It is Signify Policy to comply in full with all applicable rules and regulations related to Supply Chain Security (SCS) such as defined by C-TPAT, EU AEO and other governmental security programs based on the World Customs Organization (WCO) SAFE Framework.

The purpose of the Signify SCS Program is to secure the goods flow in such a way that tampering, unobserved goods replacement, addition of unfamiliar goods, theft or other unauthorized access to the goods flow will be prevented as much as reasonably possible.

If not agreed otherwise, Supplier will meet security requirements that will be demonstrated by being minimum partially compliant with Signify SCS Program prior starting business with Signify and full Compliancy with the program will be demonstrated not later than within 24 months. Full compliancy is meant by self-assessment score >=95%, or GSV rating as low risk, or valid AEO, C-TPAT certification. Partial compliancy: self-assessment score >=85% or GSV medium risk rating

When requested Supplier will perform an annual self-assessment (as provided by Signify) of all security measures (procedural, physical and employee), unless Supplier is certified participant in US C-TPAT or EU AEO or other by Signify recognized SCS certification program (e.g. Intertek Global Security Verification)

Signify minimum security requirements for suppliers:

All suppliers taking part in the Signify Supply Chain shall at least comply with minimum security requirements. These are general recommendations that should be followed on a case by case basis depending on the company's size and structure and may not be applicable to all. The company should have a written security procedure plan in place that addresses the following:

Physical Security: All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Perimeter fencing should enclose the areas around cargo handling and storage facilities.
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area.
- Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety
- Adequate locking devices for external and internal doors, windows, gates, and fences.
- Adequate lighting provided inside and outside the facility to include parking areas.
- Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.
- Unloaded and or empty trailers and or containers must remain inside the secured fenced area until such time they are backed up to a dock to be unloaded/loaded (in permanent observation); otherwise they must be locked.
- Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.
- Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.
- Alarm Systems and Video Surveillance Cameras should be utilized to monitor premises and prevent unauthorized access to security areas

Access Controls: Unauthorized access to the facility and secure areas (shipping, loading dock and cargo areas) should be prohibited. Controls should include:

- The positive identification of all employees, visitors and vendors.
- All visitors should be escorted and should visibly display temporary identification
- Procedures for challenging unauthorized/unidentified persons.
- Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges.
- Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

Procedural Security: Measures for the handling of incoming and outgoing goods should include the protection against the introduction, exchange, or loss of any legal or illegal material. Security controls should include:

- Procedures to ensure that all information related to the shipments is protected from unauthorized access
- Having a designated security officer to supervise the introduction/removal of cargo.
- Properly marked, weighed, counted, and documented products.
- Procedures for verifying seals on containers, trailers, and railcars.
- Procedures for detecting and reporting shortages and overages.
- Procedures for tracking the timely movement of incoming and outgoing goods.
- Proper storage of empty and full containers to prevent unauthorized access.
- Procedures to notify Signify contact, Customs and/or other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.

Container and Trailer Security: Container and trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers. A high security seal must be affixed to all loaded containers and trailers shipped internationally.

A seven-points inspection is recommended for all containers shipped internationally: Front wall, left side, right side, floor, ceiling/roof, insight/outside doors, outside undercarriage, container seals.

Containers and trailers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

Personnel Security: Companies should conduct employment screening and interviewing of prospective employees to include periodic background checks and application verifications. The procedure must be in place to remove identification, facility, and system access for terminated employees.

Information Technology Security: Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

A system must be in place to identify the abuse of IT security including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.

Education and Training Awareness: A security awareness program should be provided to employees including recognizing internal conspiracies, maintaining product integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.