



Guideline for Security Plan

May 2014

1. REQUIREMENTS

As part of the application for a licence, certificate, or permit for types E (high), I (initiating systems), and D (military and law enforcement) explosives, a Security Plan must be submitted. The Security Plan must include:

- 1.1 an assessment of the security risks resulting from the presence of explosives at the magazine, factory, or satellite or client site;
- 1.2 a description of the measures that will be taken to minimize those risks;
- 1.3 a description of the procedures that will be followed to respond to security incidents; and
- 1.4 a description of the procedures that will be followed to report security incidents.

In addition to having a Security Plan, the *Explosives Regulations, 2013* state that it must be implemented and changed if new circumstances adversely affect the security of the explosives.

2. PURPOSE OF A SECURITY PLAN

The purpose of a Security Plan is to enhance and maintain the security of a licensee's operation by assessing a site for security risks, developing measures to address security issues by incorporating current security programs and developing new ones if necessary, and formalizing responses to and reporting procedures for security incidents. A Security Plan also enables the licensee to:

- 2.1 see how various elements of a security program integrate;
- 2.2 set out roles and responsibilities for the security program, thereby ensuring tasks are assigned, understood, documented, tracked, and organized in a consistent manner;
- 2.3 identify partners and resources in enhancing and maintaining the security of its operations; and
- 2.4 adjust security preparations and operations in response to changing circumstances.

The Security Plan Components section below identifies components that must be addressed within a Security Plan. Section 4. provides a sample Security Plan that may be used as a guide to assist licensees in the development of a Security Plan for their operations; however, its use is not mandatory.

3. SECURITY PLAN COMPONENTS

The Security Plan must address the following components and should include a description of the licensee's current security programs and associated measures, including those already required by the Explosives Regulatory Division (Magazine Standards, Directive #5). The plan should also reference any related documents (i.e., plans, policies, procedures, etc.). These will be described in detail in the following sections:

- 3.1 licensee information;
- 3.2 assessment of security threats and how they are addressed;
- 3.3 procedures to respond to threats to the security of explosives; and
- 3.4 security incident reporting procedures.

3.1 Licensee Information

A Security Plan must be submitted for each licence, certificate, or permit at a magazine, factory, or satellite or client site for types E (high), I (initiating systems), and D (military and law enforcement) explosives. The Security Plan is site-specific and the Licensee Information section identifies the company, the specific site, and a person responsible for the Security Plan at the specified site. The information that should be contained in the Licensee Information section is identified below:

- company identification;
- site identification; and
- the person responsible for the Security Plan at the site (if different from the person making the application).

3.2 Assessment of Security Threats

An assessment of the security threats is designed to look at a specific site, determine any vulnerabilities, including “what if” scenarios, and develop effective strategies to address these threats. Some of the scenarios may have a higher risk (have a higher probability of happening) than others; however, appropriate responses need to be made for all scenarios considered. Just recognizing a potential threat is one of the most effective ways of dealing with it.

This section of the Security Plan should include an overview of the security environment in which the licensee conducts its activities. Thought must be given to vulnerability to theft, sabotage, and unauthorized access by staff, contractors, visitors, or outsiders, and to dealing with unexplained losses. It should include a description of the current security measures in place to prevent, mitigate, respond to, and recover from a security incident, and can include:

- fences, guards, alarms, or lighting;
- magazine construction (*Storage Standards for Industrial Explosives, May 2001*);
- magazine surveillance (Directive #5) or site monitoring;
- in-process storage details; and
- company policies and procedures.

Things to consider and include when developing your security risk assessment:

- 3.2.1 list of locations where types E, I, or D explosives are stored, processed, manufactured, loaded, unloaded, or temporarily stored on the site:
 - are there other equipment or chemicals that could be attractive to thieves being stored at the site?
 - are there mobile storage or process units?
- 3.2.2 approximately what maximum amount of explosives could be at the identified locations at any one time;
- 3.2.3 describe measures currently in place to deter, detect, and respond to unauthorized access (current measures might include perimeter fencing, access controls, guarding, surveillance systems, alarm systems, magazine construction, and training);
- 3.2.4 describe measures currently in place to deter, detect, respond to, and investigate theft or stock discrepancies (unexplained losses) of explosives at these sites (current measures might include inventory, magazine construction, allocation of accountability, limiting accessibility, regular auditing, surveillance systems, and training);
- 3.2.5 assess the threat and vulnerability of your site to “what if” scenarios related to the theft of explosives (consider how the theft could occur, the likelihood of each scenario occurring, the extent to which your current security measures are adequate or need extending, and what else could reasonably be done to reduce the risks of theft of explosives):

- 3.2.5.1 has your company been the target of thieves in the past?
- 3.2.5.2 has there been theft of explosives in the area in recent years?
- 3.2.5.3 is it easily accessible by road?
- 3.2.5.4 is it in a remote location?
- 3.2.5.5 is there a possibility of concealment?
- 3.2.6 describe current record-keeping procedures to reconcile stored, incoming, and outgoing quantities of explosives:
 - 3.2.6.1 who is responsible for updating procedures?
 - 3.2.6.2 who will conduct the reconciliation?
 - 3.2.6.3 who is accountable?
 - 3.2.6.4 are all persons authorized?
 - 3.2.6.5 reconciliation of shipping/receipt invoices against the storage inventory records, the explosives usage records, and the blasting logs;
- 3.2.7 describe any procedures your company has in place to determine and investigate any unexplained loss of explosives (current measures might include records, allocation of responsibility, training, regular auditing, use of seals, and written procedures); and
- 3.2.8 access – who has access and do they have an approval letter or other acceptable equivalent document?

3.3 Response Procedures and Policies

The Security Plan is designed to consolidate all matters addressing the security of explosives. It must also contain all procedures and policies that must be followed and assign who is responsible for conducting those procedures. By consolidating all procedures and policies related to explosives into one document, they can be accessed and followed when needed without having to review or consult a number of documents that may not always be readily available. Documents that should be included are:

- 3.3.1 procedures/responses for handling surveillance system alarms (including contacts) and system testing;
- 3.3.2 procedures for stock record keeping;
- 3.3.3 procedures/responses for dealing with immediate risks (sabotage);
- 3.3.4 procedures/responses to address unauthorized personnel gaining access to the explosives or means of containment during business and off hours:
 - 3.3.4.1 those that need to be on site (contractors, visitors, unauthorized employees), and
 - 3.3.4.2 those who are on site surreptitiously (trespassers);
- 3.3.5 assign persons for each procedure/response (include alternates);
- 3.3.6 nominate a responsible person (include alternates) to implement and maintain the Security Plan;
- 3.3.7 reporting procedures (see Section 3.4 below); and
- 3.3.8 other company policies and procedures relevant to the security of explosives (screening, access control, training, etc.).

3.4 Security Incident Reporting

All incidents must be reported. This section describes the procedures for reporting security incidents related to the explosives on your site (including thefts, attempted thefts, unexplained

losses, sabotage or attempted sabotage, break-ins, attempted break-ins, and any other security incidents). The procedures must outline how an incident is investigated and by whom, and to which agencies the reports must be submitted, along with timelines. An incident is an opportunity to learn and reporting provides an opportunity for all to take action against it recurring within your industry.

Things to consider and include:

3.4.1 internal reporting:

3.4.1.1 what procedures will be followed and what measures will be taken in an explosives incident?

3.4.1.2 significant findings (description of what was witnessed, the sequence of events, what may have contributed to the incident, probable cause(s) and contributing factors), and

3.4.1.3 recommendations, corrective actions, and mitigation measures (based on investigative findings) – may or may not include revision of Security Plans;

3.4.2 external reporting:

3.4.2.1 what procedures will be followed and what measures will be taken in an explosives incident?

3.4.2.2 in addition to notifying the Chief Inspector of Explosives, what external partners need to be contacted (i.e., police, municipal, provincial and/or federal agencies), and

3.4.2.3 summarize any arrangements in place with other external parties requiring them to report security incidents and set out the reporting processes those parties are to follow;

3.4.3 outline the processes for investigating security incidents (how will an incident be investigated to determine why it occurred); and

3.4.4 which individuals and positions will be responsible for implementation of the procedures.

3.5 Considerations

3.5.1 Confidentiality of the Security Plan

The Security Plan should be treated as a security-sensitive document. The licensee should limit and control distribution of the Security Plan and ensure that the original and approved copies of the plan are stored in a secure location. Security risk assessments should be reviewed annually at licence renewal or whenever circumstance changes, particularly in light of any security incidents that occur.

3.5.2 Partnerships

As part of your overall plan, other organizations or individuals may have an interest or responsibility in ensuring the security of your explosives. Letting the local police know about your plans and getting them on board either formally or informally is recommended. The more eyes you have looking out for you, the better. If appropriate, contact your neighbors to help identify suspicious persons or activity, and have a way for them to contact you. If you have a shared site, each partner needs to know their responsibility with either a formal or informal agreement. It is recommended that any partnerships and their details be included in the Security Plan so those implementing any of the plan's procedures know what they are.

3.5.3 Reviews

Your Security Plan, as well as your company policies and procedures, should be reviewed regularly to ensure they are up to date and reflect the current status of your site. It is recommended that you place a review date on these documents and assign a person to initiate the reviews.

Note that if you have a zone licence, a plan may be somewhat generic and additional details that are site specific may need to be addressed.

3.5.4 Training

The Security Plan is only as effective as the persons responsible for its implementation. Depending on the plan complexity and employee turnover, it is recommended that regular training on the contents of the Security Plan be conducted for those that need to know. While it is a confidential document, persons responsible for the various parts need to be informed and trained if necessary.

3.5.5 Other Considerations

Although not required to be submitted with the Security Plan, a Key Control Plan and a list of employees requiring screening approval letters is required under the Regulations and must be made available. Separate guidelines are available for developing a Key Control Plan and for understanding requirements under the screening provisions of the Regulations. It is recommended you include them as part of your Security Plan as they form part of the overall explosives security program for your site.

For an example of a Site Security Plan, contact your Regional office and request Guideline G05-25.

If you have any questions, the Explosives Regulatory Division can be reached at the coordinates below.

**Pacific Region:
BC + YT**

1500 - 605 Robson St.
Vancouver, BC
V6B 5J3
Tel.: 604-666-0366
Fax: 604-666-0399
ERDpacific@nrcan.gc.ca

**Western Region:
AB + SK + NT**

214 - 755 Lake Bonavista SE
Calgary, AB
T2J 0N3
Tel.: 403-292-4766
Fax: 403-292-4689
ERDwestern@nrcan.gc.ca

**Central Region:
ON + MB**

580 Booth St. 10th Floor
Ottawa, ON
K1A 0E4
Tel.: 613-948-5187
Fax: 613-948-5195
ERDcentral@nrcan.gc.ca

**Eastern Region:
QC + NU + Atlantic**

2050 Girouard W - Box 100
St. Hyacinthe, QC
J2S 7B2
Tel.: 450-773-3431
Fax: 450-773-6226
ERDeastern@nrcan.gc.ca

Headquarters:

580 Booth St. 10th Floor
Ottawa, ON
K1A 0E4
Tel.: 613-948-5200
Fax: 613-948-5195
ERDmms@nrcan.gc.ca