Safety Management System Modules

Element 25 – Security Management

What and Why

Each railway will be exposed to a different level of security risk. Operators must be able to show how they have assessed the security level that applies to their operations. The types of events to consider are theft, assault, sabotage, terrorism and other criminal acts. Other events may be relevant to specific operators depending on where and what they operate.

For the purposes of section 112 (Security management plan) of the Law, a Security Management Plan must include:

- a list of the security risks;
- description of the preventative and response measures to be used to manage those risks

a description of the policies, procedures and equipment and other physical resources needed to manage those risks.

How

Operators should conduct a risk assessment focused on security matters such as theft, assault, sabotage, terrorism and other criminal acts. The risk assessment should also consider:

- Any additional events that could occur (ie protesters or activists);
- What arrangements should be in place where an operator has an interface with another rail transport operator and how those arrangements are communicated, understood and incidents reported;
- How security incidents will be reported, recorded and responded to;
- What security roles are required and how will they be performed, and by who;
- How will the operator liaise with emergency services in the event of a security incident?
- How will the operator liaise with other operators or rail infrastructure managers in the event of an incident (if relevant);
- How and when will security measures be reviewed, and by who?

Once a risk assessment has been completed, operators should develop a plan that describes:

- The measures they have put in place to prevent and respond to the types of incidents listed above;
- Who to report reporting security incidents to;
- How incidents will be recorded, analysed and responded to;
- Who is responsible for performing security related roles;
- How those people have been made aware of their security related role and what they are expected to do;
- Who will liaise with external parties;
- How security arrangements will be reviewed.

Who

Operators should consider if a single point of contact for security incidents is required, and any details be included in the documented security plan. Details of these responsibilities should be included in the relevant job/role description.

Persons who have nominated security roles are expected to perform their duties in line with their job/role description and the procedures described in the security plan.

The Executive Committee/ Board may wish to sign off on the security plan as part of their governance procedures.

When

Security arrangements should be reviewed:

- As part of the SMS review;
- As part of regular document reviews and updates;
- Changes to any aspect of the security measures put in place;
- After a reported security incident;
- After analysis of any findings associated with an incident;
- as part of the normal risk assessment processes;
- Where there is an increase in the Australian National Terrorism Threat Level.

List of relevant documents (internal)

Element 8 – SMS Review

Element 26 – Emergency Management

Security plan

Security procedures – bomb threat, terrorist activity, environmental activists;

Job descriptions

Links (external)

ONRSR – Guideline – Small isolated line heritage operations – Safety Management System (SMS)

ONRSR Website – Guideline - Safety Management System

ONRSR Website – Rail Safety National Law

RISSB Security Management Handbooks Vol 1 and 2 (membership required)

www.nationalsecurity.gov.au

Appendices

None