NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

AEO New Zealand
SECURE EXPORTS SCHEME

SES Secure Site Minimum Standards

This document outlines the minimum security requirements that must be met by Secure Export Scheme (SES) partners.

Each business is unique and may require different levels of security depending on the circumstances. The standards may not all be relevant to your business and will be applied as appropriate.

Contents

1. Site security

1.1.	Sites must have appropriate fencing and access controls to prevent unauthorised entry. If perimeter fencing is not possible or realistic, sites must have other security controls to prevent unauthorised access.
1.2.	Buildings, fences, and other security measures used to protect the site must be checked regularly and any required maintenance must be done as soon as possible.
1.3.	Sites must have adequate lighting in entrances and exits, cargo handling and storage areas, fence lines and parking areas.
1.4.	Sites must have adequate security and access controls to prevent unauthorised access to, as applicable: • Offices containing export documentation • Offices containing seals • Buildings/areas where export goods are stored • Buildings/areas where export goods are packed • Container loading areas • Container storage areas
1.5.	If a third-party security contractor is used, there must be written agreements covering patrols, the services provided and incident reporting procedures in place.
1.6.	If security cameras are being used, the following must be recorded in the security plan: • The type of recording system • The operating procedures including documented periodic functionality testing and review • How the content is monitored • How long images are stored for
1.7.	All security technology infrastructure must be physically secured against unauthorised access.
1.8.	Management or security personnel must issue any access cards/codes and keys and keep an up-to-date record of who has them.
1.9.	A site plan must be provided. This should identify, as appropriate: • Buildings and their access points • Areas related to: – Cargo storage – Packing – Container loading – Container storage (including empty and sealed containers) • Emergency Evacuation Assembly point • Areas accessible to vehicles including: – Transport Operator traffic flows

	– Other traffic flows – Vehicle parking areas • Security camera locations • Security lighting locations • Perimeter fencing and access points • Perimeter roads

2. Personnel security and training

2.1.	ID, reference and background checks must be conducted when hiring for key positions. The results of the checks undertaken on successful candidates should be retained. Key positions are ones where employees will be responsible for export documentation, packing and loading of export goods, issuing staff access cards, access codes and/or keys to the property.
2.2.	Companies must have procedures for ongoing maintenance of personnel integrity of all positions. Checks must be conducted periodically or in response to suspicious changes in employee behaviour.
2.3.	Companies must have controls that enable authorised people on the property to be identified. Large companies are expected to have a formal employee ID system in place, such as ID cards and/or uniforms.
2.4.	Companies must have procedures for recovering company property issued to employees and removing employee access to systems when employment ceases.
2.5.	Personnel in positions that handle export goods or documentation must receive training covering applicable SES procedures and obligations.
2.6.	All employees should be provided security training that includes: • Challenging unauthorised or unidentified people in secure areas • Reporting security incidents or suspicious activity • Cybersecurity awareness around computer access and protecting passwords
2.7.	A record must be kept of relevant training employees receive.
2.8.	Contractor and transport operator inductions must cover relevant SES processes and security practices.

3. Visitors

3.1.	Sites must have controls for maintaining security of export products while visitors are on the premises. This must include, as appropriate: • Sign-in and sign-out procedures for visitors • Checking visitor identity on arrival • Issuing visitors temporary identification • Requiring employees to accompany visitors on site

4. Contractors

4.1.	Sites must have procedures for contractor sign-in, sign-out and monitoring while onsite.
4.2.	Any/all obligations that SES members have also apply to anyone contracted to do the work. The SES member must be assured that contractors will meet those obligations prior to selecting the contractor. This aspect does not apply retrospectively to existing contractors.

5. Transport operators

5.1.	Sites must have procedures for confirming the identity of transport operators who uplift the secure packages.
5.2.	Sites must have procedures for giving transport operators access to the site and monitoring transport operators while they are on site.
5.3.	Sites must have procedures for maintaining site security if transport operators need to access the site after-hours or unsupervised.

6. Packing and loading

6.1.	Customs approved packages must be used for SES shipments.
6.2.	The type/s of Customs approved secured packages the company will use are to be listed in the security plan.
6.3.	The positions with management responsibility for loading and packing of export goods must be recorded in the security plan.
6.4.	The area where export goods are packed and loaded should be separated from the vehicle parking area, unless close proximity is required for work tasks. If it is not possible to separate these areas, other controls must be used to prevent unauthorised goods from being added to the package.

6.5.	Unless specifically authorised, only personnel involved in the loading of containers are to be present in the load out area.
6.6.	Before loading a container, a 7/8 point container inspection must be completed to ensure it is not concealing illicit goods. This includes checking the: • Front wall • Left side • Right side • Floor • Ceiling/roof • Inside/outside doors • Outside/undercarriage • Motor area (refrigerated containers only) The inspection must be recorded and signed (or if electronic, acknowledged) by the checker/s. If the transport operator undertakes any part of the 7/8 point inspection, it must be documented and signed/acknowledged. The load site must keep a record of the inspection. When containers are delivered to the site by rail, the undercarriage is checked by the rail operator and does not need to be rechecked at the site.
6.7.	Companies must have processes to check the correct goods and the correct quantity of those goods are loaded and accurately recorded. The company must keep a record of these checks, along with the identity of the employees who did the checks. Companies must have procedures for internal reporting when errors with documentation or product lines are identified.
6.8.	Containers must be continuously monitored while being loaded. If a container is left unattended part way through the loading (e.g. load breaks or overnight) the container doors must be secured. If applicable, the type of lock or seal used for temporarily securing the container doors in this situation must be recorded in the security plan
6.9.	When a container is partially loaded at multiple sites: • All sites involved in the loading must have SES security plans. • The transport operator used must have SES security plans covering the movement of goods between the sites. • The container must be locked or temporarily sealed with a non-SES seal between loads. • The final load site must apply the SES seal
6.10.	Product that has been assembled or combined into a larger package but has not been secured under SES conditions must be inspected on arrival at secure sites to check that nothing has been concealed in the package.
6.11.	When sealed containers are stored, the seal must be regularly checked to confirm it has not been tampered with.

7. Additional air cargo requirements

7.1.	The security plan must include a full description of the sealing method used. If applicable, this includes palletising.
7.2.	The documentation used for recording the contents of the package must be stated in the security plan.
7.3.	Checks must be done to ensure that only the correct goods have been packaged and the relevant documentation is accurate.
7.4.	Sites must check the package remains securely sealed immediately before the package is uplifted for export.

8. SES seals

8.1.	The type of SES seal (this may be a seal, marking, substance or device) used must be listed in the security plan. The conditions that apply to the specific type of seal to be used will also be in the security plan.
8.2.	SES seals must only be used when sealing a container or package for export at a secure site.
8.3.	Companies must have written policies and procedures covering how SES seals are stored, used and recorded.
8.4.	Seals will be delivered to the locations listed in the seal purchase approval document.
8.5.	Seals can only be delivered to sites that Customs has specifically approved.
8.6.	If exporting via sea freight, sites must maintain a seal register that records the: • Individual seal number • Date the seal was received • Date the seal was applied • Container number it was applied to • Identity of the person who applied it
8.7.	When seals are received, they must immediately be recorded into the seal register.
8.8.	Seals need to be stored in a locked receptacle and access limited to authorised people.
8.9.	Employees involved in handling, applying and checking seals must receive appropriate training to do their tasks correctly.

8.10.	If a seal is damaged or broken, a new seal is to be used, and this must be recorded in the seal register. Customs does not require the damaged or broken seal to be retained by the site or returned to Customs.
8.11.	Companies must periodically check the seals being stored match the records in the seal register.
8.12.	Companies must record and report to Customs any seals are lost or have been tampered with.
USING SEALS – SEA CARGO	
8.13.	An SES seal must be applied as soon as the container is loaded and closed. If the container cannot be immediately sealed, the doors must be secured.
8.14.	An employee must check the seal has been correctly applied and the seal number correctly copied onto the load paperwork. This check and the checker’s name need to be recorded.
8.15.	Container seal checks must follow the VVTT method, this includes: • **View** seal and container locking mechanism for damage • **Verify** seal number against documentation • **Tug** on seal to ensure it is affixed properly • **Twist** bolt seal to ensure its components do not unscrew or separate
8.16.	Once sealed with an SES seal, a container can only be transported by SES approved transport operators. All transport operators used to transport containers are listed in the security plan.
8.17.	When the transport operator uplifts the container, the driver must follow the VVTT method to confirm the seal is correctly applied before taking responsibility for the container. Sites must keep a record of this check.
USING SEALS – AIR CARGO	
8.18.	The SES seal must be applied as soon as the goods have been packaged.
8.19.	Once sealed with an SES seal, packages can only be transported by RACAs. All transport operators used to transport air cargo must be RACAs. RACA’s do not need to be listed in the security plan.
8.20.	Transport operators that uplift air cargo must be RACA's, and checks when picking up cargo are covered by CAA Rule Part 109.

9. Contingency planning

9.1.	Companies must have contingency plans for securing areas involved in producing, loading, storing and documenting export goods during emergencies and evacuations. Any partially loaded containers/packages that are left unattended during an evacuation must be repacked unless the container/package was under observation during the evacuation, or security camera footage of the container can be reviewed.
9.2.	The company must have contingency plans for securing sealed packages during disruption to business, such as sea port/airport closures and transport breakdowns.

10. Documented working business practices

10.1.	Companies must do regular quality assurance checks to ensure the requirements in the site's security plan are being adhered to.
10.2.	Companies must routinely check the accuracy of export documentation. These checks should be documented.
10.3.	Companies must get written approval from Customs for any changes to their security plan.

11. Digital security

11.1.	Companies must maintain information security policy and procedures to protect systems that contain export documentation. This includes: • Using passwords • Using firewalls and/ or antivirus software • Using genuine/licenced software products • Having checks to detect suspicious access or changes to systems that contain export data
11.2.	Passwords should be assigned to individual users. Users must change their passwords periodically.
11.3.	Information related to export goods must be regularly backed up.
11.4.	The company should, as appropriate, implement digital security best practices. E.g. implement the National Cyber Security Centre (NCSC) guidelines into company cybersecurity policies.

12. Reporting to Customs

12.1.	Companies must assign a staff member responsibility for how SES is implemented and adhered to in their organisation. The person with this role will be expected to: • Be the main point of contact with Customs for all SES enquiries • Take responsibility for ensuring all incidents are reported to Customs • Understand the company’s commitments as a SES partner • Be responsible for maintaining the security plan and ensuring it is being adhered to • Keep customs updated with changes to business (e.g. change of address)
12.2.	Employees are trained to report security incidents or suspicious activity to a manager/supervisor.
12.3.	Companies are required to have documented procedures for reporting to Customs anything that may compromise the security of the export good, package or container. Including but not limited to: • Any container which has been tampered with • A documented procedure has not been followed • Unauthorised entry to the site • Suspicious or unusual documentation requests • Unauthorised goods within the container or package • Missing seals • Seal tampering (apart from seals replaced on site) • Cybersecurity breaches

13. Other government accreditations

13.1.	In the case where accreditations from other government agencies have been used as evidence to support the company's credential as a secure exporter; the company must inform Customs if these accreditations are revoked or not renewed after expiry.