COGNEX VENDOR DATA SECURITY REQUIREMENTS

These Vendor Data Security Requirements apply to Seller's provision of Products to Buyer. Capitalized terms used but not otherwise defined herein have the meaning ascribed to them in the Cognex Terms and Conditions of Purchase applicable to the associated Order.

1. **SECURITY PROGRAM**. Seller will maintain a written information security program of policies, procedures and controls aligned to the ISO27001 Series, or substantially equivalent standard, governing the processing, storage, transmission and security of Buyer Data (the "Security Program"). "Buyer Data" means all non-public, confidential or proprietary information of the Buyer and electronic data uploaded by or for Buyer and processed by Seller. The Security Program will include industry-standard practices designed to protect Buyer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Seller will update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that no such update will materially reduce the overall level of commitments or protections provided to Buyer as described herein.

2. **MINIMUM STANDARDS**. At a minimum, Seller's safeguards for the protection of Buyer Data shall include: (i) limiting access to Buyer Data to Seller's employees who have a need to know or access it to enable Seller to perform its obligations under this Order; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting Buyer Data stored on any media; (vii) encrypting Buyer Data when transmitted over public or wireless networks; (viii) strictly segregating Buyer Data from information of Seller or its other customers so that Buyer Data is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Seller's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Seller's employees.

3. **TECHNICAL MEASURES**. Seller will maintain on its platforms and networks the following controls:

    a. Network Perimeter Protection: firewalls designed to screen incoming and outgoing network traffic, and intrusion detection tools designed to monitor for malicious activity. Seller will use processes and technologies that include industry standard antivirus protection, anti-malware protection and software updates, personal firewalls, operating system hardening and updates, power-on passwords, password-protected keyboard or screen locks that automatically trigger through inactivity, and full disk encryption where permitted by law.

    b. Physical Access Controls: appropriate physical security controls that include the use of physical monitoring and intrusion detection systems, implementation of locks and access barriers, and access screening to facilities and equipment used to provide the Products.

    c. Logical Access Controls: appropriate logical access controls that include authentication of claimed identity (using means such as passwords, PINS or tokens), periodic review of user IDs and accounts to verify continued business need, and management of user privileges in accordance with job function. Password rules will follow strict requirements, including a minimum number and type of characters and uniqueness from previous user passwords.

    d. Access Authorization Controls: Seller shall permit only those personnel with a current business need who are authorized with physical and logical access to facilities and systems used to provide the Products. Access is removed upon staff reassignment or termination of employment. Physical and logical access controls will be revalidated at defined time intervals to verify that personnel continue to have a legitimate business need for access.

    e. Security Advisories: Seller will be supported by internally distributed security advisories to appropriate personnel that originate from industry security organizations and equipment, software and systems suppliers. Security advisories will be categorized and assigned a severity rating along with a timeframe within which the Seller will endeavor to remediate the vulnerability, if applicable.

4. **ISO SELF-ASSESSMENT**. Seller will be subject to scheduled self-assessment against the security section of ISO 27001 or a similar standard. Upon Buyer request, Seller will provide documentation summarizing the assessment against Security Best Practices in accordance with ISO 27001.

5. **SECURITY INCIDENT RESPONSE**. Seller will engage in commercially reasonable efforts to monitor and identify security incidents and threats related to the Products. Seller will notify the Buyer without undue delay if it determines that unauthorized access to Buyer non-public data has occurred. Seller will also provide required notices consistent with applicable law.

6. **BUSINESS CONTINUITY**. Seller uses controls and maintains a documented and operational business continuity and disaster recovery program to manage business risk due to disasters and other disruptions to business continuity, such as disaster resilience and recovery and multi-site operations (the "BCP"). The BCP describes the plans for recovering from disaster occurrences, resuming normal business operations, and meeting recovery requirements, including plans for communicating the status of the recovery efforts until resolution. The BCP will be subject to regular testing and evaluation and updated at least annually. Upon request, Seller will supply Buyer with a copy of its BCP.

7. **AUDITS**. Upon request, Seller will supply to Buyer its then-current SOC 2 Type 2 (or its successor) report (SOC 2 – Type 2 report) and selected policies, procedures and evidence approved for distribution to customers. Limited to once every 12 months, and upon request given in writing not less than thirty (30) days in advance, Buyer may initiate an on-site audit at a representative Seller facility involved in the preparation or delivery of the Products, at reasonable times during business hours.