Protections from Malware**. Supplier will deploy antivirus and end point management solutions to maintain anti-malware controls to protect such systems and assets from malicious software, including malicious software that originates from public networks.
(c) **Configuration Management**. Supplier will have policies that govern the installation of software and utilities by Personnel.
(d) **Change Management**. Supplier will maintain and implement procedures to ensure that only approved and secure versions of the code, configurations, systems, and applications will be deployed in production environments.
(e) **Logical Separation**. Supplier will maintain appropriate isolation of its production, non-production, and other environments, and, if Kyndryl Materials are already present within or are transferred to a non-production environment (e.g., to reproduce an error), then Supplier will ensure that the security and privacy protections in the non-production environment are equal to those in the production environment.

3.10. Communications Security

(a) **Information Transfer**. Supplier will restrict access through encryption to Kyndryl Materials stored on media that is physically transported outside of Facilities. Supplier will ensure that it is possible to verify and establish the extent to which Kyndryl Materials have been or may be transmitted or made available using data communication equipment.

(b) **Security of Network Services**. Supplier will ensure that security controls and procedures are implemented for all network services and components consistent with Industry Standard Practices, irrespective of whether such services are provided in-house or outsourced.

(c) **Intrusion Detection**. Supplier will deploy intrusion detection or intrusion prevention systems and measures for the prevention and denial of service attacks for all systems used to provide the Services and Deliverables including continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

(d) **Firewalls**. Supplier will implement firewalls that only allow documented and approved ports and services to be used. All other ports will be in a "deny all" mode.

(e) **Monitoring**. Supplier will monitor use of privileged access and maintain security information and event management measures to: (i) identify unauthorized access and activity, (ii) facilitate a timely and appropriate response to such access and activity, and (iii) enable audits by Supplier and Kyndryl.

(f) **Logging**. Supplier shall employ procedures to ensure that all systems, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized logging system in order to enable the security audits referred to below. Supplier shall: (i) retain logs for at least 180 days, (ii) ensure that no logs contain confidential information, (iii) protect logs from unauthorized modification or erasure, (iv) backup up logs daily, and (v) monitor logs for risk and functional anomalies. Supplier will provide such logs to Kyndryl upon request.

3.11. System Acquisition, Development and Maintenance

(a) **Application Hardening**

i) Supplier will maintain and implement secure application development policies, procedures and standards consistent with Industry Standard Practices such as the SANS Top 25 Security Development Techniques or the OWASP Top Ten project.

ii) All Supplier Personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Services and Deliverables and receive appropriate training regarding Supplier's secure application development practices.

(b) **System Hardening**

i) Supplier will establish and ensure the use of standard secure configurations of operating systems. Images should represent hardened versions of the underlying operating system, and the applications installed on the system. Hardening includes removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, applying patches, closing open and unused network ports, and implementing intrusion detection systems and/or intrusion prevention systems. These images should be validated on a regular basis to update their security configuration as appropriate. Supplier will implement patching tools and processes for both applications and operating system software. When outdated systems can no longer be patched, Supplier will update to the latest version of application software. Supplier will remove outdated, unsupported, and unused software from the system.

ii) Supplier will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

(c) **Infrastructure Vulnerability Scanning**. Supplier will scan its internal environments (e.g., servers, network devices, etc.) related to the Services and Deliverables monthly and external environments related to the Services and Deliverables on a weekly basis. Supplier will have a defined and documented process with specific timeframes to address any findings commensurate to the risk posed and the severity level.

(d) **Application Vulnerability Assessment**. Supplier will perform an application security vulnerability assessment prior to any new public release. Supplier will have a defined and documented process to address any findings commensurate to the risk posed.

(e) **Penetration Tests and Security Evaluations**. Supplier will perform a comprehensive penetration test and security evaluation of all systems involved in providing Services and Deliverables on a recurring basis no less than once annually. Additionally, Supplier will have an industry-recognized independent third party perform an annual test. Supplier will have a defined and documented process to address any findings

commensurate to the risk posed. Upon Kyndryl's written request, but no more than once per year, Supplier will provide an attestation confirming that an independent third-party penetration test has been completed and Supplier has implemented a process to address findings according to a risk assessment. Supplier will provide a summary of the findings, including the number of systems or applications tested, testing dates, testing methodology, and the number of critical, high, medium, and low findings.

(f) **Disaster Recovery**. During the term of the Agreement, Supplier will maintain a disaster recovery ("**DR**") or high availability ("**HA**") solution and related plan for the Services and Deliverables that are consistent with Industry Standard Practices. Supplier will test the DR or HA solution and related plan at least once annually. In addition, the solution and related plan will ensure:
   i) that installed systems used to provide the Services and Deliverables will be restored in case of interruption,
   ii) Supplier's ability to restore the availability and access to Kyndryl Materials in a timely manner in the event of a physical or technical incident, and
   iii) the ongoing confidentiality, integrity, availability, and resilience of systems Supplier uses to provide the Services and Deliverables.

3.12. Security Incidents

(a) Supplier will maintain and follow an information security incident response program consistent with Industry Standard Practices, including documented procedures for investigating and addressing information security incidents. The information security incident response program will address topics such as prioritization of incidents, roles and responsibilities, internal escalation procedures, tracking and reporting, and containment and remediation. The information security incident management program will be tested, reviewed, and approved on a periodic basis, but at least annually.

(b) Supplier will promptly (and in no event any later than 48 hours) notify Kyndryl after becoming aware of a Security Incident by sending an email to cyber.incidents@kyndryl.com. With respect to a Security Incident, Supplier will promptly:
   i) provide Kyndryl with reasonably requested information about such incident, Supplier's investigation of the incident, and the status of any Supplier remediation and restoration activities. By way of example, reasonably requested information may include factual findings relating to the nature, cause, and impact of the incident, logs demonstrating privileged, administrative, and other access to Devices, systems, services, or applications, summaries based on forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the incident or Supplier's mitigation, remediation and restoration activities;
   ii) ensure that appropriate Supplier Personnel with knowledge of the incident attend conference calls requested by Kyndryl;
   iii) engage third party incident response, data breach incident management, forensics and electronic discovery subject matter experts, at Kyndryl's reasonable request;
   iv) provide Kyndryl with reasonable assistance to satisfy any legal obligations (including obligations to notify regulators, Data Subjects, Customer or other third parties) of Kyndryl, Kyndryl affiliates and Customers (and their customers and affiliates); and
   v) timely and appropriately mitigate and remediate the effects of the Security Incident and implement additional controls and processes to lessen the risk of similar incidents in the future, while affording due consideration to any Kyndryl input on such mitigations and remediation.

(c) Supplier is responsible for all costs and expenses incurred by Supplier in investigating, responding to, mitigating, and remediating a Security Incident. Subject to the limitation of liability in the Agreement, Supplier is also responsible for any out-of-pocket costs and expenses incurred by Kyndryl, Kyndryl affiliates, and Customers (and their customers and affiliates) in connection with the investigation, response, mitigation, and remediation of the Security Incident. Security Incident remediation costs and expenses may include costs related to detecting and investigating a Security Incident, determining responsibilities under laws and regulations, reloading data, correcting product defects (including through Source Code or other development), retaining third parties to assist with the foregoing or other relevant activities, and other costs and expenses that are necessary to remediate the harmful effects of the Security Incident.

(d) In case of a Security Incident involving Kyndryl Personal Data, Supplier is responsible for any costs it incurs and will reimburse Kyndryl for any costs and expenses Kyndryl incurs related to:

i) Providing notification of the Security Incident to applicable regulators, other government and relevant industry self-regulatory agencies, the media (if required by applicable law), Data Subjects, Customers, and others;
ii) Establishing and maintaining a call-center to respond to questions from Data Subjects about the Security Incident and its consequences, for 1 year after the date on which such Data Subjects were notified of the Security Incident or longer, if required by applicable data protection law. Kyndryl and Supplier will work together to create the scripts and other materials to be used by call-center staff when responding to inquiries concerning Kyndryl Personal Data; and
iii) Providing identity theft protection, credit monitoring and credit restoration services for 2 years after the date on which Data Subjects affected by the incident who choose to register for such services were notified of the Security Incident or longer, if required by applicable law.

(e) Supplier will not, directly or indirectly, identify Kyndryl to any third party as having been affected by a Security Incident, unless Kyndryl approves doing so in writing or where required by law. Supplier will notify Kyndryl in writing prior to distributing any legally required notification to a third-party that directly or indirectly reveals Kyndryl's identity.
(f) Supplier will also promptly notify Kyndryl of any actual or imminent threat of violation of these Terms or its security policies, security procedures, or acceptable use policies related to delivery of a Deliverable or the Services.

3.13. Supplier Relationships

(a) **Subcontractors**. Supplier is responsible for compliance with these Terms even if Supplier uses a Subcontractor. Supplier will contractually commit those Subcontractors to protect Kyndryl Materials through terms no less complete or stringent than those that apply to Supplier in the Terms. Supplier is liable to Kyndryl for the performance of each Subcontractor's performance.
(b) **Quality Control and Security Management**. Supplier will perform quality control and security management oversight of software development outsourced to a Subcontractor.
(c) **Pre-contractual information**. Supplier represents and warrants that all material information provided during pre-contractual discussions with Kyndryl related to privacy, security and data governance, whether pursuant to these Terms or otherwise, is accurate in all material respects and is not, whether by omission or otherwise, misleading.

3.14. Verification, Cooperation, Security Compliance and Assessment

(a) **Verification.** Supplier will maintain an auditable record demonstrating compliance with these Terms.
(i) Kyndryl, by itself or with an external auditor, may, upon 30 Days prior written notice to Supplier, verify Supplier's compliance with these Terms, including by accessing any Facility or Facilities for such purposes, though Kyndryl will not access any data center where Supplier Processes Kyndryl Data unless it has a good faith reason to believe that doing so would provide relevant information. Supplier will cooperate with Kyndryl's verification, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like. Supplier may offer proof of adherence to an approved code of conduct or industry certification or otherwise provide information to demonstrate compliance with these Terms, for Kyndryl's consideration.
(ii) A verification will not occur more than once in any 12-month period, unless: (A) Kyndryl is validating Supplier's remediation of concerns resulting from a previous verification during the 12-month period or (B) a Security Incident has arisen and Kyndryl wishes to verify compliance with obligations relevant to the incident. In either case, Kyndryl will provide the same 30 Days prior written notice as specified in paragraph (i) above, but the urgency of addressing a Security Incident may necessitate Kyndryl conducting a verification on less than 30 Days' prior written notice.
(iii) A regulator or, where legally entitled, other Controller may exercise the same rights as Kyndryl in paragraphs (ii) and (iii), with the understanding that a regulator may exercise any additional rights it has under the law.
(iv) If Kyndryl has a reasonable basis for concluding that Supplier is not compliant with any of these Terms (whether such basis arises from a verification under these Terms or otherwise), then Supplier will promptly remediate such non-compliance.

(v) This Section shall apply in addition to clause "Record Keeping and Audit Right" or other similar Audit clause in the Agreement.

(b) **Cooperation**. If Kyndryl has reason to question whether any Services or Deliverables may have contributed, are contributing, or will contribute to any cyber security concern, then Supplier will reasonably cooperate with any Kyndryl inquiry regarding such concern, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like.

(c) **Security Compliance**. Supplier will obtain (i) a certification of compliance with ISO 27001, from an independent public auditing firm, (ii) a report by an independent public auditing firm demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 2 Type 2, which at a minimum will include the Trust Service Principles of Security (also known as the Common Criteria), Availability and Confidentiality, and (iii) a report by an independent public auditing firm demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 1 Type 2, if the Services impact Kyndryl's financial reports. Supplier will comply with future guidance relating to SSAE18 as issued by the AICPA, IAASB, the Securities and Exchange Commission or the Public Company Accounting. Upon request, Supplier will promptly provide Kyndryl with a copy of each certificate and report Supplier is obliged to obtain.

(d) **Kyndryl Compliance Assessment**. Upon Kyndryl's reasonable request, but no more than once in any 12-month period for each individual Service or Deliverable, Supplier will accurately and timely (not to exceed 14 Days) complete a questionnaire to verify Supplier's compliance with its cybersecurity and data governance obligations under the Agreement and these Terms ("**Compliance Assessment**"). If, after completion of the Compliance Assessment, Kyndryl reasonably determines that Supplier's security and data governance practices and procedures do not meet Supplier's obligations, then Kyndryl will notify Supplier of the deficiencies. If Supplier agrees with Kyndryl's assessment of the deficiencies, Supplier will, without unreasonable delay: (i) correct such deficiencies at its own expense within a timeframe agreed with Kyndryl based on an assessment of the risk; and (ii) provide Kyndryl, or its duly authorized representatives, with reasonable documentation and information confirming the remediation of the deficiencies. If Supplier fails to remediate any high or critical rated deficiencies within the agreed timeframe, Kyndryl has the right to terminate the applicable Transaction Document or the Agreement for material breach immediately upon notice to Supplier. Kyndryl will not disclose the documentation to any third party other than its own auditors without Supplier's written consent. If Supplier disagrees with Kyndryl's assessment of the deficiencies, Supplier will promptly provide Kyndryl with a written explanation detailing its reasons, and if Kyndryl does not accept Supplier's reasons, the parties will escalate to their respective Chief Privacy Officer, Chief Information Security Officer, or an executive having similar scope and authority for timely resolution. If any deficiencies are caused by Kyndryl's use of the Services, Supplier will provide reasonable technical support to assist Kyndryl in appropriate use of the Services to remediate such deficiencies.

Article IV. ACCESS TO KYNDRYL NETWORKS

This Article applies if Supplier employees will have access to any Corporate System.

4.1. General Terms

(a) Kyndryl will determine whether to authorize Supplier employees to access Corporate Systems. If Kyndryl so authorizes, then Supplier will comply, and will ensure its employees with such access to comply, with the requirements of this Article.
(b) Kyndryl will identify the means by which Supplier employees may access Corporate Systems, including whether such employees will access Corporate Systems through Kyndryl or Supplier provided Devices.
(c) Supplier employees may only access Corporate Systems and may only use the Devices that Kyndryl authorizes for that access, to provide Services, which will either be a Kyndryl provided Device ("Kyndryl Device") or a Supplier provided Device ("Supplier Device").
(d) Supplier employees will not copy Kyndryl Materials that are accessible through a Corporate System without Kyndryl's prior written approval (and will never copy any Kyndryl Materials to a portable storage device, such as a USB, an external hard drive, or other like items).
(e) Upon request, Supplier will confirm, by employee name, the specific Corporate Systems which its employees are authorized to access, and have accessed, over any time period that Kyndryl identifies.
(f) Supplier will notify Kyndryl within twenty-four (24) hours after any Supplier employee with access to any Corporate System is no longer: (i) employed by Supplier or (ii) working on activities that require such access. Supplier will work with Kyndryl to ensure that access for such former or current employees is immediately revoked.
(g) Supplier will immediately report any actual or suspected security incidents (such as loss of a Kyndryl Device or Supplier Device or unauthorized access to a Kyndryl Device or Supplier Device or data, materials or other information of any kind) to Kyndryl and cooperate with Kyndryl in the investigation of such incidents.
(h) Supplier may not permit any agent, independent contractor or subcontractor employee to access any Corporate System, without Kyndryl's prior written consent; if Kyndryl provides that consent, then Supplier will contractually commit those persons and their employers to comply with the requirements of this Article as if those persons were Supplier employees, and will be responsible to Kyndryl for all actions and omissions to act by any such person or employer with respect to such Corporate System access.
(i) Kyndryl may revoke access to Corporate Systems at any time, for any Supplier employee or all Supplier Personnel, without prior notice to Supplier or any Supplier employee or others, if Kyndryl believes that doing so is necessary to protect Kyndryl.
(j) Kyndryl's rights are not blocked, lessened, or restricted in any way by any provision of the Transaction Document, the associated base agreement between the parties, or any other agreement between the parties, including any provision that may require data, materials or other information of any kind to reside only in a select location or locations or that may require that only persons from a select location or locations access such data, materials or other information.

4.2. Device Software

(a) Supplier will direct its Personnel to timely install software on Kyndryl Devices and Supplier Devices that Kyndryl requires to facilitate access to Corporate Systems in a secure manner. Neither Supplier nor its Personnel will interfere with the operations of that software or the security features that the software enables.
(b) Supplier and its Personnel will adhere to the configuration rules for the Kyndryl Devices and Supplier Devices that Kyndryl sets and otherwise work with Kyndryl to help ensure that the software functions as Kyndryl intends. For example, Supplier will not override software website blocking or automated patching features.
(c) Supplier Personnel may not share usernames, passwords, or the like, for the Kyndryl Devices and Supplier Devices with any other person.
(d) If Kyndryl authorizes Supplier Personnel to access Corporate Systems using Supplier Devices, then Supplier will install and run an operating system on those Supplier Devices that Kyndryl approves and will upgrade to a new version of that operating system or a new operating system within a reasonable time after Kyndryl so instructs.

4.3. Kyndryl Devices

(a) Supplier employees may not use the Kyndryl Devices to provide services to any other person or entity, or to access any Supplier or third-party IT systems, networks, applications, websites, email tools, collaboration tools, or the like for or in connection with the Services. Supplier employees may not use the Kyndryl Devices for any personal reason (e.g., Supplier employees may not store personal files such as music, videos, pictures or other like items on such Kyndryl Devices and cannot use the Internet from such Kyndryl Devices for

personal reasons). Supplier employees may not share the Kyndryl Devices with other employees of Supplier they use to access Corporate Systems.

(b) Kyndryl has the unqualified rights to monitor Kyndryl Devices and the Corporate Systems and remediate potential intrusion and other cyber security threats in whatever ways, from whatever locations, and using whatever means Kyndryl believes is necessary or appropriate, without prior notice to Supplier or any Supplier employee or others. As examples of such rights, Kyndryl may, at any time, (i) perform a security test on any Kyndryl Device, (ii) monitor, recover through technical or other means and review communications (including emails from any email accounts on the Kyndryl Devices), records, files, and other items stored in any Kyndryl Device or transmitted through any Corporate System, and (iii) acquire a full forensic image of any Kyndryl Device. If Kyndryl needs Supplier's cooperation to exercise its rights, Supplier will fully and timely satisfy Kyndryl's requests for such cooperation (including, for example, requests to securely configure any Kyndryl Device, install monitoring or other software on any Kyndryl Device, share system level connection details, engage in incident response measures on any Device, and provide physical access to any Kyndryl Device for Kyndryl to obtain a full forensic image or otherwise, and similar and related requests).

(c) Kyndryl will retain title to all Kyndryl Devices, with Supplier bearing the risk of loss of Kyndryl Devices, including due to theft, vandalism, or negligence. Supplier will not make or permit any alterations to Kyndryl Devices without Kyndryl's prior written consent, with an alteration being any change to a Device, including any change to Device software, applications, security design, security configuration, or physical, mechanical, or electrical design.

(d) Supplier will return all Kyndryl Devices within 5 business days after the need for those Devices to provide Services ends, and if Kyndryl requests, destroy all data, materials and other information of any kind on those Devices at the same time, without retaining any copy, by following NIST standards to permanently erase all such data, materials and other information. Supplier will pack and return Kyndryl Devices in the same condition as delivered to Supplier, other than reasonable wear and tear, at its own expense to the location that Kyndryl identifies. Supplier's failure to comply with any obligation in this paragraph (d) constitutes a material breach of the Transaction Document and associated base agreement and any related agreement between the parties, with the understanding that an agreement is "related" if access to any Corporate System facilitates Supplier's tasks or other activities under that agreement.

(e) Kyndryl will provide support for Kyndryl Devices (including Device inspection and preventive and remedial maintenance). Supplier will promptly advise Kyndryl of the need for remedial service.

(f) For software programs that Kyndryl owns or has the right to license, Kyndryl grants Supplier a temporary right to use, store, and make sufficient copies to support its authorized use of Kyndryl Devices. Supplier may not transfer programs to anyone, make copies of software license information, or disassemble, decompile, reverse engineer, or otherwise translate any program unless expressly permitted by applicable law without the possibility of contractual waiver.

Article V. DEFINITIONS

The terms "Services" and "Deliverables" are likely defined in the Supplier Relationship Agreement or equivalent Agreement or a Transaction Document; but if they are not, then "**Services**" means any hosting, consulting, installation, customization, maintenance, support, staff augmentation, business, technical or other work that Supplier performs for Kyndryl, as specified in the Transaction Document, and "**Deliverables**" means any software programs, platforms, applications or other products or items and their respective related materials that Supplier provides to Kyndryl, as specified in the Transaction Document.

5.1. **Adequate Country** means a country providing an adequate level of data protection with respect to the relevant transfer pursuant to the applicable data protection laws or decisions of regulators.

5.2. **AI System** means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

5.3. **Business Contact Information** ("**BCI**") means Personal Data used to contact, identify or authenticate an individual in a professional or business capacity for administrative and contract management purposes (e.g., billing and account management, calculating partner incentives, internal reporting and business modeling such as forecasting, revenue and capacity planning). Typically, BCI includes an individual's name, business e-mail address, physical address, telephone number or similar attributes. For example, names and email addresses

used to contact Supplier Personnel for support services are BCI, however, names and email addresses included in diagnostic support data are Kyndryl Personal Data.

5.4. **Cloud Service** means any "as a service" offering that Supplier hosts or manages, including "software as a service", "platform as a service", and "infrastructure as a service" offerings.

5.5. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

5.6. **Corporate System** means an information technology system, platform, application, network, or the like that Kyndryl relies upon for its business, including those located on or accessible through Kyndryl's intranet, the Internet, or otherwise.

5.7. **Customer** means a Kyndryl customer.

5.8. **Data Importer** means either a Processor or a Subprocessor that is not established in an Adequate Country.

5.9. **Data Subject** means a natural person who can be identified, directly or indirectly.

5.10. **Day** or **Days** means calendar days, unless "business" days are designated.

5.11. **Device** means a Kyndryl-provided or Supplier-provided workstation, laptop, tablet, smartphone or personal digital assistant.

5.12. **Facilities** means a physical location where Supplier hosts, accesses or otherwise Processes Deliverables or Kyndryl Materials.

5.13. **Industry Standard Practices** means those practices recommended or required by the National Institute of Standards and Technology ("**NIST**") or International Organization for Standardization ("**ISO**"), or any other body or organization of similar reputation and sophistication.

5.14. **Kyndryl Data** means any and all data, files, materials, text, audio, video, images or other data, including Kyndryl Personal Data, Kyndryl BCI and Kyndryl non-Personal Data, that are provided to or accessible by Supplier (including, without limitation, via a Cloud Service) in connection with the delivery of the Services or a Deliverable, regardless of whether provided or made accessible by Kyndryl, Kyndryl Personnel, a Customer, Customer employee or contractor, or any other person or entity.

5.15. **Kyndryl Materials** means all Kyndryl Data and Kyndryl Technology.

5.16. **Kyndryl Personal Data** means the Personal Data, excluding Kyndryl BCI, that Kyndryl provides or makes accessible to Supplier for the delivery of the Services or Deliverables. Kyndryl Personal Data include Personal Data that Kyndryl controls and Personal Data that Kyndryl Processes on behalf of Other Controllers.

5.17. **Kyndryl Technology** means Source Code, other code, description languages, firmware, software, tools, designs, schematics, graphical representations, embedded keys, certificates and other information, materials, assets, documents and technology that Kyndryl has directly or indirectly licensed or otherwise made available to Supplier in connection with a Transaction Document or the Agreement.

5.18. **Non-Adequate Country** means a country that is not deemed adequate pursuant to applicable data protection laws or a decision of a competent regulator.

5.19. **Other Controller** means any entity other than Kyndryl that is a Controller of Kyndryl Data, such as a Kyndryl affiliate, Customer, or a Customer affiliate.

5.20. **On-Premise Software** means software provided by Supplier as a Deliverable that Kyndryl or a Kyndryl subcontractor runs, installs or operates on Kyndryl's or the subcontractor's servers or systems.

5.21. **Personal Data** means any information relating to a Data Subject and any other information that qualifies as "personal data" or the like under any data protection law.

5.22. **Personnel** means individuals who are employees of Kyndryl or Supplier, agents of Kyndryl or Supplier, independent contractors engaged by Kyndryl or Supplier, or provided to a party by a subcontractor.

5.23. **Process** or **Processing** means any operation or set of operations performed on Kyndryl Data, including storage, use, access and reading.

5.24. **Processor** means a natural or legal person that Processes Personal Data on a Controller's behalf and includes "service provider" or substantially similar terms under any data protection law.

5.25. **Security Incident** means (a) an occurrence that actually or imminently jeopardizes the confidentiality, integrity, or availability of any Kyndryl Materials or an information system used by Supplier or its Subcontractors to provide the Services or Deliverables, (b) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Kyndryl Data transmitted, stored or otherwise Processed, or (c) the unauthorized access to or use of Source Code that is used by Supplier or its Subcontractors in or related to the delivery of the Services or a Deliverable.

5.26. **Sell** (or **Selling**) means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, data for monetary or other valuable consideration.

5.27. **Share** has the meaning given in the California Consumer Privacy Act of 2018, as amended by the Consumer Privacy Rights Act of 2020.
5.28. **Standard Contractual Clauses** ("**SCCs**") means the contractual clauses required by applicable data protection laws for the transfer of Personal Data to Controllers or Processors that are not established in an Adequate Country.
5.29. **Source Code** means human readable programming code or code that is capable of being converted to human readable form that developers use in creating, developing, or maintaining a product, but that is not made public in the normal course of the product's commercial distribution or use.
5.30. **Subprocessor** means any Supplier Subcontractor, including a Supplier affiliate, that Processes Kyndryl Personal Data.
5.31. **Supervisory Authority** means an independent public body responsible for overseeing the application of data protection laws within a specific country or region.