



Foreword

The *Transportation of Dangerous Goods by Rail Security Regulations* (hereafter referred to as the Regulations), require railway carriers and railway loaders who offer for transport, handle or transport any of the dangerous goods set out in Schedule 1 of the Regulations to implement a security plan.

The purpose of this document is assist railway carriers and railway loaders in the development of their security plan. Railway carriers and railway loaders may choose to use the security plan template included in this document, but are not required to do so. The template is a guide that outlines how railway carriers and railway loaders may structure their security plan. Any other format is acceptable, provided it meets the content requirements of subsection 10(1) of the Regulations, included below:

- 10 (1)** A railway carrier or railway loader is required to implement a security plan that
- (a)** is in writing;
 - (b)** identifies, by job title, a senior manager responsible for the plan's overall development and implementation;
 - (c)** describes the railway carrier's or railway loader's organizational structure, identifies the departments that are responsible for implementing the plan or any portion of it and identifies every position whose incumbent is responsible for implementing the plan or any portion of it;
 - (d)** describes the security duties of each identified department and position;
 - (e)** sets out a process for notifying each person in a position referred to in paragraph (b) or (c) and who is responsible for implementing the plan or any portion of it that the plan or that portion of it must be implemented;
 - (f)** includes an assessment of the security risks associated with the offering for transport, handling or transport of the dangerous goods set out in Schedule 1 that the railway carrier or railway loader offers for transport, handles or transports;
 - (g)** sets out a process for security inspections referred to in section 7, including
 - (i)** a procedure for conducting security inspections,
 - (ii)** a method for determining whether security has been compromised,
 - (iii)** a method for determining whether additional security inspections are necessary when, given the circumstances, security could be compromised, and
 - (iv)** a method for addressing the situation, if it is determined that security has been compromised;
 - (h)** sets out measures to prevent access by unauthorized persons to the dangerous goods set out in Schedule 1 and to the railway vehicles used to transport those dangerous goods;
 - (i)** sets out measures to verify information provided by candidates for positions that involve access to the dangerous goods set out in Schedule 1;
 - (j)** sets out a policy on limiting access to security-sensitive information and sets out measures for the sharing, storing and destruction of that information;
 - (k)** sets out measures to address other security risks identified in the assessment referred to in paragraph (f);
 - (l)** sets out a program for the security awareness training required under section 14 and the security plan training required under section 11; and
 - (m)** sets out measures to respond to a security incident and for reporting it.

Additional guidance material is available and may be referred to when developing a security plan. All guidance materials can be found on the following website:

<https://www.tc.gc.ca/eng/railsecurity/enhancing-security-transportation-dangerous-goods-rail.html>.

Once completed, a security plan should be treated as a security-sensitive document. It is recommended that all pages be marked appropriately, in accordance with the railway carrier's or railway loader's policy on marking protected and classified information.

Cover Page

Security Plan

Under the *Transportation of Dangerous Goods by Rail Security Regulations*

< INSERT COMPANY NAME >

CONFIDENTIAL – SECURITY-SENSITIVE INFORMATION

< INSERT DATE >

< INSERT VERSION NUMBER >

APPROVED BY: < NAME AND POSITION TITLE >

SIGNATURE: < INSERT >

DATE: < INSERT DATE SIGNED BY APPROVER >

Table of Contents

| | |
|---|------------|
| Record of Revisions | < PAGE # > |
| Introduction | < PAGE # > |
| 1.0 Security Objectives | < PAGE # > |
| 2.0 Security Management | < PAGE # > |
| 2.1 Responsible Security Manager | < PAGE # > |
| 3.0 Security Organization | < PAGE # > |
| 3.1 Security Duties | < PAGE # > |
| 3.2 Process for Notification of the Security Plan | < PAGE # > |
| 4.0 Security Risk Assessment | < PAGE # > |
| 4.1 Other Risks | < PAGE # > |
| 5.0 Security Inspections (railway carriers only) | < PAGE # > |
| 6.0 Access Control Measures – Security-sensitive Dangerous Goods | < PAGE # > |
| 7.0 Personnel Security/Screening | < PAGE # > |
| 8.0 Access Control Measures – Security-sensitive Information | < PAGE # > |
| 9.0 Security Training | < PAGE # > |
| 9.1 Security Plan Training Program | < PAGE # > |
| 9.2 Security Awareness Training Program | < PAGE # > |
| 10.0 Security Incidents – Response and Reporting | < PAGE # > |
| 11.0 Review Process | < PAGE # > |

< INSERT CLASSIFICATION MARK >

Record of Revisions

| Revision # | Revision Date | Section(s)/ Page(s) | Description of Changes | Initials |
|------------|---------------|------------------------|---------------------------|----------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Introduction

Example: This security plan has been developed in order to meet the requirements respecting the implementation of a security plan under the Transportation by Dangerous Goods by Rail Security Regulations (Regulations). The following sections are aligned with the requirements under subsection 10(1) of the Regulations.

1.0 Security Objectives

The Regulations require training on the railway carrier's or railway loader's security objectives under paragraph 12(a). As such, it is recommended that the railway carrier or railway loader set out their security objectives in their security plan, either in the introduction or a separate section.

[Insert text]

2.0 Security Management

2.1 Responsible Security Manager

The security plan must identify, by job title, a senior manager responsible for the plan's overall development and implementation. This information may be included separately or as part of another section, as long as it is clearly sets out the identified individual and their associated security duties.

[Insert text]

3.0 Security Organization

The security plan must include a description of the company's organizational structure. The information provided must also include the department(s), name(s) and position title(s) of all individuals responsible for implementing the plan.

This information may be provided in the form of a table, organizational chart or any other manner, provided it meets the requirements of paragraph 10(1)(c) of the Regulations.

[Insert text]

3.1 Security Duties

The security plan must describe the security duties of each identified department and position. This information might be provided in the section above, under Organizational Structure, or in a separate section. Either way, the security duties of each department and positions must be clearly described.

[Insert text]

3.2 Process for Notification of the Security Plan

The security plan must describe how each person responsible for the development and implementation of the security plan is made aware of his or her responsibilities. Examples of how a railway carrier or railway loader may satisfy this requirement include, but are not limited to, the following:

- Notification in writing via email or an information bulletin with instructions regarding implementation of the plan;
- Notification through individual or group information briefings; or
- Notification through individual or group training sessions.

[Insert text]

4.0 Security Risk Assessment

The security plan must include an assessment of the security risks associated with the offering for transport, handling or transport of the dangerous goods set out in Schedule 1 that the railway carrier or railway loader offers for transport, handles or transports. The risk assessment may be included within the security plan, or as a separate document outside of the plan.

Transport Canada does not prescribe a specific methodology for conducting security risk assessments. Rather, it is up to each railway carrier and railway loader to decide a methodology to adopt to conduct their security risk assessment.

[Insert text]

4.1 Other Risks

The security plan must also set out measures to address other risks identified in the company's risks assessment, in accordance with paragraph 10(1)(k).

[Insert text]

5.0 Security Inspections (railway carriers only)

Railway carriers who are required to conduct security inspections, as set out in section 7 of the Regulations, must set out a detailed process for conducting visual security inspections in their security plan. The process must include the following:

- A procedure for conducting security inspections,
- A method for determining whether security has been compromised,
- A method for determining whether additional security inspections are necessary when, given the circumstances, security could be compromised, and
- A method for addressing the situation, if it is determined that security has been compromised.

[Insert text]

6.0 Access Control Measures – Security-sensitive Dangerous Goods

The security plan must set out the measures to prevent access by unauthorized persons to the security-sensitive dangerous goods set out in Schedule 1 and to the railway vehicles used to transport those dangerous goods.

Access control measures can include but are not limited to;

- intrusion detection systems;
- surveillance systems;
- contracted security guards; and
- front office reception for visitor check-in etc.

The access control measures that the company puts in place for its sites should be appropriate for the size and scope of the company and its operations.

[Insert text]

7.0 Access Control Measures – Security-sensitive Information

The security plan must identify and describe measures and/or technologies in place to protect, store, safely share, limit access to and destroy security-sensitive information. Such information could include internal or external classified reports, security intelligence, security procedures, etc.

Examples of such measures could include, but are not limited to, the following:

- Storage of information in a secure location, such as password-protected computers, or locked cabinets and offices;
- Use of encrypted email to share security-sensitive information with appropriate company personnel; and
- Use of an industrial shredder to destroy security-sensitive information.

The company's policy on the sharing, storing and destruction of security-sensitive information should be reflective of the company's size and operations. Positions that involve access to or handling of security-sensitive information should be identified in the security plan.

[Insert text]

8.0 Personnel Security/Screening

The security plan must include the measures that the railway carrier or railway employs to ensure that candidates for positions that involve access to security-sensitive dangerous goods set out in Schedule 1 are properly screened. Example of such measures include, but are not limited to, reference checks from previous employers and police background checks.

[Insert text]

9.0 Security Training

9.1 Security Plan Training Program

The security plan must set out a program for the security plan training required under section 11. While the training program itself may be included outside of the plan, the security plan should describe how the security plan training program is set out.

It is recommended that the security plan also describe the persons required to undergo security plan training, who is responsible for delivering the training, how the training is delivered, a description of the content of the training, and how and where the records of the training are retained.

[Insert text]

9.2 Security Awareness Training Program

The security plan must set out a program for the security awareness training required under section 14. While the training program itself may be included outside of the plan, the security plan should describe how the security awareness training program is set out.

It is recommended that the security plan also describe the persons required to undergo security awareness training, who is responsible for delivering the training, how the training is delivered, a description of the content of the training, and how and where the records of the training are retained.

[Insert text]

10.0 Security Incidents – Response and Reporting

The security plan must set out the measures to respond to a security incident and for reporting it. This requirement applies to both railway carriers and railway loaders.

It is recommended that the security plan contain the following details related to the response to and reporting of security incidents:

- Who is responsible for reporting a security incident;
- Who individuals are required to report security incidents to;
- The reporting structure and timeframe(s) for reporting a security incident;
- How incidents are required to be reported within the company;
- What information must be included in the report; and
- What response measures are required to be taken.

For railway loaders, this may include security incident reporting measures applicable under other legislation.

Railway carriers are required to immediately report any potential threat or other security concern by telephone to the Transport Canada Situation Centre, as per subsection 3(1) of the Regulations. As such, procedures for reporting security incidents included in their security plan must also be in line with the requirements set out in section 3 of the Regulations.

Further information for railway carriers on reporting security incidents to Transport Canada can be found in the [Railway Security Reporting Guidance](#). Additionally, Transport Canada has developed an optional [Railway Security Reporting Template](#) for reporting security incidents.

[Insert text]

11.0 Review Process

It is recommended that the railway carrier and railway loader describe their process for the annual review of the plan required under subsection 10(2) of the Regulations.

Example: This security plan will be reviewed annually by < insert department > on < insert date > and will be revised, if necessary. The plan will also be revised whenever a change in circumstances is likely to affect the security risks identified in < company's name > security risk assessment.