



## DATA & NETWORK SECURITY SCHEDULE

This global Data & Network Security Schedule (“DNSS”) and its Addenda form part of the Agreement. Capitalized terms not specifically defined herein shall have the meaning set forth in the Agreement. This DNSS shall be considered a Schedule under the Agreement and shall be deemed a part of the Agreement by and between DXC Technology (“DXC”) and (“Supplier”).

### 1. PURPOSE OF THE DNSS & ORDER OF PRECEDENCE

- 1.1. Purpose of the DNSS. The purpose of the DNSS is to establish:
  - 1.1.1. Supplier’s obligations in relation to the use and Processing of Data;
  - 1.1.2. Minimum data security standards applicable to the Services or Products provided by Supplier; and
  - 1.1.3. Minimum security standards to be met by Supplier in relation to the Processing of Data and access to DXC Information Systems.
- 1.2. Order of Precedence. Nothing in this DNSS relieves Supplier of any obligations under the Agreement, nor shall be deemed a waiver by DXC of any rights or remedies therein. In the event any term or condition in this DNSS conflicts with a term or condition of any Agreement with Supplier, then the term or condition of this DNSS shall take precedence and control over any conflicting terms in the Agreement.

### 2. DEFINITIONS

- 2.1. **“Agreement”** means any terms and conditions under which Supplier will provide Services or Products to DXC, as requested from time to time, and as may further be described in Addendums that may be attached.
- 2.2. **“Applicable Laws”** means applicable local, state, and federal laws, executive orders, rules, regulations, ordinances, codes, orders, and decrees of all governments or agencies of domestic or foreign jurisdictions (including privacy laws) in which services are performed or to which services are performed pursuant to the Agreement.
- 2.3. **“Customer”** means an enterprise customer of DXC or its Affiliates.
- 2.4. **“Confidential Data”** means all non-public proprietary or confidential information of DXC or a third party (including a Customer) which is obtained by or made available to Supplier in connection with the Services, whether in oral, visual, written, electronic or other tangible or intangible form, whether or not marked or designated as “confidential” and including, without limitation, information relating to strategy, DXC financials, analytical reports, pricing, internal process or policies, provided, however, that Confidential Information does not include any information that: (a) is obtained by Supplier on a non-confidential basis from a third-party that was not legally or contractually restricted from disclosing such information; (b) was in Supplier’s possession prior to DXC’s disclosure hereunder; or (c) was or is independently developed by Supplier without using any Confidential Information.
- 2.5. **“Data”** means Confidential Data, DXC Personal Data and all other non-public data Processed by Supplier through the DXC Information Systems or provided to or accessed by Supplier in connection with the Services.
- 2.6. **“Sensitive Personal Data”** means any information (a) relating to a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or



sex life (or as otherwise defined by applicable Privacy Law); (b) which may facilitate identity theft; (c) which may permit access to an individual's financial account; (d) which requires notification under any data breach notification law if compromised; and (e) Social Security Number (SSN) or National ID number, driver's license number, credit or debit card information or other payment card information, bank account or other financial information, health care, insurance or payment information.

- 2.7. **"DXC Personal Data"** means any Personal Data, including Sensitive Personal Data of which DXC, its affiliates or Customers is the Controller which DXC or its Affiliates will provide to Supplier for Processing on its or their behalf.
- 2.8. **"Information Systems"** means any systems, including, but not limited to, net-services, networks, computers, personal computing device, mobile devices, removable media, communication system and other information systems used and all associated authentication methods.
- 2.9. **"Personal Data"** means any information relating to an identified or identifiable living individual (such as name, mailing address, phone number or email address) or as otherwise defined by applicable Privacy Law.
- 2.10. **"Process", "Processing", or "Processed"** means any operation or set of operations which is performed whether or not by automatic means (including, without limitation, accessing, collecting, recording, organizing, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Data) and any equivalent definitions in Applicable Laws to the extent that such definitions should exceed this definition.
- 2.11. **"Product" or "Products"** means any software, code, or logic bearing component (including, but not limited to, applications, mobile applications, websites, i-frames, pixel tags, operating system software, BIOS and firmware, middleware, software development kits, compiled binaries, source code, open source, processors, memory card, or storage capable components).
- 2.12. **"Security Breach"** means an actual or reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, exfiltration, alteration or unauthorized disclosure of, or access to Data, Information Systems, Product or Service.
- 2.13. **"Service" or "Services"** means the services to be provided by Supplier pursuant to this Agreement, as further described in a Statement of Work.
- 2.14. **"Supplier"** includes any third party who Processes Data or provides a Service or Product in the fulfilment of Supplier obligations under the Agreement.
- 2.15. **"Supplier's Facilities"** means the facilities in or from which Supplier or its agents, employees or subcontractors Processes Data.



### **3. DATA SECURITY**

- 3.1. Without superseding or limiting any security requirements pursuant to the Section 'Data Protection and Privacy' and any other Sections of this Agreement or any SOW that further addresses information security, Supplier shall implement organizational, operational, and technical security measures to protect the integrity, availability, and confidentiality of all data Processed by Supplier or provided by DXC to Supplier of any type, including but not limited to Sensitive Information, Confidential information, Personal Data, and PHI (collectively, "DXC Data"). Such security measures shall meet all applicable legal standards (including any encryption requirements imposed by law) and shall meet or exceed accepted security standards in the industry, such as ISO 27001/27002.
- 3.2. The Supplier shall develop, implement and maintain a comprehensive information security program with information security industry standard safeguards in place to define roles and responsibilities, protect Data and to provide Services or Products which comply with the contractual obligations set out in this Agreement. Supplier shall ensure that such information security program is documented, available, and communicated to Supplier employees and subcontractors. Upon request, Supplier shall provide a primary and alternate information security program contact to act as Supplier's contact.

### **4. ACCESS, USE AND DISCLOSURE**

- 4.1. Supplier shall only Process Data and access Information Systems to the extent and manner necessary to provide the Services, in accordance with DXC instructions as set out in this Agreement or as otherwise authorized by DXC in writing.
- 4.2. Any access to or use of DXC Information Systems or Processing of Data by or on behalf of Supplier for any other purpose shall be deemed a material breach of the Agreement by Supplier.
- 4.3. Supplier shall not sell, rent, transfer, distribute, disclose, copy, alter, or remove DXC Data, DXC Information System, or Product unless authorized in writing by DXC.

### **5. SECURITY REQUIREMENTS**

Supplier shall:

- 5.1. Ensure all Processing of Data and provisioning of Services and Products complies with all Applicable Laws. Supplier shall ensure that, where required, Supplier has made the appropriate legal notifications, filings, and registrations and obtained the appropriate permits, as required by Applicable Laws. If Supplier cannot Process the Data or provide Services or Products in accordance with such Applicable Laws and DXC Security Requirements, or believes that DXC instructions violate Applicable Laws, then Supplier shall immediately notify DXC in writing.
- 5.2. Impose on Supplier subcontractors the same obligations imposed on Supplier and DXC customers under the Agreement for the protection of Data, Services, and Products. Supplier shall be responsible for the acts and omissions of its Subcontractors including such actions resulting in a breach of this Agreement. In accordance with obligations applicable separately to each of DXC and its Customer, Supplier shall provide DXC with reasonable cooperation



and assistance needed to fulfil DXC's obligation under contract between DXC and Customer to perform security audits and compliance evaluations related to services rendered.

- 5.3. Regularly, no less frequently than annually, test and monitor the effectiveness of Supplier's and Supplier subcontractor's security program relating to Data, Services and Products to ensure compliance with the security requirements of the Agreement and Applicable Laws. Supplier shall adjust and strengthen its information security program based on the results of such testing and monitoring, as well as in response to operational changes that may have a material effect on Supplier's information security program.

## **6. PERSONNEL SECURITY**

Supplier shall take all reasonable steps to ensure that all Supplier Personnel used to provide the Services under this Agreement, or any SOW, have undergone security checks and have been deemed trustworthy, experienced, and of suitable character and integrity to handle DXC Data. Supplier will advise DXC in advance if a security check of the type required hereunder cannot be performed by Supplier because of any legal or regulatory restraints on investigating personnel in the local venue.

## **7. INFORMATION SECURITY ASSESSMENTS**

DXC, or a third party chosen by DXC, may perform a security assessment "Information Security Assessment" (ISA) of Supplier's Information Systems, Services, Solutions, and Products. DXC may use industry security standards, frameworks and manual techniques to assess the security of Supplier, Services, and Products. Supplier will work cooperatively with DXC to determine whether additional or different security measures are required to protect the Data, Services or Products. Any Information Security Assessment performed by DXC shall be subject to the limitations identified in Scope of Information Security Assessments below.

7.1. DXC may perform an ISA:

7.1.1. Prior to Supplier providing service to DXC ("Pre-service Assessment");

7.1.2. Annually or upon termination / expiration of the Agreement, upon at least 10 (ten) calendar days advanced written notice from DXC ("Routine Compliance Assessment"); and

7.1.3. In the event of a Security Breach and after prior written notice of at least two (2) calendar days.

7.2. Supplier shall promptly disclose to DXC all relevant information requested by DXC in order to allow DXC to complete an ISA. Supplier shall permit DXC to perform an ISA using industry standard tools and manual techniques. The results of the ISA shall be treated as both Confidential Data and confidential data of the Supplier.

7.3. During an ISA, DXC may:

7.3.1. Inspect Supplier's facilities where Data is Processed, Services are performed, or Product is developed, and

7.3.2. View copies or extracts of Supplier's records and processes resulting from Supplier's fulfilment of the requirements of the Agreement. DXC reserves the right to perform an ISA by any of the following methods: onsite inspection, questionnaires with requests for



supporting documentation, technical testing, conference calls, or a combination of such methods.

- 7.4. Scope of Information Security Assessments. Information Security Assessments shall not entitle DXC to view, or in any way access records and/or processes:
  - 7.4.1. Not directly related to Data Processed or Services provided by Supplier to DXC;
  - 7.4.2. In violation of Applicable Laws; and/or
  - 7.4.3. In violation of Supplier's confidentiality obligations owed to a third party that Supplier makes DXC aware of in writing.
- 7.5. Remediation Plan. Any findings during an ISA will be addressed in a mutually agreed upon remediation plan and Supplier shall comply with, and complete, such remediation plan within a mutually agreeable timeframe set forth therein ("Remediation Plan").

## 8. NOTIFICATION

All Notifications, whether related to Security Breach, Inquiry, or non-compliance, shall be made to DXC Security Incident Response and Control Center via email at SIRCC@DXC.com. In the event of a security breach the Supplier will:

- 8.1. Give notice of such Incident to DXC as soon as reasonably possible, and in no event more than one (1) business day, after becoming aware of an actual or suspected Incident. DXC reserves the right to be a participant in, and Supplier shall cooperate with such participation in, any Security Breach investigations involving DXC Data, including DXC's review of forensic data relating to the Security Breach.

## 9. DATA RETENTION

- 9.1. During Agreement Term. Supplier shall retain Data over the term of the Agreement unless otherwise agreed to with DXC. Supplier shall provide DXC with a means to access and manage Data and, where it is not possible for DXC to do so itself, provide DXC with a copy of all Data held by it in the format and on the media reasonably specified by DXC, or update, correct or delete Data on DXC's request.
- 9.2. Upon termination or expiration of Agreement, unless otherwise agreed in writing, consistent with Applicable Laws, Supplier shall: (a) Return all Data in an agreed upon format to DXC or DXC's designated recipient no later than 30 calendar days; and (b) Destroy all Data, no later than 90 calendar days. Upon request, Supplier will provide DXC with a certificate or attestation of return or destruction.



## 10. ENCRYPTION

All Data transmitted by Supplier over any unsecure network or wirelessly (including but not limited to email, instant messaging and web traffic), stored on portable devices, removable media and in transit between Supplier's facilities must be encrypted. Supplier shall at all times meet or exceed the cryptography requirements below. All DXC Data stored on Information Systems must be encrypted at rest. Supplier will implement and maintain industry standard cryptography.

- 10.1. Transmission. Supplier must maintain secure protocols and cipher suites within the environment as accepted by the wider security industry and documented by Qualys SSL Labs best practices (<https://www.ssllabs.com/projects/documentation/>).
- 10.2. Storage. For storage and database (including back up media) encryption, AES must be configured in a secure, industry best practices manner which may be validated by DXC.
- 10.3. Use of Hash Algorithms. The SHA-256, SHA-384, and SHA-512 hash algorithms are approved as minimum acceptable algorithms for performing digital signatures and HMACs. For systems which will not leverage a DXC-provided authentication solution, industry best practices must be followed to hash the password in storage (<https://www.owasp.org/index.pDXC/Password Storage Cheat Sheet>).

## 11. DISASTER RECOVERY

Supplier shall maintain a disaster recovery plan for restoring its current and offsite Data files Processed pursuant to the Agreement. Supplier will be responsible for routine backups and preservation of any Data Processed on behalf of DXC. All backup copies of Data shall be treated as Confidential Data.