SES Exporter Minimum Standards

This document outlines the minimum security standards that must be met by a prospective partner of the Secure Exports Scheme (SES) who exports goods but uses third party secure load sites to do all the packing and loading for them.

Each business is unique; some circumstances require a higher level of security in response to a specific risk, and some standards may not be relevant to your business.

Contents

Personnel security and training

1.	**Personnel security and training**
1.1.	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, issuing staff access cards, access codes and/or keys to the property.
1.2.	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.
1.3.	Personnel in positions that handle documentation must receive training covering applicable SES procedures and obligations.
1.4.	All employees should be provided security training that includes cybersecurity awareness around computer access and protecting passwords
1.5.	A record must be kept of relevant training employees receive.

SES seals

Exporters who do not handle seals are not expected to meet the seal minimum standards themselves but are expected to ensure sites that pack and load for them are meeting these standards.

If a business receives and distributes seals to their secure load sites, they are expected to securely store the seals.

2.	**SES seals**
2.1.	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.
2.2.	Seals need to be stored in a locked receptacle and access limited to authorised people.
2.3.	Companies must have written policies and procedures covering how SES seals are stored, used and recorded.
2.4.	Seals will be delivered to the locations listed in the seal purchase approval document.
2.5.	Seals can only be delivered to sites that Customs has specifically approved.

2.	**SES seals**
2.6.	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
2.7.	When seals are received, they must immediately be recorded into the seal register.
2.8.	Seals need to be stored in a locked receptacle and access limited to authorised people.
2.9.	Employees involved in handling, applying and checking seals must receive appropriate training to do their tasks correctly.
2.10.	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.
2.11.	Companies must periodically check the seals being stored match the records in the seal register.
2.12.	Companies must record and report to Customs if any seals are lost or have been tampered with.
USING SEALS – SEA CARGO	
2.13.	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.
2.14.	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.
2.15.	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
2.16.	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.

2.	**SES seals**
2.17.	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	
2.18.	The SES seal must be applied as soon as the goods have been packaged.
2.19.	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.
2.20.	Transport operators that uplift air cargo must be RACA's, and checks when picking up cargo are covered by CAA Rule Part 109.

Contingency planning

3.	**Contingency planning**
3.1.	The company must have contingency plans for securing sealed packages during disruption to business, such as sea port/airport closures and transport breakdowns.

Documented working business practices

4.	**Documented working business practices**
4.1.	Companies must do regular quality assurance checks to ensure the requirements in the site's security plan are being adhered to.
4.2.	Companies must routinely check the accuracy of export documentation. These checks should be documented.
4.3.	Companies must get written approval from Customs for any changes to their security plan.

Cybersecurity

5.	**Cybersecurity**
5.1.	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
5.2.	Passwords should be assigned to individual users. Users must be automatically prompted to change their passwords periodically.
5.3.	Information related to export goods must be regularly backed up.
5.4.	The company should, as appropriate, implement digital security best practices. E.g. implement the National Cyber Security Centre (NCSC) guidelines into company cybersecurity policies.

Reporting to Customs

6.	**Reporting to Customs**
6.1.	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)
6.2.	Employees are trained to report security incidents or suspicious activity to a manager/supervisor.

6.3.	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

Other government accreditations

7.	**Other government accreditations**
7.1.	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.