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 Services, LLC ("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.

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.

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 processed 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 systems and other information systems used and all associated authentication methodologies.

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 fulfillment 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.

3.3 Supplier shall ensure that supplier and any sub-contractor acting under Supplier authority shall, Process and Transfer the Personal Data only (i) as needed to provide the Services and (ii) in accordance with the specific documented instructions Supplier has received from DXC and/or DXC customer, as set forth in the Agreement, DXC, and any applicable Statements of Work (SOW), unless required otherwise to comply with any other applicable laws, in which case Supplier shall provide prior notice to DXC of such legal requirements, unless that law prohibits this disclosure on

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 ensure that only such of Supplier's personnel who may be required to assist it in meeting its obligations under this Agreement shall have access to the DXC Data.

4.4 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.

4.5 In the event of any change to the scope of the Services, Products or Data made available to Supplier, the parties shall review the Data Security clauses and consider any amendments required by either party as a consequence of the change in scope.

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 Meet or exceed physical, technical, and administrative safeguards as identified in DXC Security Requirements and any of its Agreement, to ensure that DXC Data, Product and Services are protected against Security Breach.

5.3 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 fulfill DXC's obligation under contract between DXC and customer to perform security audits and compliance evaluations related to services rendered.

5.4 Provide annual training regarding compliance with physical, technical, and administrative information security safeguards and compliance with this agreement to Supplier employees and subcontractors.

5.5 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. CLOUD, XaaS, ASP OR OTHER HOSTING SERVICES

If Supplier will be hosting or providing an DXC customer or DXC employee-facing solution/service/website ("Solution"), this section shall apply.

7.1 For any DXC customer or DXC employee-facing Solution hosted on behalf of DXC, but not DXC branded, Supplier shall:

(a) Clearly and conspicuously communicate to users that Supplier is the Solution provider; and
(b) Clearly and conspicuously communicate Supplier's privacy policy to the users. If the Solution is co-branded, both companies' privacy policies must be clearly and conspicuously posted.

7.2 Provide appropriate controls to maintain logical data segregation of Data from Supplier's other customer data. It must not be possible for data to be disclosed to other parties, nor should Supplier personnel with direct access to Data have cross customer access with DXC competitors.

7.3 For any internet-accessible application requiring DXC user access, Supplier shall accept and implement SAMLv2 DXC assertions.

7.4 The Cloud, XaaS, ASP or Other Hosting Services must have a current anti-malware software solution installed which is to be a licensed and managed, commercial-grade product with a current anti-malware engine and real- time protection enabled. Furthermore, anti-malware definitions are not to be more than two (2) days old.

7.5 Ensure the Solution is free of common web application security vulnerabilities as defined by, but not limited to, the OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

7.6 Any vulnerability findings discovered by either DXC or Supplier 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.

8. INFORMATION SECURITY ASSESSMENTS AND VULNERABILITY SCANNING.

8.1 Information Security Assessments. DXC, or a third party chosen by DXC, may perform a security assessment ("Information Security Assessment") 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 and Vulnerability Scanning below.

8.1.1 DXC may perform an Information Security Assessment:

(a) Prior to Supplier providing service to DXC ("Pre-service Assessment")
(b) Annually or upon termination/expiration of the Agreement, upon at least 10 calendar days advanced written notice from DXC ("Routine Compliance Assessment"); and
(c) In the event of a Security Breach and after prior written notice of at least two (2) calendar days.

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

8.1.3 During an Information Security Assessment, DXC, or a third party selected by DXC, may:

(a) Inspect Supplier's Facilities where Data is Processed, Services are performed, or Product is developed, and,
(b) View copies or extracts of Supplier's records and processes resulting from Supplier's fulfillment of the requirements of the Agreement, DXC reserves the right to perform an Information Security Assessment by any of the following methods: onsite inspection, questionnaires with requests for supporting documentation, technical testing, conference calls, or a combination of such methods.

8.1.4 If DXC reasonably determines that any portion of the Information Security Assessment must be performed at Supplier's Facilities, the assessment will be performed:

(a) not more frequently than once per calendar year (unless there has been a Security Breach),
(b) At DXC's expense for travel and per diem,
(c) On a date and time mutually agreeable to Supplier and DXC, and
(d) Pursuant to any other restrictions and/or limitations mutually agreed to by DXC and Supplier in writing.

8.2 VULNERABILITY SCANNING

8.2.1 DXC may perform periodic vulnerability scanning using industry standard tools and manual techniques to assess the security of Supplier, Services, and Product ("Vulnerability Scanning").

8.2.2 Vulnerability scanning results shall be communicated to Supplier and treated as both Confidential Data and confidential data of Supplier.

8.2.3 Authorized DXC cyber security professional(s) may work with Supplier to manually validate findings on production and test systems in order to help reduce false positives.

8.2.4 If Supplier utilizes a third party co-location facility in support of Services, Supplier shall be responsible for (a) informing such third party of DXC's rights and (b) ensuring Supplier has written authorization from such third party allowing DXC to conduct Vulnerability Scanning.

8.2.5 Vulnerability scanning process includes background research using publicly available information.

8.3 Scope of Information Security Assessments and Vulnerability Scanning.

Information Security Assessments, and Vulnerability Scanning shall not entitle DXC to view, or in any way access records and/or processes:
8.3.1 Not directly related to Data Processed or Services provided by Supplier to DXC;

8.3.2 In violation of Applicable Laws; and/or

8.3.3 In violation of Supplier's confidentiality obligations owed to a third party that Supplier makes DXC aware of in writing.

8.4 Remediation Plan. Any findings during an Information Security Assessment and Vulnerability Scanning 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").

9. **DATA RETENTION**

During Agreement Term and Termination.

9.1 Supplier shall retain Data over the term of the Agreement unless otherwise agreed to with DXC. If Supplier cannot retain the Data, Supplier will regularly provide such Data to DXC for DXC to retain.

9.2 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.

9.3 Unless otherwise agreed to by DXC and Supplier in writing, in a manner consistent with Applicable Laws, Supplier shall either (a) destroy all Data, including, without limitation, any and all copies and derivatives thereof, no later than 90 calendar days after the termination or expiration of the Agreement or portion thereof; or (b) return all Data in an agreed upon format to DXC or DXC's designated recipient no later than 30 calendar days after the termination or expiration of the Agreement or portion thereof.

9.4 If Supplier is unable to return or destroy the Data per Applicable law, Supplier shall (a) notify DXC, (b) cease from actively Processing the retained DXC Personal Data, (c) and implement security measures to protect the data.

9.5 Supplier may retain limited transactional data to meet legal or business requirements.

9.6 Upon request by DXC, Supplier will provide DXC with a certificate or attestation of return or destruction

9.7 If DXC reasonably suspects that Supplier has not adequately removed or returned Data, DXC or a third party selected by DXC may audit Supplier. If the audit identifies Supplier's unauthorized retention of Data, then Supplier shall reimburse DXC for the cost of the audit.

9.8 Data Placed on 'Legal Hold'. Supplier will not block, erase or dispose of any Data which Supplier has been notified it must retain in response to an DXC "Legal Hold". In the event that Supplier believes it is legally required to destroy Data on Legal Hold, Supplier must notify, consult and cooperate with DXC prior to any destruction. Supplier obligations to retain such "Legal Hold" Data shall not be limited by any agreed-to records

or data retention policies or internal policies of Supplier. If Supplier cannot retain the "Legal Hold" Data, Supplier will provide the Data to DXC for DXC to retain.

10. **NOTIFICATION**

10.1 All Notifications, whether related to Security Breach, Inquiry, or non-compliance , shall be made to DXC Security Incident Response and Control Center via (a) email at SIRCC@DXC.com and (b) telephonically to +**61 283499651**.

10.1.1 **DXC subcontractor to adhere to customer requirements**

10.2 In the event of a security breach the Supplier will:

(a) 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.

(b) make a written report to DXC as soon as possible, but no later than five (5) business days after having ascertained the existence of such Incident, that contains all then known information concerning the nature and impact of the Incident, including but not limited to identifying the DXC Data relating, directly or indirectly, to the Incident and all governmental and agency reporting or disclosing relating to the Incident that has occurred or is being contemplated, and Supplier's steps to mitigate this impact. Further, Supplier shall, at its own costs, cooperate as reasonably requested by DXC in order to further investigate and resolve the Incident. In the event of an Incident caused by Supplier or any of its subcontractors, agents or other representatives engaged in the Processing of DXC Data, Supplier agrees to pay all costs and expenses associated with the Incident that DXC may incur, including but not limited to notification costs and costs relating to credit monitoring. Supplier agrees to secure and preserve all evidence and logs pertaining to such Incident, to take no action that would impair evidence or the tracking and tracing of the Incident, to make no public statements to the press regarding the Incident without approval from DXC, and to inform DXC without delay of any and all interactions with law enforcement in connection with such Incident.

10.3 Notification of Inquiry

10.3.1 Except where expressly prohibited by Applicable Laws, Supplier shall, prior to any disclosure, notify DXC of any claim or information request received from a judicial, governmental authority, Customer or DXC employee, that it receives (each, for purposes of this DNSS an "Inquiry") to allow DXC to object and intervene.

10.3.2 In the event Supplier is expressly prohibited by law from notifying DXC, Supplier shall formally request the inquirer to seek the Data directly from the Data Controller. Notification of an Inquiry to DXC shall include a copy of the request and any supporting details. Supplier shall use commercially reasonable efforts to provide DXC with notification within one (1) business day after Supplier becomes aware of an Inquiry.

10.3.3 Within 5 business days of receipt, Supplier shall promptly provide DXC with such information and assistance, at no additional cost to DXC, as is required by any court of competent jurisdiction or national regulatory authority, or as is required to timely respond to or otherwise address any Inquiry, access request, complaint, enforcement notice, claim or similar action raised.

10.4 Breach of Agreement

10.4.1 Supplier agrees that any Processing of DXC Data in violation of applicable Data Privacy Laws, the provisions of the Agreement (including any SOW), Section 'Data Protection and Privacy' and/or Section 'Data Security' shall constitute a material breach of this Agreement and may cause immediate and irreparable harm to DXC for which monetary damages may not constitute an adequate remedy.

Therefore, the parties agree that DXC may seek specific performance and/or injunctive or other equitable relief for such violation, in addition to its remedies at law, without proof of actual damages or for the security or posting of any bond in connection with such remedy. In addition to all other legal and contractual rights, if Supplier has breached the 'Data Protection and Privacy' and 'Data Security' sections of this Agreement, DXC may, at its absolute sole discretion, terminate this Agreement, in whole or in part (with respect to any affected SOW) or suspend the transfer to or Processing of DXC Data by Supplier or any Supplier subcontractor for such time reasonably determined by DXC in order for Supplier to remedy such breach. In the event Supplier does not remedy such breach within the allotted timeframe, DXC shall be entitled to terminate the Agreement, effective immediately upon notice of termination (or such other time as stated in such notice).

11. MOBILE DEVICE SECURITY

If Supplier is using mobile devices to support or provide Services to DXC, Supplier shall:

11.1. Implement a policy that prohibits the use of any mobile and portable devices that are not administered and/or managed by Supplier.

11.2 As defined in this Agreement, Encryption requirements below, use encryption, to protect all Data stored on, transmitted by, or remotely accessed by mobile and portable devices.

11.3 When using network-aware mobile and portable devices that are not laptop computers to access and/or store Data, such devices must:

(a) Apply remote wipe capabilities;

(b) Promptly initiate deletion of all Data when the device is lost or stolen; and,

(c) Automatically delete all stored Data after a reasonable number, not to exceed ten (10), consecutive failed login attempts.

12. ENCRYPTION

12.1 All DXC 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:

12.2 Key Lifecycle.

12.2.1 Keys must be generated in a secure manner.
12.2.2 Keys must only be available to authorized users.
12.2.3 Keys must be protected from unauthorized use, disclosure, alteration, and destruction.
12.2.4 If the private key associated with an asymmetric key pair is compromised for any reason, all associated certificates must be revoked.
12.2.5 Keys must have an appropriate lifetime which does not exceed two years, after which they are securely destroyed.

12.3 DXC Approved Cryptography. Supplier will implement and maintain industry-standard cryptography.

12.3.1 Transmission.

(a) The vendor 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/
(b) An "A" rating or above is required on the Qualys SSL Labs SSL Server Test: https://www.ssllabs.com/ssltest/. Upon DXC's request, Supplier shall provide server test documentation.

12.3.2. Storage.
For storage and database (to include back up media) encryption, AES must be configured in a secure, industry best practices manner which may be validated by DXC.

Use of Hash Algorithms

(a) The SHA-256, SHA-384, and SHA-512 hash algorithms are approved as minimum acceptable algorithms for performing digital signatures and HMACs.
(b) For systems which will not leverage an DXC-provided authentication solution, industry best practices must be followed to hash the password in storage.
https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet PGP. RIPE-MD/160 Algorithm. RIPE-MD/160 algorithm is approved for use with the OpenPGP protocol.

12.3.3 If at any time the above noted cryptography is no longer recognized as an industry best practice, or if Supplier is unable to implement cryptography consistent the requirements of this Agreement, Supplier must receive DXC Security written approval prior to implementing alternate cryptography.

12.3.4 Where DXC Information is stored on non-portable devices and media capable of data storage and transmissions, Supplier shall ensure that such devices and media are protected to prevent unauthorized logical and physical access. When such data storage mediums are destroyed or repurposed, any DXC Information contained therein is to be deleted or destroyed to industry standards that render it unreadable.

13. **DISASTER RECOVERY**

13.1 Supplier shall maintain a disaster recovery plan for restoring its current and offsite Data files Processed pursuant to the Agreement.

13.2 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.

13.3 Supplier will maintain a business continuity plan for restoring its critical business functions.

13.4 Upon request, Supplier will allow DXC to view the disaster recovery and business continuity plans.

Addendums to be added where relevant:

14. **NETWORK CONNECTIVITY & NETWORK SECURITY**

If Supplier is (1) utilizing a remote Network Connection or (2) utilizing a Network Connection at an DXC Facility to Process Data or provide Services, this section shall apply.

14.1 Supplier's Use of Network Connection.

14.1.1 Network Connection, duration of connection and mechanism to transmit Data between Supplier and DXC shall be through DXC IT approved secure solution.

14.1.2 Supplier may only use the Network Connection for the business purposes as authorized by DXC.

14.1.3 Supplier will allow only Supplier's employees who are approved in advance by DXC ("Authorized Supplier Employees") to authenticate and access DXC Information Systems or DXC Owned Equipment.

14.1.4 Supplier shall be solely responsible for ensuring that Authorized Supplier Employees are not security risks, and upon DXC's request, Supplier will provide DXC with any information reasonably necessary for DXC to evaluate security issues relating to any Authorized Supplier Employee.

14.1.5 Supplier will promptly notify DXC whenever any Authorized Supplier Employee no longer requires access to DXC Information Systems or DXC Owned Equipment.

14.2 Use of DXC Owned Equipment at Supplier Facilities.

14.2.1 DXC may, at DXC's sole discretion, loan to Supplier equipment or software for use in Supplier Facilities ("DXC Owned Equipment") under the terms of an DXC Equipment Loan Agreement. DXC Owned Equipment will be used solely by Supplier at Supplier's Facilities and for the purposes set forth in the Agreement or an DXC Equipment Loan Agreement.

14.2.2 Supplier may not modify the configuration of the DXC-Owned Equipment unless otherwise set forth in the Agreement or DXC Equipment Loan Agreement.

14.3 Use of Supplier-Owned Equipment at DXC Facilities. DXC may, at DXC's sole discretion, authorize Supplier to utilize Supplier-owned equipment in DXC Facilities. Supplier-owned equipment must conform to the applicable security standards set forth in this DNSS.

14.4 Security of DXC Network. Supplier shall ensure its use of the Network Connection (and Supplier's use of DXC-Owned Equipment) is secure and is used only for authorized purposes, and that DXC Data and Information Systems are protected against improper access, use, loss, alteration, or destruction.

DATA, SERVICE AND PRODUCT SECURITY REQUIREMENTS

15. Manufacturing on Behalf of DXC. If Supplier is providing supply chain or manufactured Products, Supplier shall:

15.1 Ensure shipping and logistics processes are certified as compliant with the Customs Trade Partnership against Terrorism (C-TPAT) program or comparable programs approved by DXC.

15.2 Perform security and integrity testing, according to sampling rates established in writing by the DXC business unit, on logic bearing components, software and/or code development, and on final Products prior to shipment to ensure that Product has not been tampered with or altered and that malware or unexpected code or files have not been installed.

15.3 Ensure only DXC authorized software and images are utilized.

15.4 Upon DXC's request, provide a certificate of physical destruction for any failed or faulty Product. Certificates of destruction must be retained per the data retention requirements agreed to in writing.

15.5 Ensure that information and processes used to capture production metrics (such as quality and quantity reporting) and associated metrics data and records are not altered.

16. Product Security and Integrity. If Supplier is providing or developing Product (Original Equipment Manufacturer (OEM) or other code based Product), Supplier warrants that:

16.1 Supplier shall meet or exceed security industry best practices throughout the Product development lifecycle and throughout the deployment of Product developed for or licensed by DXC. Such Security industry best practices include, but are not limited to:

(a) Prohibit the use of real or production data in a test or development environments;
(b) Security reviews and approvals throughout the design and development of the Product;

(c) Security testing of all code and Product additions, deletions or modifications prior to release:

(i) Conduct threat modeling, static code analysis and black box testing for known vulnerabilities, which should include SANS Top 20 or OWASP Top 10 vulnerabilities;
(ii) Conduct routine scanning and manual testing for new vulnerabilities;
(iii) Remove test and debugging related files, executables or program insertions, such as backdoors;

(d) Upon request, Supplier shall provide DXC with a copy of test results and associated remediation efforts;

(e) If the Product is internet-accessible or holds Sensitive Personal Data, Supplier shall provide to DXC the results and remediation efforts of an independent software security testing assessment performed at Supplier's sole cost;

(f) DXC shall have the right to perform its own security testing on the Product; and

(g) Supplier shall notify SIRCC@DXC.com and (b) telephonically to +**61 283499651**, within 24 hours of Supplier becoming aware of any suspected or known security vulnerability in a released product.

17. **LOGISTICS SECURITY**

If Supplier is providing logistics services including but not limited to logistics functions such as order fulfillment, packaging, shipping or delivery, on behalf of DXC, DXC Buyers, and/or DXC customers, Supplier must:

17.1 During Customer-defined order fulfillment such as racking and imaging/configuring or testing:

(a) Use only DXC authorized parts; and,

(b) Ensure inventory control processes and records are in place, such as Bill of Material (BOM).

17.2 Obtain DXC's prior written approval before making any order substitution or using any alternate parts.

17.3 Maintain complete and accurate documentation of damaged or destroyed components, parts and/or products during handling and transportation. Upon DXC's request, provide a certificate of physical destruction for any failed or faulty Product. Certificates of destruction must be retained per the data retention requirements agreed to in writing.

17.4 Ensure that software, hardware, components, and system related documentation for DXC Products are not unbundled and are not otherwise tampered with.

17.5 Prohibit processes which compromise Product security and integrity including but not limited to, changing BIOS, using admin passwords, or installing testing software, during post-build testing.

17.6 Ensure that Product is free from any unauthorized components.

17.7. Any Product returned from a customer must be securely erased or disposed

17.8 Upon DXC's request, provide a certificate of secure erasure for any refurbished Product. Certificates of secure erasure must be retained per the data retention requirements agreed to in writing.

17.9 Securely erase, using the NIST 800-88 standard, any used or refurbished components prior to installation into any DXC Product.

18. **CALL RECORDING DATA**

If Supplier is Processing call recordings, then this section shall apply.

18.1 Supplier shall not enable, activate, nor make operational any call recording capabilities for Data collected and processed on behalf of DXC unless approved by DXC in writing.

18.2 Supplier shall notify the other party that Supplier is recording the conversation ("Recording Notice") and include the ability to disable inbound and outbound call recordings if so requested.

18.3 Recording Notice shall comply with Applicable Laws and must include the clear and specific purpose of the recording such as quality monitoring, workforce management, agent and customer service representative training, evaluation and verification, dispute resolution or accurate incident reconstruction.

18.4 Permission must be obtained from DXC in writing for 50% or greater recording of Call Recording Data.

18.5 If Supplier intends to use call recordings for Supplier's internal training purposes, Supplier shall redact all Personal Data.

18.6 Call recordings must be promptly deleted after Supplier satisfies the specific purpose stated in the Recording Notice, which must in no case be longer than 90 calendar days after the original recording was made, unless otherwise authorized by DXC in writing.

18.7 Call recordings must be protected in accordance with this Agreement.

19. **PROCESSING PAYMENT CARDS**

If Supplier will be Processing Payment Card Data, then this section shall apply.

19.1 All capitalized terms used in this section, but not defined in this Agreement shall have the meaning ascribed to them in PCI SSC DSS.

19.2 Supplier shall comply with the current Payment Card Industry Security Standards Council Data Security Standards ("PCI SSC DSS").

(a) Prior to commencement of Services and annually thereafter, Supplier shall provide (i) a copy of the executive summary from the current Report on Compliance (“RoC”) or a letter of attestation signed by a PCI SSC certified QSA describing the scope and Services assessed; and (ii) an Attestation of Compliance (“AoC”) signed by a PCI SSC certified QSA.
(b) PCI compliance artifacts as described in this section shall be submitted to DXC via encrypted email.

19.3 Upon completion of the services under any Statement of Work or termination of the Agreement, Supplier will promptly remove all Payment Card Data from Supplier’s Information Systems in accordance with the required process under PCI SSC DSS or other applicable standard no later than the earlier of 90 days from termination of the services.

19.4 Supplier will notify DXC immediately if at any time Supplier is not in compliance with PCI SSC DSS and if at any time Supplier knows of any third party claim regarding PCI SSC DSS compliance.