Sterling Information Security Requirements

("Security Requirements")

1. SCOPE

1.1. The standards established in this Security Requirements document are an enhancement of, and incremental to, requirements set forth in any Master Relationship Agreement (MRA), Data Protection Agreement (DPA), Sterling Terms and Conditions (both Commercial and Government versions), Purchase Order, Statement of Work, or other agreement into which these terms may be incorporated.

1.2. If Partner receives, maintains, creates, or transmits individually identifiable health information ("PHI") as a subcontractor for Sterling, the terms of the Business Associate Subcontractor Agreement will apply to and be supplemented by this Security Requirements.

2. DEFINITIONS

2.1. Capitalized terms used but not defined in these requirements will have the same meaning as set forth in the Sterling Computers Terms and Conditions.

2.2. **"Intrusion Detection System"** or **"IDS"** means a device or software application that monitors a network or systems for malicious activity or policy violations. A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of a NIDS.

2.3. **"Intrusion Prevention System"** or **"IPS"** means a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.

2.4. **"Standards"** means the requirements set forth by these requirements.

2.5. **"Security Incident"** means an incident or realized scenario that involves or may involve accidental, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, use, modification, disposal, compromise, or access to any of Sterling Systems, Sterling Data, Partner data or either party's information or intellectual property, or any security incident that has the potential to cause harm to the Sterling brand, Sterling customers, or to any Sterling asset (e.g. people, facility, equipment, etc.)

2.6. **"Sterling Data"** means any and all data provided by Sterling, its customers, authorized agents and/or subcontractors to Partner, or otherwise processed by Partner in connection with the provision of products and services, including but not limited to: (a) all non-public information and data provided to or accessed by Partner through Sterling's network, or provided to or accessed by Partner for hosting or outsourcing services; (b) Technical Data; (c) Sensitive Information; (d) Telemetry Data, and/or (e) user tracking data.

2.7. **"Sterling Intellectual Property"** means any and all intellectual property rights worldwide arising under statutory or common law, including, without limitation, intellectual property which is acquired or obtained under a contract with a third party, and whether or not perfected, comprised of any of the following: (a) copyrights, copyright applications, copyright registrations; (b) mask work rights and mask work registrations; (c) designs, inventions, discoveries and rights arising from or related to all classes or types of patents, utility models and design patents (including, without limitation, originals, divisions, continuations, continuations-in-part, extensions or reissues) issued or issue-able thereon, and

applications for these classes or types of patent rights; (d) any trade secrets and any know-how; (e) any right analogous to those set forth herein in foreign jurisdictions; and (f) any renewals or extensions of the foregoing (as and to the extent applicable) now existing, hereafter filed, issued or acquired.

2.8. **"Sterling Systems"** means any of Sterling's electronic infrastructure, including all computer systems, software, hardware, networks, databases, electronics, platforms, servers, interfaces, applications, websites, devices, products, solutions, and related information technology systems and services, used, accessed by or made accessible to Partner.

2.9. **"Telemetry Data"** means technology asset, device, or system data, often machine to machine, that communicates the operating status of said asset, device, or system, including but not limited to; operating system software version, power and battery health, hard drive efficiency, etc.

3. GENERAL PROTECTION OF STERLING INTELLECTUAL PROPERTY

3.1. Partner shall maintain controls and processes to prevent the unauthorized replication or duplication of Sterling Intellectual Property, sub-assemblies, parts, or materials used manufacturing, and/or finished goods.

3.2. Partner shall maintain controls ensuring that Sterling Intellectual Property, Sterling information or Sterling Data are accessed only on a need-to-know basis.

3.3. Partner shall establish and maintain controls to identify and prevent tampering, theft, or replication of Sterling Data and Sterling Intellectual Property.

3.4. Data Retention: Unless (i) required by applicable law or (ii) otherwise directed by Sterling, Partner's retention of Sterling Data shall not exceed ninety (90) days from the completion of Service.

4. SOURCING SECURITY

4.1. **Component Sourcing**

4.1.1. To the extent that Partner develops electronic components and hardware, Partner shall only procure directly from the original manufacturer or through a distributor authorized by the OEM.

4.1.2. Partner shall maintain controls and processes for guarding against, identifying, and mitigating the use of counterfeit components and or tainted or compromised software/firmware.

4.1.3. Partner shall maintain a documented process for identifying and removing counterfeit or tainted components. Such processes shall include notification to Sterling (contracts@sterling.com) within two (2) business days upon discovery of any counterfeit or suspected counterfeit component that may have gone to Sterling.

4.1.4. Partner shall establish a documented process that ensures a documented purchase history and Process of Record (POR) for all components and hardware, in compliance with Sterling's AML as part of verifying compliance with Sterling GSCM-SBM031 for counterfeit control measures. Partners shall make purchase histories available to Sterling upon request.

4.1.5. Partner must maintain a documented process that provides Sterling with a Bill of Materials (BOM) that specifies all subcomponents contained within Sterling products or software, and that includes traceability for each component back to an Original Component Manufacturer (OCM) or Original Equipment Manufacturer (OEM).

4.1.6. Partner shall maintain processes that manage, monitor, safeguard, and limit access only to authorized personnel for all Sterling products and components within their control.

4.1.7. All inventories must be responsibly managed to reduce risk for Partner, Sterling, and its customers. Therefore, Partner must: (a) maintain controls and processes to safeguard and limit access to authorized personnel on a need to know basis to Sterling Intellectually Property or Sterling Data, sub-assemblies, parts, or materials used in manufacturing goods and/or finished goods; and (b) implement physical security measures to restrict and manage access to high value materials that if stolen, altered or duplicated would compromise the integrity of the finished product, or would cause significant business impact and/or financial impact to Partner and/or Sterling. Partner shall be responsible for evaluating their own materials and components for impact and applying appropriate controls.

4.2. **Partner Software and Firmware Security; Vulnerability Response.**

4.2.1. To the extent Partner develops software, firmware or components with embedded logic, Partner shall follow a documented Secure Development Lifecycle (SDL) based upon industry standards and best practices (e.g., SAFECode, ISO 27034, Microsoft's SDL or similar) and shall: (a) follow a documented Product Security Incident Response Team (PSIRT)/Vulnerability Response Program/Process based upon industry standards and best practices (e.g., FIRST PSIRT Services Framework or similar); (b) have measures in place to continuously monitor external security advisory sources (e.g. cooperative security tests, external security research, open source, and third-party disclosures), and track vulnerabilities that may impact Sterling Data or Sterling products, including third party components; (c) use best effort to ensure that any third parties that provide Partner with software or products have their own security practices and meet the security measures set forth in these Security Requirements; and (d) implement and maintain controls to identify all security vulnerabilities in software during development and after release, and the test such software to ensure it is free of errors as listed in "CWE/SANS Top 25" (http://cwe.mitre.org) and/or "OWASP TOP 10" (http://www.owasp.org) at the time of delivery (e.g. robustness against unexpected inputs such as SQL Injection, predictable behavior in overload situations, etc.) and in subsequent releases.

4.2.2. Partner shall make available, upon request, information that describes Partner's practices for secure software development and assurance. Sterling may further request that Partner self-certify that its development practices align with secure software development and integrity standards developed by industry code security and integrity organizations. Partner must further ensure that its code does not contain spyware, counterfeits, backdoors or other malicious code and Sterling may request that Partner certify the absence thereof and the integrity of its code. If Partner uses Sterling-provided Register Transfer Level (RTL) on Complex Programmable Logic Devices (CPLD) or Field Programmable Gate Arrays (FPGA) it shall have a process to ensure the integrity of the RTL used on such devices.

4.2.3. Partner shall implement and demonstrate upon request, the authenticity and integrity of Partner code provided to Sterling by digitally signing mobile code, distributing verifiable product code from a trusted website, or other method as agreed to by the parties.

4.2.4. Partner shall have a governance structure to provide oversight to its software/firmware security program, including review and signoff on the security posture thereof and shall train developers on secure engineering practices on an ongoing basis consistent with changing practices and the threat landscape.

4.2.5. Partner shall have development/engineering processes that track components throughout the life cycle, that are likely targets of tainting.

4.2.6. Partner shall use up-to-date commercial malware detection tools as part of its code acceptance and development processes prior to delivery, as applicable.

4.2.7. Partner shall remediate all identified vulnerabilities regardless of source of discovery (e.g., Sterling, internal, third-party researcher, open source, Permitted Subcontractor, pen-testing, SDL, etc.) and regardless if code is Partner's or third-party component code.

4.2.8. If Partner receives reports from Sterling of a security vulnerability in Partner's code, Partner shall provide to Sterling: (a) within **five (5) business days** of Sterling reporting the security vulnerability, confirmation of the security vulnerability or a detailed response summarizing its reasonable basis for denying the security vulnerability; and (b) within **ten (10) business days** of confirmation of the security vulnerability, a remediation plan and share information with Sterling, including the applicable CVE, CVSS score and components affected.

4.2.9. For any publicly known or Sterling-reported vulnerabilities with a base score greater than or equal to 4, as defined by Common Vulnerability Scoring System v3 (CVSS), Partner shall promptly remediate and/or provide a temporary fix to Sterling, as applicable, on a timeline commensurate with risk and in accordance with the following timeframes, unless otherwise agreed to by Sterling.

CVSSv3 base score	**Maximum time to provide a temporary fix**	**Maximum time to provide an official fix**
9.0-10.0	Seven (7) calendar days	Earlier of the next available release or within thirty (30) calendar days
7.0-8.9	Not applicable	Earlier of the next available release or within thirty (30) calendar days
4.0-6.9	Not applicable	Ninety (90) calendar days

4.2.10. Partner's use of third-party components shall not alter or reduce Partner's responsibility to identify and remediate vulnerabilities as described herein. Partner shall have a system to be notified of all publicly released third-party vulnerabilities in its software/firmware and components and to evaluate applicability thereof. Partner must also ensure that Open Source & Third-Party Software included in new product releases are recent and still supported.

4.2.11. Upon remediating a security vulnerability in Partner code, Partner shall have a process to communicate the following information to Sterling, as applicable: (a) a description of the security vulnerability, including the potential scope of risk to Sterling products, services, solutions and environments, and the versions of Partner code impacted; (b) the remedy information and location (e.g., patch, maintenance update, or product version upgrade); (c) the Common Vulnerabilities and Exposures (CVE) ID (where applicable); and (d) any other relevant information on workarounds or mitigating options for the security vulnerability.

4.2.12. If there is a known mitigation or workaround for a vulnerability, Partner agrees to notify Sterling of the mitigation as soon as it is known, even if the issue is not publicly known.

4.2.13. To promote coordinated disclosure, Partner shall provide Sterling with **at least ten (10) business days advance** written notice before publicly disclosing a security vulnerability that affects Partner

code. Partner shall coordinate with Sterling (contracts@sterling.com) regarding the content of any such public disclosure. In the case that Partner must make an emergency response to a security vulnerability publicly disclosed by a third party, Partner shall coordinate with Sterling as soon as possible. Partner shall provide Sterling with information, which Sterling reasonably requests, to identify and understand the security vulnerability and validate the remedy.

4.2.14. Partner shall provide Sterling written notice about the impact and remediation plan for any **high-profile** (i.e. publicly-acknowledged vulnerabilities, zero-day exploits, actively exploited issues, high media attention issues, "branded" issues, publicly-known issues with proof of concept, etc.) issue **within five (5) business days** of public acknowledgement. For such high-profile issues, Sterling expects an expedited remediation and may request an expedited remediation timeline, as mutually agreed to by the parties.

4.2.15. If at any time Partner deems that a vulnerability (regardless of CVSS score) poses significant risk to Sterling that cannot be addressed in accordance with Partner's applicable remediation timeframe, Partner shall provide Sterling information about the issue, any known workarounds or mitigations and any options to turn off the related code.

4.2.16. Partner shall limit sharing of non-remediated issues and follow industry coordinated vulnerability disclosure practices.

4.3. **Counterfeit Mitigation.** To the extent Partner develops or provides parts to Sterling or its customers, the following requirements shall be required: Partners must (a) implement and maintain counterfeit mitigation measures that substantially meet the system criteria specified in 48 CFR 252.246-7007 (Contractor Counterfeit Electronic Part Detection and Avoidance System); (b) provide to Sterling, on Sterling's request, information concerning such counterfeit mitigation measures; and (c) address any material deficiencies in such mitigation measures that may be identified by Sterling or by Partner.

5. CYBERSECURITY. This Section identifies the minimum Partner cybersecurity requirements. Partner must also review and comply with applicable Privacy Laws and existing agreements with Sterling, which may require additional security controls.

5.1. **Information Security**

5.1.1. Partner shall implement policies and procedures to provide a data protection policy consistent with the requirements of applicable law and existing agreements with Sterling.

5.1.2. Partner shall identify a person or organization responsible for managing information security risks. Upon request, Partner shall provide the contact information of such individual or organization to Sterling.

5.2. **Network Security**

5.2.1. Partner shall implement policies and procedures to ensure that network systems are well designed and properly configured to ensure that only authorized network traffic is transmitted over networks. These policies and procedures must include: (a) controls to permit passing of only approved types of network traffic and block unapproved traffic; (b) network segmentation and isolation; (c) monitoring to ensure the controls and configurations of network devices comply with these Security Requirements; (d) strict access control to any physical or wireless networks, with access restricted to authorized personnel only; (e) prevention of the deployment of unauthorized wireless networks; and

(f) policies and controls regarding the access of personally owned computing devices to Partner's corporate network and other IT infrastructure.

5.3. **Encryption**

5.3.1. All data transmission supporting business with Sterling shall be encrypted, at a minimum using 256-bit encryption per NIST 800-131Ar2.

5.3.2. Applications, data storage and network devices shall use cryptographic algorithms defined per NIST 800- 131Ar2 or NSA Suite B.

5.3.3. Strong encryption at-rest is required on all mobile devices and removable storage containing Sterling Data.

5.3.4. All wireless networks connected to Partner networks shall implement strong encryption for authentication and transmission.

5.4. **Anti-Malware, Secure Patch and Vulnerability Management**

5.4.1. Partner shall maintain industry standard tools and processes in place to prevent, detect and contain any attacks on, or unauthorized access to, its IT network infrastructure devices and client devices (e.g., desktop/notebook computers). Partner shall review and update its threat identification processes on a yearly basis. Vulnerability remediation efforts shall be tracked, monitored, and verified. Partner shall have a vulnerability reporting program in place for the safe and timely external reporting and internal remediation of vulnerabilities, threats, and exploits.

5.4.2. All devices accessing, processing, or storing data related to Sterling business shall have an active and up- to-date anti-malware solution installed. Web and email traffic processed by Partner infrastructure shall be scanned with anti-malware solutions.

5.4.3. Security patches that affect Partner's infrastructure and applications supporting Sterling shall be deployed as soon as available, and in any case within the recommended timeframe of 30 days for high-risk vulnerabilities and 90 days for medium and low-risk vulnerabilities. Applications and infrastructure storing and/or processing Sterling Data shall be maintained to the latest security patching levels, including minimum version levels. Deployment of patches shall follow a formal change management process. Partner shall maintain all system components in adherence with NIST 800-53 Rev 4 which requires replacement of system components when support for the components are no longer available from the developer, vendor, or manufacturer. Exceptions to patching shall be communicated to Sterling and simultaneously documented with patch testing results, a short-term remediation date and acceptance of risk in writing by Partner official or organization responsible for managing information security risks.

5.4.4. Partner shall maintain a policy and assign staff responsible for monitoring Partner's vendor and industry sites for vulnerability announcements, patch and non-patch remediation and emerging threats, determining the impact of those vulnerabilities on Partner network, and implementing mitigating actions including a minimum of annual penetration test, semi-annual vulnerability scans.

5.4.5. Partner shall maintain one or more of the following executable restrictions in place: (a) Windows Security Settings: Software Restriction Policies; (b) technology in place to prevent unauthorized executables from running; and (c) policies requiring macros to be turned off.

5.4.6. Partner shall maintain email protective measures, which shall include custom filtering, anti-spam, anti-phishing.

5.5. **Penetration Tests and Security Evaluations**

5.5.1. Partner will have an industry recognized independent third-party perform a comprehensive penetration test and security evaluation of all assets used to store, access, or process Sterling Data prior to use and on a recurring basis no greater than every 12 months. The penetration test and security evaluation will include but not be limited to tests to detect vulnerabilities listed in the SANS Critical Security Controls for Effective Cyber Defense or the Open Web Application Security Project ("OWASP") current at the time of the penetration test and security evaluation. Vendor will perform appropriate mitigations to address issues identified. Partner will provide a summary of the most recent penetration test and security evaluation to Sterling upon request.

5.6. **Threat Modeling**

5.6.1. To the extent Partner develops software, Partner shall perform threat modeling and testing (“modeling”) according to the modeling requirements of an agreed-upon standard (such as the STRIDE/DREAD, OCTAVE, etc.). Partner will document modeling findings according to the reporting requirements of the standard. Partner will provide the modeling findings to Sterling.

5.7. **Segregation of Duties**

5.7.1. Where segregation of duties and system access cannot be consistently maintained by an organization or team, Partner shall have a formal governance process in place that will rank the risk of non-adherence. Any segregation of duties exceptions shall be communicated in writing to Sterling.

5.8. **Access Controls**

5.8.1. Access to Sterling Data shall be controlled in accordance with Sterling policies and procedures, Partner policies and standards, applicable law, and all applicable contractual restrictions set forth by Sterling in Partner’s existing agreements with Sterling. Such controls shall protect against any unauthorized access.

5.8.2. Business users shall be granted appropriate access based on their role, following the principles of “least privilege” and “need to know”. Role based access lists (i.e., group profiles) should be used whenever possible.

5.8.3. Access credentials may not be group-based or team-based. Each individual user shall have auditable user account credentials.

5.8.4. All user and administrator accounts hall have an auditable trail of request, approval, creation, modification, recertification, and removals actions.

5.8.5. Access privileges shall be reviewed at least quarterly to determine if access rights remain appropriate for a user’s job duties.

5.8.6. User accounts shall be disabled immediately upon the user’s termination of employment. Access shall be modified immediately as appropriate upon any modification of a user’s employment role.

5.8.7. Memorized secrets and passwords shall meet the guidelines set out in NIST Special Publication 800-63B or, at a minimum, the requirements listed below when they are created, changed, or handled:

(a) passwords shall not be shared between users or accounts; (b) passwords shall be a minimum of 8 characters, or 15 characters for privileged/ administrator accounts; (c) passwords shall contain 3 of the following: uppercase, lowercase, numeric, non-alphanumeric and any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase; (d) passwords shall be changed upon a user's first login, or after any password reset, but only by the account owner; (e) passwords shall be changed at least every 90 days. The number of unique new passwords a user shall select before an old password can be reused is 10; and (f) default passwords shall be changed upon system implementation.

5.8.8. In addition to a valid user ID, users accessing Partner applications outside of Partner's network require a second form of authentication to log in to his/her account (e.g. a Two-Factor Authentication (2FA) token).

5.8.9. If Partner allows employees or third parties to access its network remotely, then (a) Partner shall have policies and controls in place to secure such access and (b) network traffic between the remote client and Partner's network shall be encrypted.

5.8.10. Removable Storage Devices: The use of personally owned storage devices shall be prohibited. Removal storage devices include: thumb drives; writable CD/DVD media; USB/Firewire hard drives; network-attached storage (NAS) devices or similar; or any other removal storage devices.

5.9. **Logging and Alerting Controls**

5.9.1. Partner shall record and retain access and system logs from infrastructure host and server operating systems, network perimeter access control systems, data bases and critical applications for a minimum of ninety (90) days.

5.9.2. Logs shall provide enough details to assist in the identification of the source of an issue and enable a sequence of events to be recreated. Logs shall record the date, time, and source location (e.g., Internet Protocol address/hostname) for all network access attempts. Logs shall capture system and network security event information, alerts, failures, events, and errors.

5.9.3. Logs shall be stored in a central location to preserve the integrity and security of the logs. Integrity of log files shall be maintained and protected from tampering by restricting access to systems that store log information.

5.9.4. Monitoring requirements shall be considered during the implementation of new IT resources and should be designed to reflect the classification of the asset and the criticality of the services it provides.

5.9.5. Partner shall have an Intrusion Prevention System (IPS) and/or an Intrusion Detection System (IDS) in place. Partner shall retain evidence that the IDS/IPS is actively managed. IDS/IPS software shall be updated to most recent patch level. IDS/IPS signatures shall be updated to the most recent version. IDS/IPS custom signatures shall be implemented by Partner. Partner shall have automated IDS incident notification procedure.

5.10. **Incident Management and Reporting**

5.10.1. Partner shall maintain an incident response policy and procedures compliant with applicable law. The incident response policy and procedure should be reviewed on an annual basis to ensure the appropriate roles and teams are up to date.

5.10.2. Partner shall inform Sterling of any Security Incidents impacting or related to Sterling or its customers. Incidents shall be reported to Sterling (contracts@sterling.com) within twenty-four (24) hours for confirmed incidents or seventy-two (72) hours for reasonably suspected incidents. Incidents include, but are not limited to, the following: Virus/Malware/Ransomware infection; Verified phishing/scam; A breach of Sterling information, Sterling Intellectual Property, and/or Sterling Data; Deliberate attempted password misuse; Suspicious/Inappropriate Handling of Sterling Data; Suspected server/workstation compromise; Denial of service; and Malicious internal or external intrusion attempts.

5.10.3. Logs shall be maintained for all confirmed or reasonably suspected Security Incidents in compliance with applicable laws and shall be made available to Sterling upon request.

6. PHYSICAL SECURITY

6.1. **Protection of Assets.** To the extent Partner is providing break/fix, depot and/or warehousing and logistics services to Sterling or its customers, Partner shall comply with the following requirements:

6.1.1. Subject to applicable law, all Partner facility structures must be constructed to prevent unauthorized access to such facilities. Facilities must be constructed of materials which resist unlawful entry and protect against outside intrusion.

6.1.2. Partner facility structures and fencing must be inspected for integrity and damage at least monthly.

6.1.3. At the minimum the inspection should include, but is not limited to, a review of the following characteristics where gates and/or fencing is used: (a) driver and man gates; (b) holes or wear in any fence lines; (c) erosion or tunneling below all fences; (d) trees and shrubs on and near the facility's property to ensure they are positioned at least thirty (30) feet away from the fence line and sufficiently trimmed not to extend over a fence; (e) integrity of top/razor wire if used; and (f) any other signs that the fence could be compromised.

6.1.4. If a third party (such as a guard service) is responsible for conducting reviews of perimeter structures, they must report any findings to authorized facility personnel to allow the facility to sufficiently scope and perform any requisite repairs.

6.1.5. Audits, inspections, and corresponding remediation activity should be kept on file for two (2) years.

6.1.6. Locking mechanisms on external and internal doors, windows, gates, and fences at Partner facilities must be in place to resist unlawful entry and to protect against outside intrusion.

6.1.7. Lighting levels inside and outside of all Partner facilities, including inside and outside of all parking areas, exit/entry areas, trash and recycling areas, perimeter fencing areas and gates, must be sufficient to enable personnel to identify and provide descriptions of individuals present in the area and must support the recording of video surveillance images in those areas where Closed Circuit Television (CCTV) is deployed.

6.1.8. An internal/external communications system with redundancy/back-up (cell back-up is acceptable) must be in place for contacting Partner security personnel or local law enforcement when necessary.

6.1.9. All access points at Partner facilities, including all personnel exit/entry doors, dock doors, fire exits, vents, air handling units, and windows must be of enough strength or design to prevent or delay forced entry. Access points must not have any gaps where physical assets could pass. Subject to applicable law and local fire safety codes, access points must meet the following requirements: (a) door hinges on external access points must either be pinned internally or spot-welded if hinges are external and external hardware such as knobs and handles should be removed on doors not designated as entry points; (b) all external overhead, man, dock, and warehouse doors must be closed and locked except when required to be open for normal transit operations and must be visible via CCTV or by security personnel; and (c) in the event of power failure, electrically controlled access doors must remain locked with emergency egress provided from inside the locked area.

6.1.10. Partner must conduct, at least weekly, random trash inspections that may include, but are not limited to, use of metal detectors or inspection by physical inspection before any such trash is removed from manufacturing, warehouse, and dock areas, or where Sterling Intellectual Property (IP) may be present.

6.1.11. Each trash inspection must be documented, which such documentation must include the date, time and person conducting inspection. Documentation should be kept for two (2) years.

6.1.12. Partner shall be certified to or compliant with all Transported Asset Protection Association (TAPA) Level A Facility Security Requirements.

6.1.13. Partner shall comply with TAPA's "Option 1: Physical Barriers in Place" for perimeter security for production facilities whenever practicable over TAPA's "Option 2: No Physical Barriers in Place".

6.1.14. Partner shall notify Sterling (Security@sterling.com) immediately in the event of a theft or unauthorized physical intrusion at facilities involved with the production of Sterling products.

6.2. **Cargo Security.** To the extent Partner is providing depot and/or warehousing and logistics services to Sterling or its customers, Partner shall comply with the following requirements:

6.2.1. Local Partner site management must be responsible for the safeguarding of all Sterling products, assets and/or Sterling IP under its control by implementing appropriate policies and procedures.

6.2.2. Only approved and authorized individuals shall be granted access to shipping areas, loading docks, cargo staging or holding areas, trailers and any shipping containers that can or will be used to transport Sterling products, assets and/or Sterling IP.

6.2.3. Employee, guest, or other passenger vehicles must be prohibited from parking in or adjacent to all cargo handling and storage areas.

6.2.4. All truck drivers are required to enter the facility through designated and approved gates manned by security officers or under video surveillance, in accordance with the requirements outlined in Section 5.5 "Closed Circuit Television (CCTV) and Security Systems" at sites with fenced shipping/receiving areas or truck yards.

6.2.5. Drivers must not be accompanied by any unauthorized passengers at any point during the receiving, transporting, and delivering of Sterling products unless previously declared and specified in writing prior to the scheduled pick up or delivery appointment time.

6.2.6. CCTV must be installed to allow for drivers to be instructed to face the applicable camera in order to record the image while presenting approved identification. Hats, bandanas, scarves or other clothing which might obscure the video capture and/or the driver's identification must be removed.

6.2.7. All truck drivers must always be accompanied or overseen by an authorized facility representative or security personnel while in receiving/shipping areas where Sterling products, assets and/or Sterling Intellectual Property are present.

6.2.8. When not in shipping/receiving areas, drivers must remain in their trucks or be confined to a designated staging area. Subject to applicable law, drivers must supply verified identification to Partner personnel or authorized third party personnel (such as a guard service) prior to gaining access to shipping and receiving areas where Sterling Intellectual Property and/or Sterling product is present.

6.2.8.1. At the minimum, the following information must be captured on a driver's log and retained for a minimum of two (2) years: Pre-alert and authorization to pick up Sterling product when pick up is the purpose for facility access; driver's corporate-issued identification card/badge; confirmation of examination of driver's personal identification (in addition to corporate- issued credential), including confirmation of validity (i.e. such identification is not expired); driver's name; driver's license number; vehicle license plate number and trailer license plate number (if the tractor and trailer are separate units); tractor/vehicle unit identification number, and trailer unit identification number (if the tractor and trailer are separate units); seal serial number (when applicable); and, date and time of pick-up.

6.2.8.2. When utilizing seals, bolts or external serialized locking devices, the following controls must be used: (a) controlling, affixing, replacing, recording, tracking, and verifying seals (when used) from the point of loading containers, trucks, and trailers; (b) prior to use, seals must be securely stored in sequence, with access control limited to authorized personnel; (c) inventory and documentation of seals must be conducted monthly; (d) any variation in the sequence of seals must be reported and investigated and any adjustments should be documented by management and must explain the reasoning behind any such discrepancy; and (e) seal inventory, when required, must be maintained for two (2) years and available for review by Sterling upon request.

6.2.8.3. Only authorized employees shall be allowed to distribute material to and from trucks, trailers, and containers. Properly certified lift and dock operators must be assigned to assist in distributing such materials.

6.2.9. Container seals and T-bars: A high-security seal must be affixed to all containers crossing international borders as well as for any other shipments designated by Sterling. All seals on containers, trucks and trailers must meet or exceed the current PAS ISO 17712 or current version standards for high security seals. Sealing of the vehicle by warehouse personnel must be witnessed by the driver and must be documented. Documentation must be retained for two (2) years and available for review by Sterling upon request. When receiving inbound goods, the seal integrity must

be physically inspected for tampering or counterfeiting, and the seal number must be verified against the original shipping documents and must be confirmed to match the original seal number. Partner shall establish and maintain procedures to recognize and report any compromised seals (when used) to the appropriate governmental customs authority. Truck seals may only be opened/broken by authorized personnel at the destination, which must be witnessed and documented by the driver. Partner shall ensure that procedures to collect and securely dispose of all seals immediately after use are in place.

6.2.10. Partner shall ensure that first break procedures are in place to sufficiently record, report, and investigate any shortages or overages of Sterling product or cargo upon discovery by Partners. First break defines the moment when a package or parcel is first opened on-site.

6.2.11. Partner shall ensure that procedures to digitally track the movement of all incoming and outgoing goods via an inventory control or warehouse management system are in place.

6.2.12. Partner shall ensure that procedures to maintain the accuracy of all information recorded in the shipping/receiving of cargo, including shipper and consignee name and address, first and second notify parties information, and the description, weight, quantity, and units of measure of all cargo recorded (e.g., boxes, cartons, pallets) are in place.

6.2.13. Partner shall ensure that all information provided and used in the shipping/receiving of cargo is legible and protected against the exchange, loss, or introduction of erroneous information.

6.2.14. Partner shall ensure that all transport documents contain the required dates, times, and signatures necessary to confirm such information.

6.2.15. Partner shall have procedures in place to ensure that manifests are accurate, complete, legible, and submitted in a timely manner to customs authorities.

6.2.16. Shipping documentation shall be attached to packaging in a manner that displays the minimum information required for processing and customs handling and shipping documentation must not reveal more information about the contents of the package to package handlers than is necessary.

6.2.17. For long-haul shipments containing Sterling product and/or Sterling Intellectual Property, the driver must provide his/her signature in the driver log acknowledging he/she is fully fueled, fed, and allowed to drive for at least 200mi/300km from origin where the load was picked up.

6.2.18. Partner shall ensure that trucks, trailers, and containers (empty or loaded, and regardless of use in direct support of Sterling business or not) are stored in a secure area in a manner which prevents unauthorized access and/or tampering.

6.2.19. Partner shall ensure that procedures are in place for reporting and preventing unauthorized entry to trucks, trailers, and containers, as well as areas where such equipment is stored (regardless of use in direct support of Sterling business or not).

6.2.20. There should be a segregation of duties and controls between the ordering of the goods (e.g. purchase duties), receipt of the goods (e.g. warehouse duties), the entering of the goods in the system (e.g. administration duties) and the payment of the invoice. The same party or individual should not be responsible for ordering, managing, and paying for goods.

6.2.21. All information involving cargo loading, cargo routing, cargo contents and shipment destination points should be restricted to authorized staff who require such information to perform their roles.

6.2.22. An approved staff list should be provided upon request, which shall identify which staff members require access to details concerning the flow of goods, cargo routing and shipment destinations as part of performing their roles.

6.2.23. Training must be provided, at a minimum annually, to staff in maintaining cargo security, including to employees in the shipping and receiving areas.

6.3. **Loading, Moving, and Receipt of Goods**

6.3.1. Partner shall support the goal of ensuring the secure management and protection of Sterling products, assets and/or Sterling Intellectual Property through effective loading, conveyance and receiving processes as set forth herein.

6.3.2. Appointed and authorized lead personnel must oversee the introduction and removal of cargo.

6.3.3. Partner shall have procedures in place to avoid leaving any cargo unsupervised, particularly product staged for longer than one (1) hour or during times of facility closure, staff shift change or down time.

6.3.4. Appointed and dedicated staff must be responsible for receiving the driver and the goods at arrival.

6.3.5. Partner shall ensure that that documented procedures to prevent the simultaneous loading and unloading of Sterling products onto the same truck, trailer, or container are in place. Partner shall endeavor to ensure that the receiving and shipping areas are segregated physically or by time to prevent co-mingling of any products.

6.3.6. Partner shall ensure that documented procedures for checking and documenting incoming and outgoing transport. Records shall be retained for five (5) years and shall include: (a) registration of the transport documents and customs papers accompanying goods. (b) comparison of the goods with the accompanying transport documents and customs papers, with documentation of any variance; and (c) notifications to the inventory control, sales, and finance functions upon completion of successful order departure.

6.3.7. An inventory system must be in place and must register goods received or picked up from stock immediately after arriving or after departure.

6.3.8. Goods received shall be assigned a put-away location and transferred to their inventory location as soon as feasible or per the terms of their operative procedure.

6.3.9. Sterling products must be properly marked, weighed, counted, labeled, and documented. At minimum, Sterling products must be marked legibly and must include indelible identification of the contents and the Sterling products' country of origin, in a location on the packaging that is easy to find and that can be read without strain.

6.3.10. Cargo weight, carton count, seal numbers, and documentation must be verified against manifest documents and any discrepancies must be recorded.

6.3.11. Products must be reviewed for damage prior to loading for departure and authorized personnel must ensure the integrity and packaging of the Sterling products are intact as part of the inspection,

including by reviewing for damaged, crushed, cut, or open boxes, as well as by reviewing the integrity of all security packing tape as applicable.

6.3.12. When pallet or package tampering is evident, an incoming goods inspection by the receiving team must be carried out while the driver is still on Partner's premise and must be reported to the shipping party and Sterling (contracts@sterling.com) within forty-eight (48) hours. Any damage or short shipments must be noted on shipping documentation and reported to the shipping party.

6.3.13. Trucks, trailers or containers containing Sterling products or assets that are approved for pre-loading or are at transfer or arrival points that are not immediately unloaded must be locked and monitored by security representatives or must remain under live monitored CCTV, in accordance with the requirements outlined in Section 5.5 "Closed Circuit Television (CCTV) and Security Systems".

6.3.14. Full and partial pallets, as well as single-shipped master/gaylord cartons, must have parcels counted and pallet and/or carton weighed. Count and weight must be documented in shipping paperwork.

6.4. **Access Control**

6.4.1. **Physical Access Control**

6.4.1.1. High Value Areas: High Value Areas are defined as sensitive areas housing information systems (production or development) that access, store, process or transport Sterling business information or Sterling customer business information. These areas include, but are not limited to, data centers, labs, telecommunications rooms, Main Distribution Frames (MDF), Intermediary Distribution Frames (IDF), Network Video Recording Rooms (NVR), tape and backup rooms and any other computer rooms or spaces which transmit or store secure files and Sterling Intellectual Property.

6.4.1.1.1. Each area defined as such shall be protected by an appropriate access control to ensure that only authorized personnel are allowed access. The access control shall log activity in/out of the area, and visitors shall be documented on a visitor log capturing: the name, company, time, date, and escorting personnel. Violations shall be documented and reported immediately.

6.4.1.1.2. Apart from pre-approved official reviews, incident responses, repairs, development activities in Labs or work conducted in conjunction with the, personnel shall not enter secure areas regardless of whether such personnel possess standing access to such areas.

6.4.1.1.3. Access lists for High Value Areas shall be posted, reviewed, and amended monthly to ensure only appropriate personnel retain access to such areas.

6.4.1.2. Secure Perimeter: High Value Areas shall be controlled by a secure perimeter. A secure perimeter provides an additional validation of access via barriers (e.g. a wall), a card-controlled entry gate/door, a manned reception desk, or any other physical, electronic, or virtual control point. The positioning, strength, type, and design of such barriers should be commensurate with the TAPA Level A Facility Security Requirement standard. As per the above, access lists and violations should be identified and reported.

6.4.1.3. Partner shall prohibit unauthorized photography and video recording in manufacturing areas.

6.4.1.4. Partner shall ensure that policies are in place (i) prohibiting personal devices, including notebooks, tablets, and other recording devices, from entering manufacturing area and (ii) preventing cellular phones from being used as recording devices, including deactivation/inspection of applicable cameras/storage.

6.4.2. **Physical Access**

6.4.2.1. Subject to applicable law, all necessary and reasonable means shall be employed to ensure unauthorized persons do not gain access to facilities where Sterling Data and/or Sterling Intellectual Property are stored, managed and/or used.

6.4.2.2. Partner shall keep written site security plans, which shall be made available for review by Sterling upon request. The site security plans should include the physical security profile, policies and standards utilized to define access control to such facilities. Partner shall implement, as a minimum obligation, the additional facility access procedures set forth below.

6.4.2.3. Employee photo or serialized identification badges and visitor badges shall always be issued and visibly worn by all employees, regardless of rank or position.

6.4.2.4. Site access security procedures shall include a documented process for challenging and addressing access attempts by unauthorized or unidentified persons.

6.4.2.5. Access/egress to the facility shall be allowed only through defined and monitored entry/exit points.

6.4.2.6. "**Personal Containers**" include, but are not limited to, lunch boxes, backpacks, coolers, and purses. Personal Container handling shall be controlled within the facility, and shall include the following control procedures:

6.4.2.6.1. Subject to applicable law, Partner shall have a documented procedure for exit searches of Personal Containers during shift changes, breaks or other times when employees are leaving/entering production areas or other sensitive areas; and,

6.4.2.6.2. At the minimum, the procedure shall address the "right to search" criteria, should a need arise to introduce searches when they are normally not required (e.g. when workforce pilferage is suspected).

6.4.2.7. Physical access privileges shall be updated when individuals depart the organization, and at the minimum access logs should be reviewed at least quarterly, or immediately when a supervisor/manager leaves the organization, or immediately when a change to a role occurs where former access privileges are no longer required.

6.4.2.7.1. Procedures shall be in place to remove facility access and Partner-issued employee identification when an employee departs Partner's organization or is terminated.

6.4.2.8. Where card access systems are used: (i) access reports shall be reviewed at a minimum of every quarter for violations; (ii) card access system transactions shall be retained for a minimum of five (5) years, in either electronic or hard-copy format; and, (iii) access to card access system functions shall be restricted to dedicated and authorized personnel only.

6.4.2.8.1. The access control system shall prohibit the sharing of access devices and/or access codes and shall prohibit the process of "tailgating", whereby otherwise authorized employees or personnel are followed into a facility by another person or persons not so authorized.

6.4.2.8.2. If a third-party security firm is contracted to provide on-site or remote security monitoring, such firm: (i) shall be actively licensed when so required by applicable law; (ii) shall have no business affiliation with any firm providing temporary staff to the site; and, (iii) shall adhere to the same background and on-boarding requirements set forth for local employees.

6.4.2.8.2.1. Partner shall have procedures in place to protect Sterling Intellectual Property from unauthorized viewing and/or access when exceptions are made. This includes providing the requisite level of protection of Sterling Intellectual Property in any Partner Labs that shall be shared with other customers.

6.4.2.8.2.2. Sterling Data or physical area should not be shared with competitors, physical area should be limited through badge access.

6.4.2.8.2.3. Clean desk audit should be performed, and log of audits shared with Sterling.

6.4.2.8.2.4. Lab should have at least the same network defense as Partner's corporate network.

6.4.2.8.2.5. Lab entry/exit and activity logs should be made available to Sterling during audit sessions.

6.4.3. **Visitor Access Control**. The following shall be adhered to when allowing external visitors, contractors, guests, inspectors, and delivery people to all facilities where Sterling products, assets and/or Sterling Data are present:

6.4.3.1. Subject to applicable law, visitors shall provide government-issued photo identification prior to being granted access to the areas in the facility where Sterling products, assets and/or Sterling Intellectual Property are present. No special accommodations will be made for visitors, regardless of affiliation or status;

6.4.3.2. Visitor log requirements: the site shall maintain a written visitor log or electronic visitor management system, which shall include the visitor's or delivery person's name, company, date of visit, time of visit, and purpose of visit. These visitor logs shall be maintained for a minimum of two (2) years;

6.4.3.3. Visitors shall always be issued a guest badge or credential to be worn throughout the duration of the visit on Partner's premises and the credential should always remain visible; and,

6.4.3.4. Visitors and vendors shall be accompanied by an authorized employee and/or the Sterling account manager when permitted in any area of the facility (including secure internal locations) where Sterling products, assets and/or Sterling Intellectual Property is stored or used. No special accommodations will be made for visitors, regardless of affiliation or status.

6.5. **Control and Threat Monitoring**

6.5.1. Security Monitoring, Alarms, and Intrusion Detection

6.5.1.1. Intrusion detection systems, e.g. door contacts, infrared, motion, sound, or vibration detection (IDS) shall include the monitoring of alarm events 24x7x365 via an approved internal or 3rd party external monitoring center, which shall be protected from unauthorized access.

6.5.1.1.1. Monitoring centers may be located on or off site, and can be company-owned, or third party.

6.5.1.1.2. If the monitoring center is on-site, then a contingency plan shall be in place to cut over operations in the event of a local failure or crisis.

6.5.2. A documented procedure shall be in place to ensure access to security systems is restricted to authorized individuals or system administrators. Security systems shall include servers, consoles, controllers, panels, networks, and security data.

6.5.3. Security systems housing alarm panels, controllers/wiring, camera systems, and badge readers should be secured in accordance with section 5.3.1a “High Value Areas.”

6.5.4. Any operational, production, or emergency system activated during non-operational hours shall be linked to the main alarm system.

6.5.5. Alarm notification shall be transmitted on power failure/loss, or in instances where uninterrupted power supply (UPS) or generators cut overpower.

6.5.6. For systems with UPS, an alarm shall be transmitted when the UPS battery fails.

6.5.7. Alarm arming guidelines and verification:

6.5.7.1. Partner shall have documented procedures for validating that alarms are armed during non-operational hours and for audit opening/closing reports;

6.5.7.2. Alarm contacts, motions, photoelectric beams, or other security mechanisms shall not be overridden to set the alarm;

6.5.7.3. If viable, alarm systems should be partitioned to allow segregated monitoring of high value or only partially used spaces;

6.5.7.4. Alarm call tree and response should be reviewed monthly for accuracy; and,

6.5.7.5. All alarm points should be tested monthly to ensure functionality.

6.5.8. Alarm notification shall be transmitted in the event of a line failure.

6.5.9. Redundant communication system shall be in place on device and/or line failure, to include cell/ethernet/radio or alternate communication device.

6.5.10. IDS is required to monitor internal production spaces. The IDS alarms shall be activated and linked to the main alarm system during non-operational hours (i.e. when production facility is closed).

6.5.11. Door magnetic contacts shall be installed on all doors entering the shipping, receiving and warehouse areas.

6.5.12. Emergency exits shall be alarmed 24/7 and have local alarm sounders installed to alert employees that an emergency exit has been opened. Sounders shall be activated continuously until reset at the facility's main keypad.

6.5.13. A panic/duress button shall be installed at a centralized location in the shipping and receiving area that will allow employees to activate and annunciate a silent alarm to a central monitoring center, should they come under duress. Portable devices are acceptable if wired devices are unavailable or cannot be installed.

6.5.14. Alarm systems shall include all points of entry as well as the ability to detect unauthorized access within sensitive areas (e.g. High Value Areas, production areas, etc.).

6.5.15. Alarm notification shall be redundant, meaning, where land phone lines are the primary means of notification to security or law enforcement, a backup method of communication shall be provided.

6.5.16. All facility external doors shall be alarmed and linked to the main security system with an audible alarm buzzer that will sound locally when door is open and shall trigger alarm notification in the case of a 24/7 accessible employee door.

6.5.17. All security system alarms shall be responded to in real-time, 24/7.

6.5.18. Partner's monitoring center shall acknowledge any alarm-activations and shall follow pre-defined response protocols.

6.5.19. All responses to system alarms shall be documented and retained for five (5) years.

6.5.20. The facility shall have a functioning alarm system which is armed any time the facility is left unattended, including during non-business hours.

6.6. **Closed Circuit Television (CCTV) and Security Systems**

6.6.1. Partner shall support Sterling's goal of ensuring the secure management and protection of Sterling products, assets and/or Sterling Intellectual Property through the effective use of CCTV, access control system (ACS) and IDS.

6.6.2. Partner shall have CCTV systems arrayed to view critical areas of the facility as identified by the site's annual risk assessment. These areas should include, but are not limited to: (a) all vehicle and pedestrian entrances/exits; (b) server rooms; (c) interior/exterior views of shipping and receiving docks; (d) building perimeter; (e) internal locations where Sterling product is stored; (f) workstations where Sterling Intellectual Property or Sterling Data is being handled or used in work processes; and, (g) parking lots.

6.6.3. All CCTV cameras should be in a protective housing or dome. The cameras must also be connected to a digital video recorder (DVR) or network video recorder (NVR) that allows for a minimum of ninety (90) days retention. In addition, the DVR/NVR should have remote viewing capability, CD-RW capability and UPS.

6.6.4. Each camera must have a specific task and purpose and must have a specifically defined and unobstructed field of view. The task and purpose must be documented for each camera and noted in the specific site security plan for each facility.

6.6.5. Partner shall have written protocols for CCTV systems to ensure continuous operation and maintenance.

6.6.6. Subject to applicable law, Partner must make CCTV images/video available to Sterling upon request.

6.6.7. CCTV, ACS and IDS equipment must be housed in a secure internal location.

6.6.8. CCTV images must be stored in a secure internal location for at least ninety (90) days.

6.6.9. CCTV must be digital to provide enough quality and resolution to identify and provide descriptions of individuals and to provide an electronic audit trail.

6.6.10. Partner must maintain documentation of maintenance and test activity of all CCTV equipment for up to five (5) years.

6.6.11. An accurate time and date stamp must be included on all CCTV recorded video images.

6.6.12. Systems must be checked in adverse conditions, and contingency plans made for when the systems do not work. Security must be alerted if the system becomes dysfunctional for any reason, including inclement weather, and should have a plan in place to provide coverage until the system is back in operational order.

6.6.13. Cameras must be checked daily to ensure they have the proper field of view and that the resolution is acceptable to provide an electronic audit trail. The required level of camera resolution will be “Identification”. “Identification” level is defined as the ability to determine the identity of a human intruder.

6.6.14. Cameras must be positioned to view the site, building and critical area entry points. Cameras must be installed: inside the protected area, at a height enough to prevent tampering. For new camera installations, twenty-five (25) feet of additional cabling must be available for each new camera to allow for relocation.

6.6.15. Enough lighting must be maintained to ensure the effective and efficient operation of all cameras during nighttime hours.

6.6.16. Cameras should be tested daily to ensure cameras are recording, and a minimum of ninety (90) days recorded video for each camera is on the DVR/NVR. Camera test results should be documented, and such documentation must be maintained for five (5) years. Stationary cameras should have control test photographs for security to review to validate cameras are capturing the correct view. Procedures must be in place to mitigate CCTV downtime.

6.6.17. TV systems must operate within Partner network and meet Partner cybersecurity control.

7. SECURITY MANAGEMENT SYSTEMS

7.1. **Critical Security Systems and Processes**

7.1.1. Partner shall implement and maintain a comprehensive security program with defined roles and responsibilities that identify and implement security requirements which protect the confidentiality, integrity and availability of Partner and Sterling Data and Intellectual Property. The security program shall include processes and allocated responsibility to ensure security risks are identified and mitigated, and a formal risk assessment is conducted at least annually. The program shall ensure that

Partner conducts audits and assessments to ensure that security requirements are being maintained and managed, and that any identified nonconformities are remediated in a timely manner.

7.1.2. Partner shall have a documented risk management program which evaluates organizational and administrative risks and performs ongoing risk identification, prioritization, and mitigation efforts quarterly.

7.1.3. Partner shall have an information security policy that is communicated to employees, contractors and vendors and approved annually and is aligned with industry standard leading practices (e.g. ISO 27001). This documentation shall include current emergency Sterling and local management contacts to be contacted in case of Security Incidents.

7.1.4. Partner shall have a cloud security policy in place that ensures that the use of cloud services is managed so as to ensure the protection of all Sterling Data and Intellectual Property. The policy shall at a minimum include the following:

7.1.4.1. Partner shall encrypt all information and/or data by using current industry-standard strong encryption, key management, and related standards (NIST 800-53 Rev 4), when processing, transmitting and/or storing Sterling Data in any private cloud environments;

7.1.4.2. Only Partner-managed or Sterling-managed IT infrastructure should be used to store, manage or share Sterling Data, or Sterling Intellectual Property; and,

7.1.4.3. Partner shall assure that subcontractors providing cloud services adhere to the most recently published version of ISO/IEC 27001.

7.1.5. Partner shall maintain a secure backup of any critical Sterling Intellectual Property or sensitive data for purposes of business continuity.

7.1.5.1. Access to backups should be limited to a small group of users which is monitored and reviewed monthly.

7.1.5.2. Partner shall prevent the unauthorized disclosure of computer files containing product keys when operating computer backup equipment.

7.1.5.3. Security systems and tools, including, but not limited to, security access control systems and CCTV, shall have functioning failover and backup capability such that required records, images and video, and data are not lost by Partner.

7.1.6. Partner shall maintain secure file & data deletion policies (NIST SP 800-88) that ensure that computer files and/or other media devices containing Sterling Data are deleted from computer systems in a secure manner once they are no longer required for the performance of Sterling's business matters.

7.1.7. Partner shall maintain an internal security policy document that addresses the following areas at site specific level:

7.1.7.1. Security policies for Partner site and facility access security;

7.1.7.2. Security policies for the management and control of Sterling Intellectual Property; and

7.1.7.3. Security policies for Partner's information systems and network security.

7.2. **Personnel Security**

7.2.1. Subject to applicable law, Partner shall perform employment background checks on all employees who will have direct or remote contact with Sterling Intellectual Property and/or sensitive Sterling Data, including the personal information of Sterling customers.

7.2.2. Partner shall also ensure the above-mentioned employees take all relevant security-related training, including but not limited to those listed below.

7.3. **Security Training**

7.3.1. Training for the topics identified in this section shall occur at least annually, or more frequently as specific items change (such as new lines of business, equipment or process changes, disclosure changes, or other changes that may impact how security is implemented at the site).

7.3.2. Partner shall document all training it conducts in accordance with this Security Requirements, including the content provided, the dates conducted, and the personnel trained. Partner shall retain such documentation for a minimum of two (2) years.

7.3.3. Information Security Training: All Partner employees who will have direct or remote contact with Sterling Intellectual Property and/or Sterling Data shall receive privacy, data protection and information security training at least annually. Training shall address the following: (a) information security threats and best practices; (b) information security and data privacy policies, procedures, and controls in place to protect Sterling Data; and, (c) each representative's roles and responsibilities in the protection of Sterling Data.

7.3.4. Partner Security Training: All Partner employees who have access to or manage Sterling products, assets and/or Sterling Intellectual Property, as well as those with access to and/or knowledge of supply chain cargo routing of Sterling products and/or assets, must be trained on the relevant Sterling supply chain security policies and requirements contained within this Security Requirements which pertain to the function(s) they perform involving Sterling products, assets and/or Sterling Intellectual Property. Training must be provided to: (a) authorized Partner personnel; (b) hiring managers; and (c) subcontracted staff.

7.3.5. Security Threat Program: A threat awareness program shall be established and maintained to recognize and foster an awareness of the threat posed by terrorists, contraband smugglers, internal bad actors, and malicious nation state actors or unaffiliated individual actors at each point in the supply chain. As warranted by such risk, this training program shall include briefings and/or other distributed information illustrating smuggling trends, seizures, and information on terrorist threats along routes or areas within the extended supply chain for Sterling products.

7.3.6. Security Threat Training: Partner shall provide annual security threat training to its employees, which such training shall address security awareness and security policy training to employees covering information on: (a) how to recognize internal conspiracies; (b) how to recognize internal theft, malfeasance and misappropriation of Sterling Intellectual Property and other types of insider threats; (c) how to determine and address unauthorized access to facilities, Sterling Data and/or Sterling Intellectual Property; and (d) how to maintain cargo security for Sterling products and assets.

7.3.7. Incident Response Training: All Partner personnel with access to Sterling Data, including those with indirect access by means of administrative privilege, shall receive annual training on the Standards, as well as on information security principles that, at a minimum, review the following: (a) incident response processes, including when to implement such processes, and any related and required actions that shall be taken in relation thereto; (b) simulated events and automated mechanisms to facilitate effective response by personnel in crisis situations; and, (c) methods that prevent various Security Incidents, such as identifying and understanding the risks of downloading malicious software. Partners shall provide and communicate a means for all Partner personnel to anonymously report illegal or suspicious activity relating to any Sterling Data and/or Sterling Intellectual Property.

7.3.8. Access Control Training: Access to event logs is considered a form of administrator access or privileged access. Users with that level of access shall be trained in procedures specific to that access.

7.3.9. Physical Security Training: Partner shall have documented policies in place to update and train security personnel at least annually on the following procedures: (a) entry/exit security procedures for all personnel, including permanent employees, temporary employees, and Partners; (b) documented training Riders to test for physical security breaches and corrective actions implemented based on key learnings; and (c) documented response protocol for Partner's security and alarm company, in the case of emergency. This shall include, but is not limited to, the following: (i) specific response protocol for contacting police and/or authorized Partner staff, including maintenance of an up-to-date telephone contact list with adequate back-up numbers; and, (ii) responders on the telephone list shall have a protocol in place that specifies when and how they should respond to being called, including reporting to the site personally, requesting police response at the site and/or contacting local security.

8. AUDITS & COMPLIANCE

8.1. Partner shall establish assessment and accountability mechanisms to monitor compliance with and performance against the Standards set forth herein and shall report the state of compliance with this Security Requirements to Sterling at least annually or upon request by Sterling.

8.2. Sterling shall have the right to audit Partner's compliance with this Security Requirements upon 30 days' notice of any such audit; provided, however, in the event of a material breach of this Security Requirements or upon the request of a regulatory entity, Sterling shall have the right to audit Partner upon 7 days' notice prior to such audit. Partner shall make available all necessary personnel, systems, and resources to effectively audit compliance with Security Requirements.

8.3. Partner shall provide Sterling with written remediation plans, including specific action and target timescales for any non-compliance identified against the requirements in this Security Requirements.

8.4. Partner shall provide independent assurances over its business and information technology controls applicable to the Services, by providing a Service Organization Report based on the Statement of Standards for Attestation Engagement No. 18 (SSAE 18) ("SOC Report") or equivalent information security certification report (e.g., ISO 27001), Such SOC Report(s) shall cover all controls and security processes and procedures that Partner and its Permitted Subcontractors perform in accordance with existing agreements with Sterling and be in the form of a SOC I Type II and SOC 2 Type II report, as applicable. The reporting period for the SOC Reports shall be for each calendar year and Partner shall provide Sterling or Sterling's third-party auditor with copies of such relevant reports upon issuance or upon Sterling's

request; provided, however, Partner shall use reasonable efforts to deliver such SOC Report(s) no later than November 15th of each year. To bridge any gap between the audit end date and December 31st of each year, Partner shall provide Sterling additional affirmation of ongoing control operating effectiveness. If a SOC Report from Partner's retained third-party auditors yields deviations, Partner shall communicate an action plan within thirty (30) days of the date of issuance of such SOC Report and provide Sterling with periodic updates until such deviations have been remediated, retested and resolved. The audit shall be at Partner's expense as part of Partner's ongoing information security program to evaluate Partner's general security controls.

9. MISCELLANEOUS

9.1. Notwithstanding anything to the contrary in other agreements between Sterling and Partner, Partner shall not be relieved of any liabilities or obligations, including obligations associated with business continuity, disaster recovery or enterprise resiliency or availability, arising from any failure or delay in performing any of its obligations caused by any force majeure events, including but not limited to natural disasters such as floods, earthquakes and uncontrollable events such as war or terrorist attack, to the extent that such liabilities (i) arise as a result of a breach of its obligations under this Security Requirements.

9.2. This Security Requirements is globally applicable unless contrary to local laws and regulations. Local law may require more stringent Standards than those set forth in this Security Requirements. In the event of a conflict, the more stringent Standards will take precedence.