Asda Goods Supplier - Supply Chain Security Standards

FRAMEWORK

This agreement relates to suppliers of Asda where Asda will be the importer of record and where the transit route does not begin and end in Great Britain. It contains procedural requirements to support the supply chain security requirements of Asda to AEO standard. The purpose of the procedures is to ensure that the selected supplier and associated parties are able to provide sufficient evidence of operations to the required security capability and suitability to be entrusted in the provision of goods on behalf of Asda. Providers must agree to routine audits of the documentation and relevant procedures provided at an agreed place of audit.

1. PERSONNEL SECURITY

1.1 New Hires

The supplier and associated facilities must have a written Employee Security Policy, which includes procedures for hiring, employment application and employee documentation, and screening of new employees.

This should include:

- Verification of the applicant's name by photo ID (country issued ID card, driver's license, passport, etc.)
- Verification of the applicant's current address
- Contacting any references
- Verification of employment history

The Employee Security Policy should be reviewed regularly and updated where necessary including applying version controls.

Prospective employees must be required to complete an employment application prior to hiring and appropriate personnel records maintained. The supplier and associated facilities must have a written procedure to perform a background check for sensitive positions such as packing/loading area, security, shipping, IT managers, etc. This background check must be evidenced and reviewed every 12 months.

1.2 Access

The supplier and associated facilities must have a written policy to issue a photo identification card or an access card to each employee for access to the facility. When an ID badge is issued it must include the employee's picture and name and the employee must have their ID on them or wear their badge while at the facility. In limited circumstances, a process by management/supervisors to verify only employees are permitted access may be employed however, this must be robust, documented in policy and appropriate to the level of risk at the facility.

1.3 Termination

The supplier and associated facilities must have a written policy for employee termination. The policy must include collection of and disabling of an employee's facility identification, access keys and cards and require that security and/or management is informed of employees who resign or are terminated.

2. THREAT AWARENESS PROGRAM

2.1 General

The supplier and associated facilities should have a written Threat Awareness Program to train employees about the security threat at each segment of the supply chain. This could include aspects such as: access by only authorised employees and registered visitors, to report someone in a work area who does not belong there, especially in sensitive or restricted areas such as the shipping area, packing area, loading area, warehouse, systems rooms and to report attempted unauthorised access to a computer terminal, etc.

The program should include the procedure for an employee to report a security issue such as a broken window/door lock, breach in perimeter fence/wall/barrier, faults with security alarms/CCTV/exterior lights, etc. along with any unusual activity they may witness.

2.2 Shipping and Receiving

The supplier and associated facilities should provide specialised job-related training to shipping and receiving employees regarding access to sensitive work areas, reporting unauthorised people in the work area, ensuring that only authorised cargo is loaded into the container or trailer, and how to report situations that may involve a conspiracy to use the supply chain for illegal purposes.

2.3 Training

Threat Awareness training should be provided during new-hire orientation and then every 12 months as refresher training to all employees. Security procedures should be displayed in common areas of facilities.

3. PHYSICAL ACCESS CONTROLS

3.1 Sensitive Areas

The supplier and associated facilities must have a written policy stating that designated restricted areas or sensitive areas are required to have access controls determining who can enter the area. Facility management should review the list of authorised employees permitted to enter sensitive and restricted areas.

The supplier and associated facilities must have a written policy stating that no personal items (such as a lunch box, a purse, a backpack, etc.) are allowed in the packing and shipping areas.

3.2 Security Patrols/Monitoring

Security guards, designated members of management or trained employees should perform patrols of the facility premises and report security incidents to the facility's management team (facility premises are not considered to include produce fields or orchards in this context). This should include inspection of existing perimeter fences/walls to check for damage, attempted illegal access, and identify needed repairs. Checklists and logs should be used to evidence that security patrols take place.

The supplier and associated facilities must use Closed Circuit Television (CCTV) or another surveillance method such as patrols to monitor activity in sensitive areas within the facility such as receiving, shipping, final packing, main offices, the lobby, and the computer server/systems room. If using CCTV, recordings should be kept for a minimum of 30 days.

3.3 Visitors and Drivers

The supplier and associated facilities should have a written procedure that requires visitors and pick-up/delivery drivers to show photo identification before entry is permitted. The photo identification of a visitor should be verified by the security staff or receptionist. There must be a written policy indicating that all visitors are escorted at all times while on the premises. It should also include that a serial numbered visitor badge/pass be issued to each visitor and that a Visitors Log is maintained.

The supplier and associated facilities must have a written policy to log truck arrivals and departures to include the driver's name, truck vehicle number, time of arrival, time of departure, and reason of visit. The log is kept for at least 30 days.

3.4 Security Incidents

The supplier and associated facilities should have a policy and procedure requiring that security incidents are reported, logged, and investigated.

4. PHYSICAL SECURITY

4.1 Policies and Procedures

The supplier and associated facilities should have a designated manager responsible for overall security to include creating the security policies and procedures and that physical security is accomplished in accordance with each security policy.

The supplier and associated facilities must have a written policy that requires all security procedures are documented as either a policy or procedure. The security policies should be reviewed every 12 months and updated when necessary.

4.2 Risk Assessment

Security assessments of the facility site must be conducted to identify weaknesses at least every 12 months, with weaknesses identified, recorded in a log, and corrected in a timely manner. The only exception to this requirement is where a pack house operates in a temporary structure or a temporary location.

4.3 Access

The supplier and associated facilities must use an appropriate method to ensure that only authorised employees and escorted visitors are permitted access to cargo handling and storage areas. Cargo handling and storage areas should be designated as restricted areas and display signage. Access gates, exterior doors, and windows should be secured with locking devices. An intrusion detection system or a security surveillance method for sensitive/controlled access areas should be in place. This can be either an electronic detection system or manual methods such as roving security guards or management/supervisors who monitor sensitive areas.

The supplier and associated facilities must have a written procedure for an Access Control Program that describes methods used to record and track keys or other access devices issued to authorised employees for use within the facility. This applies to all permanent, enclosed facilities. The program must include a control log that accounts for all keys/access cards on-hand and not issued, those issued, and any returned to include the employee's name, date signed out, date signed in, reason for use, and the name of issuing person. An inventory-check process should be in place and The Access Control Program policy should include the process to report a lost key or access card.

4.4 Structures

Where possible according to operations, the supplier and associated facility's production building(s) and storage building(s) should be constructed of materials that deter easy access by an intruder. Examples of satisfactory construction materials include metal siding, reinforced wood, brick, cement block, etc. There should be a documented process to inspect buildings for security and maintenance issues each month and to make necessary repairs. Permanent premises should be protected by a wall or fence to avoid easy and unwanted access by an intruder and underground access points such as utility tunnels or water drainage secured to prevent unauthorised access into the facility. There should be a process to ensure that only authorised personnel are issued keys/control devices to open, close, lock, and unlock the facility access gates.

4.5 Lighting

Where the facility possesses a perimeter fence or wall, lighting should sufficiently illuminate the fence, gates, or other access points to allow for visual surveillance during darkness. The facility must have outside flood lighting sufficient to illuminate areas between buildings, the fence/wall line, the container/trailer stuffing, loading and storage areas. Lighting switch access should have controls to ensure that unauthorised persons cannot access the switches.

4.6 Personnel

Where a facility uses an exterior guard post or roving guard, all security guards should be equipped with hand-held radio sets /cell phones or have access to telephone for communication with security staff/management.

The supplier and associated facilities must not permit personal vehicles parked near cargo loading or handling areas. Due to parking space restrictions, some parking areas may be combined; however, during container/trailer loading all personal vehicles should be moved.

5. CONTAINER / TRAILER SECURITY

5.1 Third Parties

The supplier and associated facilities must have a written contract with the freight consolidator that specifies security requirements consistent with the country risk rating and the facility's security standards with regards to employee hiring, security of their perimeter, security of their cargo holding areas, and security of their cargo loading docks.

5.2 Inspections and checks

A container/trailer inspection process must be maintained and include looking for signs of modification and inspecting the undercarriage for hidden devices or packages.

Gate security or a designated facility manager should perform truck outbound inspections with the results recorded in an Outbound Vehicle Log. An outbound inspection would include verifying that the transportation documents are accurate and complete, the driver has the correct container or trailer, and that the actual security seal number is the same seal number listed on the shipping document. The Outbound Log should capture the driver's name, truck license number, container/trailer number, seal number, date and time of departure based on country risk.

The supplier and associated facilities must have a procedure for the Shipping Supervisor or an authorised employee to inspect shipping documents for accuracy.

5.3 Security Incidents and Discrepancies

Outbound container/trailer incidents involving a seal number discrepancy, or a broken security seal must be reported to facility management. There should be a documented process both to report the security incident and resolve the discrepancy. Seal discrepancies must be resolved before the container/trailer is permitted to depart from the facility.

5.4 Storage

Empty or loaded containers/trailers must be kept in a secure area. When stored at the facility, empty and loaded containers/trailers must be secured with a lock or high security seal. Where a lock is used, access to the key must be controlled. Stored containers/trailers that have potentially been tampered with must be reported to a security supervisor or facility management.

5.5 Loading

Loading of containers/trailers should be supervised by either a security guard or a designated member of management to prevent introduction of non-manifested cargo and to ensure security procedures are followed. Where CCTV is used at the facility and the system captures the conveyance loading process, it should include the application of the security seal. Recordings should be kept for a minimum of 30 to 45 days.

The supplier and associated facilities must have a process to perform a 7-point inspection consisting of checking the front wall, left side wall, right side wall, floor, ceiling/roof, inside and outside of doors, and the undercarriage of the container or trailer. Anomalies must be reported to a security guard, the shipping supervisor, or a designated member of management. The 7-point inspection process and results should be recorded on a tracking log or some another document and retained for at least 45 days.

An ISO 17712 High Security Seal (bolt or cable according to risk) must be affixed to a container or trailer immediately after loading is completed. Where the facility ships break-bulk items, or cartons moving to a freight consolidation facility, a padlock may be used to secure the conveyance.

5.6 Seal Control

The supplier and associated facilities must have a process to ensure that only authorised management and the shipping supervisor has access to high security seals. The process should ensure that seals available for use are kept in a secure cabinet, secure drawer or some other secure location that is not easily accessible by unauthorised personnel. Only authorised employees should have access to the seals, with any missing seals reported to security or a supervisor.

The supplier and associated facilities should have a written procedure that states how high security seals are affixed to a container or trailer, are recorded onto a usage log, and are tracked. A Seal Control Log should be used to track seal usage. The log must include seal usage information such as container/trailer number, date used, and name of person using the seal. On-hand and available seals should be recorded on the log in sequential order. The seal control log should be kept on file for six months, either electronically or hard copy.

6. PROCEDURAL SECURITY

6.1 Tampering

The supplier and associated facilities must have security methods to prevent tampering with goods during final packaging.

6.2 Packages and Mail

The supplier and associated facilities must have a process to screen arriving packages and mail prior to distribution.

6.3 Cargo

The supplier and associated facilities must have a written procedure to ensure that data used to create cargo documents and manifests are accurate, legible, complete, and protected against tampering or loss. A review of shipment information and documentation controls should be conducted to verify accuracy and security of data. There should be a process in place that requires shipping records are kept for a specified period according to local law.

The supplier and associated facilities must have a process to ensure that international and domestic cargo shipments are kept separate in the shipping area. There must be a procedure for employees to report anything unusual found in a shipment, such as a different carton, or in the accompanying documents, such as improper cargo description. A process must be in place to ensure the correct number of cartons are loaded into a container or trailer for shipment and any overage or shortage is identified. A process must be in place to ensure that shipping cartons are properly labelled to indicate item description and weight before loading or shipping.

6.4 Transportation

If supplier or associated facility operations involve arrangement of transportation of the cargo to the port or to the border crossing location, the supplier and associated facilities must have a procedure to check the carrier's company history, employee hiring procedures, and internal security controls prior to hiring. The written contract with the transportation service company should include the commercial routes used, allowed transit time, designated rest/meal stops and the requirement for a driver to report any security issue involving the cargo. The facility must conduct a security review of their contracted transport company to ensure compliance with the contract, including driver hiring procedures, facility controls, and truck security inspection.

6.5 IT Systems

The supplier and associated facilities must have a written policy that designates which employees are permitted access to the information systems. This can include designating specific company employees or job functions with responsibility for IT system security, and access to the systems control room granted to designated systems contractors or service providers and only when accompanied by a facility supervisor.

7. INFORMATION SECURITY

7.1 Security

The supplier and associated facilities must have a designated system administrator responsible for establishing system users and their identity codes/usernames. Designated computer terminal users must be assigned a password and should be required to change their passwords periodically. Best practice would be a requirement to change personal passwords at least every six months. Each computer terminal should have a close and lock feature after a period of inactivity.

7.2 Breaches and Incidents

There must be a process in place for the systems administrator to report a security incident to facility management.

The systems administrator should receive and review records of invalid computer terminal password attempts. This includes review of the system-generated lock-out report for suspicious activity and takes necessary action to determine the cause of the lock out. There should be a method for the systems administrator to track and investigate unsuccessful attempts to access the system.

The supplier and associated facilities should have an intrusion warning program such as anti-virus programs, with data saved on a back-up system that enables restoration in the event of significant data loss.

8. CONTRACTOR SECURITY

8.1 Third Parties

The supplier and associated facilities must have a written procedure regarding security vetting of service contractors who require routine or scheduled access to the facility. This should require vetting of contractors with access to sensitive or restricted areas, which considers the contractor's security controls, employee hiring process, and corporate history. There should be a written procedure that provides security standards to contractor employees who enter the premises.

Contractor employees that enter the premises should be assigned an ID badge. This procedure includes positive identification, such as a photo ID, before issuing the ID badge. The identification badge should be issued and returned daily and accounted for by the facility.