Diebold Nixdorf

SUPPLIER SECURITY REQUIREMENTS

Supplier shall at all times comply with the requirements set forth in these SUPPLIER SECURITY REQUIREMENTS ("**Security Requirements**"). These Security Requirements are deemed a part of and incorporated into the Master Services Agreement to which these Security Requirements are attached or incorporated (the "**Agreement**"). The provisions set forth in these Security Requirements shall control in the event of a conflict between the terms and conditions of the Agreement (including any other schedules, exhibits or attachments to the Agreement) and these Security Requirements. Capitalized terms not defined in these Security Requirements shall have the meanings ascribed to them in the Agreement.

1. DEFINITIONS

a. "**Confidential Information**" has the meaning attributed to it in the Agreement and shall also include: (i) all data, formulae, processes, Cardholder Data (as defined in PCI DSS), procedures, procurement strategies and practices, fees, purchasing volumes, documentation, conclusions, analysis, information, Personal Data, records, specifications, evaluations, know how, business, assets, products, processes, and prospects related to DN communicated to, supplied to, or observed by Supplier, directly or indirectly, at any time, (ii) information related to usage of the Supplier Environment, reports and any data gathered, created or compiled by Supplier as a part of or in connection with the Services hereunder, and (iii) any other information that Supplier should reasonably understand to be considered Confidential Information whether or not such information is marked "Confidential" or contains such similar legend at the time of disclosure. For the purposes of the Security Requirements, any reference to "Confidential Information" shall mean "DN Confidential Information".

b. "**DN Environment**" means any and all facilities, equipment, workstations, servers, cloud environments, software, mobile devices, networks, storage devices, applications, and other systems owned and managed by DN.

c. "**Industry Standards**" means the most current version of the following industry standards, as may be updated or replaced from time to time, reasonably selecting between NIST and ISO standards, which include:

- ISO 27001 – Security techniques – Information security management systems – Requirements.
- ISO 27002 – Security techniques — Code of practice for information security controls.
- NIST Cyber Security Framework and applicable controls NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations.
- NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations.
- NIST Special Publication 800-190 Application Container Security Guide.
- CIS—Center for Internet Security.
- if Confidential Information is Processed or stored in a public cloud, compliance with a "moderate" impact security level in accordance with FedRAMP.
- CSA - Cloud Controls Matrix version 4.
- PCI DSS.
- PA DSS.
- NIST Special Publication 800-88 - Guidelines for Media Sanitization.
- NIST Special Publication 800-61 - Computer Security Incident Handling Guide.
- NIST Special Publication 800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

d. "**Personnel**" means the employees of Supplier and its subcontractors, including permanent employees, fixed-term contract employees, and temporary workers.

e. "**Supplier Environment**" means any and all Supplier or subcontractor facilities, equipment, workstations, servers, cloud environments, software, mobile devices, networks, storage devices, applications, and other systems that Process Confidential Information, or that provide or are used in connection with providing the Services to DN.

2 SECURITY PROGRAM AND RISK MANAGEMENT

2.1 **Information Security Program.** Supplier shall, on a continuous basis while storing or otherwise Processing Confidential Information, develop, implement, maintain, monitor, and as necessary improve and update a comprehensive, written information security program applicable to the protection of the security, confidentiality, integrity, and availability of Confidential Information (the "**WISP**"). Such WISP shall be reasonably consistent with Industry Standards, best practices, and applicable law, and shall contain administrative, technical, and physical safeguards necessary to protect and ensure the security, confidentiality, integrity, and availability of the Supplier Environment and Confidential Information. The WISP must include a documented plan for incident prevention, detection, and response in accordance with Industry Standards and applicable law, which is reviewed at least annually.

2.2 **Point of Contact.** Supplier shall identify a single point of contact for all communications regarding information security who shall: (i) serve as DN's primary security contact, (ii) have an appropriate level of industry security training and experience, and (iii) be available to assist DN twenty-four (24) hours per day, seven (7) days per week in the event of a Security Breach.

2.3 **Supplier Personnel Training.** Supplier shall ensure that Personnel who will have access to DN's Confidential Information, DN Environment and the Supplier Environment are regularly trained on how to comply with Supplier's WISP and the terms of these Security Requirements. Only Supplier Personnel with a business need in connection with the Services provided during the course of the Agreement may have access to Confidential Information. Supplier's WISP shall take into account whether and how Personnel should be allowed to use or otherwise Process records containing Confidential Information inside and outside of business premises. Supplier will impose disciplinary measures for violations of the WISP and these Security Requirements by its Personnel.

2.4 **DN Provided Training.** Supplier acknowledges that any of its Personnel who have access to the DN Environment shall be required to attend DN security training as determined by DN from time to time. Supplier shall ensure that its Personnel complete such required training.

2.5 **Risk Assessment.** Supplier shall conduct regular (at least annually) assessment of the internal and external risks to the security, confidentiality, integrity, and availability of Confidential Information and the Supplier Environment ("**Risk Assessments**"). Risk Assessments shall be conducted following Industry Standards and best practices, and, without limiting the foregoing, shall at least include vulnerability scanning, penetration testing, social engineering tests, infrastructure design assessments, and data communication assessments.

2.6 **Risk Management.** Supplier shall ensure that Supplier's WISP, the Supplier Environment, and the Services are: (i) designed, maintained, updated, and adjusted, as necessary and at Supplier's sole cost and expense, to adequately control and mitigate the risks identified through Supplier's Risk Assessment, and (ii) regularly tested and monitored to ensure the effectiveness of the key controls, safeguards, systems, and procedures.

3 SUPPLIER ADMINISTRATION AND EMPLOYEES

3.1 Security Administration. Supplier shall manage administrative controls over its compliance with these Security Requirements.

3.2 Security Administrators. In accordance with Industry Standards, Supplier must take appropriate actions to prevent unauthorized access to and use of the Supplier Environment and Confidential Information. Supplier management Personnel must retain sole responsibility for granting access to the Supplier Environment for all Personnel.

3.3 Personnel Access. Personnel access must be given following the "least privileged principle" and access must be modified upon the change of job function, transfer, or termination of any Personnel who has access to the Supplier Environment or Confidential Information. Supplier must limit Personnel access to the Supplier Environment for the purpose of making maintenance changes to only those Personnel who require access by their job responsibilities and in accordance with the least privileged principle.

3.4 Supplier Personnel. Supplier must require its Personnel to report suspected violations of Supplier's security policies (including the WISP) to Supplier management for investigation and action. Supplier must implement and document consequence management policies for violations of Supplier's security policies (including the WISP).

4 CONTROLS AND REQUIREMENTS

4.1 **Controls and Requirements.** Supplier shall implement and maintain such controls, processes, technology, training, and procedures as is necessary to protect the security, confidentiality, integrity, and availability of Confidential Information and the Supplier Environment. Without limiting the generality of the foregoing, and except where Industry Standards or applicable law require more protective measures, Supplier shall at least comply with the more particular requirements that follow in this Section 4.

4.2 Encryption. Supplier shall encrypt all Confidential Information in transit and at rest, in accordance with Industry Standards, and must be at least FIPS 140-2. Any exceptions must be previously agreed by DN in writing. Passwords stored in databases must be one-way hashed and otherwise meet Industry Standards and best practices. All Confidential Information stored in Supplier repositories or otherwise backed up must be encrypted prior to backup.

4.3 Logs. Supplier shall log, in accordance with Industry Standards and best practices, all activities by its Personnel and others related to accessing the Supplier Environment and Processing Confidential Information. Logs must be retained for a minimum of two (2) years. Supplier shall maintain log management operational processes consistent with Industry Standards and best practices. Logging must at a minimum include the following: date and time of each logged event; when session ends; source and destination IP address; user ID; details of attempted, successful and rejected access attempts; type of activity performed; and modifications. Supplier must maintain such logs in accordance with applicable law and these Security Requirements.

4.4 Data Security Controls. Supplier must document, implement, maintain, and update adequate data security controls in Supplier Environment, such as, but not limited to, logical access controls including user sign-on identification and authentication, data access controls (e.g., password protection of Supplier Environment, data files, databases, repositories, and libraries), accountability tracking, anti-virus software, secured printers, and restricted download to disk capability.

4.5 Systems Security. Supplier shall establish and maintain a security system covering the Supplier Environment, including any wireless systems, that, at a minimum, shall have the following elements:

4.5.1 Secure user authentication protocols including: (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices, (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect, (iv) restricting access to active users and active user accounts only, and (v) blocking access to user identification after multiple unsuccessful attempts to gain access or other limitations placed on access for the particular system.

4.5.2 Secure access control measures that: (i) restrict access to records and files containing Confidential Information to those who need such information to perform their job duties, and (ii) assign unique identifications plus passwords, which are not Supplier supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

4.5.3 Networks in the Supplier Environment must be configured so that each desktop and all inbound and outbound mail servers have current anti-virus protection. The Supplier Environment shall include up-to-date versions of system security agent software which must include malware protection and up-to-date patches and virus definitions (all of which must be set to receive the most current security updates on a regular basis). For files containing Confidential Information on the Supplier Environment, there must be up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of Confidential Information.

4.5.4 Supplier shall use commercially reasonable efforts to log, monitor, and prevent the installation, spread, and execution of malicious software in the Supplier Environment, and take immediate defensive and corrective actions in accordance with Industry Standards and best practice.

4.6 Patching. Supplier shall implement and maintain a patch management program that covers the Supplier Environment and that follows Industry Standards and best practices. Supplier shall scan the Supplier Environment for and remediate vulnerabilities on a continuous basis in a timeframe commensurate with the severity of the vulnerability, not to exceed the following timeframes:

- Critical vulnerabilities (CVSS Score 9.0+ or the equivalent) = 30 days
- High vulnerabilities (CVSS Score 7.0-8.9 or the equivalent) = 30 days
- Medium vulnerabilities (CVSS Score 4.0-6.9 or the equivalent) = 90 days

- Low vulnerabilities (CVSS Score < 4.0 or the equivalent) = 180 days

Where for good cause (e.g., because the patch failed testing) a patch cannot be timely implemented, Supplier shall implement effective compensating and mitigating controls.

4.7 Supplier Network. All access to the Supplier Environment shall require multi factor authentication, including a user ID and password or an equivalent security credential. Supplier must ensure that user IDs and passwords for the Supplier Environment are controlled as follows: (i) unique ("single user") ownership of user ID, (ii) no "generic" or group user ID, (iii) immediate revocation or deletion of all access rights for any terminated, leave of absence, or transferred Personnel, (iv) access rights to Confidential Information shall be provided on a "need to know", job function basis, (v) if a user ID is revoked, re-authentication and positive identification of the user must occur before the user ID can be reactivated, and (vi) passwords must meet Industry Standards or regulatory standards, as applicable. User IDs must be locked after no more than five (5) failed log-in attempts and must remain locked until the system administrator for the system resets the user's account, or until the allotted time to automatically reset login attempts has passed which shall be at least ten (10) minutes.

4.8 System and Network Security. Supplier must document and maintain adequate network-based and end point intrusion detection capabilities and intrusion prevention capabilities.

4.9 Backups and Disaster Recovery. Supplier shall regularly maintain secure backups of the Supplier Environment, including any Confidential Information, sufficient to recover the Services and the Supplier Environment from events that affect the security, integrity, or availability of Confidential Information and the correct and sufficient provision of the Services. Supplier shall maintain business continuity and disaster recovery plans, and the means to successfully execute such plans, to meet its requirements herein. Supplier shall carry out annual tests to ensure its backup and disaster recovery plans meet these requirements.

4.10 Changes to Security. Supplier shall notify DN of any technical or policy change that may materially decrease the level of security in the Supplier Environment or that may cause the Supplier to not be in compliance with these Security Requirements. Supplier shall notify DN at least 30 days prior to such changes being implemented.

5 PHYSICAL SECURITY CONTROLS

5.1 **Sites.** Supplier must document, implement, maintain, and update adequate physical security controls over all facilities hosting the Supplier Environment and where Confidential Information is Processed (collectively, "**Sites**"). Without limiting the foregoing, Supplier shall implement and maintain reasonable restrictions upon physical access to Confidential Information, including a written procedure that sets forth the manner in which physical access to such records is restricted. Storage of records and data must be done in locked facilities, storage areas, and containers. Supplier shall implement at the Sites security and environmental controls over all computer rooms and equipment that will be used in conjunction with Confidential Information and the Services, including restricting access to only approved staff.

5.2 **Secure Disposal.** Supplier shall implement at the Sites secure disposal programs that provide for the secure disposal and destruction of all storage media (e.g., data tapes, hard drives and other storage media containing Confidential Information) and any discarded material (including electronic media) that contains or could disclose Confidential Information. Such programs must be implemented in accordance with Industry Standards.

6 DN ENVIRONMENT

6.1 Access to the DN Environment. Supplier may only access the DN Environment from a Supplier authorized service location for the purpose of performing the Services under the Agreement. Supplier will not allow access to the DN Environment to any third parties without prior written consent from DN. Any such access is subject to additional policies, controls, and requirements provided by DN from time to time. All access to the DN Environment shall be via a DN approved secured connection.

6.2 Workstations. Supplier must ensure all workstations which allow access to Confidential Information and the DN Environment or which are used to provide the Services are controlled and protected in accordance with these Security Requirements, including, without limitation, required firewalls, antivirus software, intrusion detection, and endpoint detection and response applications. All such workstations must be: (i) equipped with appropriate access control, including password protected screen savers, and time-out after 15 minutes or less of non-use, and (ii) configured such that they do not enable or facilitate the transfer of Confidential Information by any portable storage medium (e.g., Zip Drives, USB memory devices, etc.), by email, or by other means such that Personnel could distribute Confidential Information without permission or consent by DN or as

permitted under the Agreement. Workstations must be configured so that Personnel cannot download or install software from any source other than those expressly approved by Supplier. Persistent local administrator permissions are prohibited.

6.3 User access. Upon request, Supplier shall provide an updated list of all accounts, users, profiles, or similar access credentials which have access to the DN Environment.

7 SECURITY INCIDENTS

7.1 Security Breaches. In the event Supplier becomes aware of any actual or reasonably suspected unauthorized access to or use, disclosure, alteration, loss or destruction of Confidential Information and/or the Supplier Environment ("**Security Breach**"), Supplier shall, within twenty-four hours after becoming aware of a Security Breach, notify DN of such Security Breach via email to InformationSecurity@dieboldnixdorf.com, specifying the details of the Security Breach and what Confidential Information has been impacted. For the avoidance of doubt, ransomware attacks affecting Confidential Information, or the Supplier Environment are considered Security Breaches.

7.2 Response. Supplier shall: (i) immediately take action to contain such Security Breach and mitigate potential risks to Confidential Information and the Supplier Environment, and the DN Environment (to the extent impacted), (ii) investigate the Security Breach (including determining what systems, data, and information have been affected by the Security Breach) and perform a root cause analysis thereon, (iii) report its findings to DN on a continuous basis (at least daily) until the investigation is completed, as reasonably determined by agreement of the Parties, (iv) provide DN with a remediation plan to address the Security Breach and prevent any further incidents, (v) remediate the Security Breach, (vi) cooperate with DN and, at DN's request, any law enforcement or regulatory officials investigating such Security Breach, and (vi) provide all reasonably requested evidence and information in relation to the Security Breach (i.e.: logs, reports, etc.).

7.3 **Notification**. Except where required by applicable law, (i) Supplier shall not notify any third party (including any individual or government authority) of any Security Breach without first obtaining DN's prior written consent, and (ii) DN shall have the sole right to determine the contents of any such notice of a Security Breach to the extent that it may be associated with or linked to DN.

7.4 **Reimbursement**. Supplier shall indemnify and reimburse DN for all Security Breach Related Costs (defined below) incurred by DN arising out of or in connection with a Security Breach. Such indemnification and reimbursement obligation is not capped or limited by the Agreement, including any limitation on liability therein. "Security Breach Related Costs" means any costs associated with addressing and responding to a Security Breach, including, but not limited to: (i) preparation and mailing or other transmission of notifications to impacted individuals and/or governmental authorities; (ii) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (iii) public relations and other similar crisis management services; and (iv) legal, forensic and accounting fees and expenses associated with DN's investigation of and response to such Security Breach.

8 AUDITS AND VERIFICATION

8.1 **Operational Audits.** Once a year, or whenever there is a Security Breach, a breach of these Security Requirements, or as requested by a regulator, Supplier shall give DN and its auditors (including internal audit staff and external auditors) access at all reasonable times to the Supplier Environment, Confidential Information, and any Supplier facility relating to the Services, for the purpose of performing audits of either Supplier or any of its subcontractors to verify whether the Supplier's or its subcontractors' security practices comply with applicable law and these Security Requirements. Supplier shall make appropriate Personnel available to facilitate the audit process.

8.2 **Security Questionnaires.** Supplier shall complete and return any information security survey, information request or questionnaire provided by DN within 10 business days after receipt.

8.3 **Third Party Audits.** At DN's request, and for no additional compensation, Supplier shall provide its SSAE 18 SOC 1, SOC 2 Type II, and ISO 27001 (or their successor standards) audit of controls report applicable to the Services and related Supplier Environment.

8.4 **Documentation.** Supplier must, upon DN's request, provide to DN: (i) copies of all internal security policies, network architecture/diagrams in relation to the Services, and standards for DN's review, and (ii) a copy of the most recent internal and/or third-party data processing or security audit or review reports, including any recent risk or security assessments, reports on compliance, penetration tests, vulnerability scans, and controls assessments, that may apply.

8.5 **Access to reports.** DN shall have the right to provide all reports, opinions and certifications delivered hereunder to its employees and professional advisors who shall have obligations of confidentiality regarding such information and only on a need-to-know basis. DN may provide such reports, opinions, and certifications to a government regulator.

8.6 **Monitoring.** DN reserves the right to monitor access and use of the DN Environment in any manner determined by DN.

9 OTHER SECURITY REQUIREMENTS

9.1 **Secure Software Standards.** Supplier represents and warrants any software developed as part of or in connection with the Services will be securely developed and maintained throughout the software development life cycle following Industry Standard secure coding processes, practices, training, testing, and controls. Supplier must ensure that software code delivered to DN as part of the Services complies and was developed in accordance with Industry Standards and best practices (e.g., OWASP), is free from security vulnerabilities, and, if applicable, does not prohibit DN from obtaining their annual PCI DSS compliance or meeting similar government or regulatory requirements needed to maintain their normal course of business. Supplier agrees to the escrow of all proprietary source code used in performance of the Agreement with a mutually agreeable third party, identifying DN as beneficiary.

9.2 Development Separation. Supplier shall maintain procedures to physically and/or logically separate any application development and production servers and environments. Live data, including direct copies of production Confidential Information, shall not be used in any non-production environment, including development and test systems Development staff must not have access to the production servers and operations staff must not generally have access to the development source.

9.3 PCI. The provisions set forth in this Section apply to Supplier if, either by itself or through a processor or other agent, Supplier stores, processes or transmits Cardholder Data (as defined in the PCI SSC) in any manner, or if, in relation to the Services, Supplier otherwise could impact the security of DN's Cardholder Data environment. Where any of the above conditions apply, Supplier is and shall be in compliance with applicable Payment Card Industry Data Security Standards ("**PCI DSS**") requirements, as set forth in the current version of PCI DSS and any amendments or modifications thereto or new versions made effective in the future. The Parties will agree in writing to any specific requirements necessary for the provision of the Services. To validate such compliance, Supplier will either: (i) undergo a PCI DSS assessment and provide evidence to DN to demonstrate such compliance, or (ii) permit its services and/or environments, as applicable, to be reviewed during the course of any DN PCI DSS assessment.

9.4 **Payment Card Industry Requirements.** In performing the Services, Supplier shall adhere to all Payment Card Industry Standards as applicable to Supplier's provision of the Services. Supplier shall provide to Diebold Nixdorf all documents reasonably requested by Diebold Nixdorf to show compliance, including a "Report of Compliance" from a Qualified Security Assessor. The cost to obtain such "Report of Compliance" shall be borne by the Supplier and in no event shall Diebold Nixdorf be obligated to pay costs in connection with Supplier obtaining such "Report of Compliance".

10 MISCELLANEOUS

10.1 **Subcontractors.** Supplier shall ensure and verify that its agents, suppliers, and subcontractors comply with these Security Requirements and applicable law.

10.2 **Conflict with Law.** Where applicable law prevents compliance with the Security Requirements, Supplier shall notify DN of such applicable laws in order to determine appropriate compensating controls. Where applicable law sets forth more stringent requirements than those set forth in these Security Requirements, Supplier shall comply with applicable law

