

# Soft target security plan

or what should not be neglected  
in its processing

April 2025



2<sup>nd</sup>  
revised  
edition




**Prepared by:**  
Security Policy Department  
Ministry of the Interior of the Czech Republic

**Editing and publishing:**  
Security Policy Department  
Ministry of the Interior of the Czech Republic

**Contacts:**  
[obp@mv.gov.cz](mailto:obp@mv.gov.cz)

**Police hotline for soft targets:**  
800 255 255

**Interior Ministry web:**  
<https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>

**Social media:**  
 <https://x.com/vnitro>  
 [https://www.facebook.com/vnitro\\_cz](https://www.facebook.com/vnitro_cz)  
 <https://www.youtube.com/user/MinisterstvoVnitraCR>

Sending a security plan to the Police of the Czech Republic can significantly improve its potential intervention. Therefore, the processed security plan can be sent in an editable form to the Operational Department of the Police Presidium of the Czech Republic ([pp.oo.opc-racni@pcr.cz](mailto:pp.oo.opc-racni@pcr.cz)), where it will be further used to prepare police officers for intervention in the soft target.

Table of Contents

**1. Soft target typology ..... 5**  
    a. Basic information about the institution/event ..... 5  
    b. Basic information about the site /venue ..... 5  
        Map of the site/premises: ..... 5  
**2. Security features of the institution/event area ..... 5**  
    a. Physical security ..... 6  
        Presence of security staff ..... 6  
        Procedures for routine situations/incidents ..... 6  
        Examples of procedures for routine situations and incidents ..... 7  
        Routine procedures ..... 8  
        Authorization to enter the premises ..... 8  
        Incident procedures ..... 9  
        Training of security staff ..... 10  
        Training of other staff ..... 10  
    Management training (beyond the basic security awareness, see above): ..... 10  
    b. Technical security measures ..... 10  
        Electronic elements ..... 10  
        Mechanical elements ..... 10  
        Procedure using X-ray ..... 11  
        Use of X-ray for the check of delivered mail ..... 11  
        Training in technical security measures ..... 13  
**3. Notification and recording of security incidents .....13**  
**4. Contacts ..... 14**

# Introduction

This manual is intended for owners/administrators and security managers or other persons responsible for soft target security (hereinafter referred to as soft target representatives) to develop practical security plan to help them address soft target security issues systematically. At first, it is necessary to define what is meant by the term **soft targets**. Soft targets represent **places with a high concentration of people and a low degree of security against major violent and terrorist attacks**. This definition is based on the [Basics of Soft Target Protection guidelines](#), which **can be downloaded from the website of the Ministry of the Interior**.

This document focuses on planning a system of protection against major violent and terrorist attacks; it does not cover other types of threats. However, proper planning in this area usually has a positive impact on the prevention and management of other types of threats (typically, for example, disruption of public order). At the same time, major violent and terrorist attacks are stressful situations to which it is necessary to be prepared in advance and to know the procedures well. Acutely written procedures and well-trained personnel can ensure an adequate response to such situations as well as the mitigation of consequences. Besides, in the event of a dispute or litigation concerning liability, a prepared security plan demonstrates that the organization is responsible and does not neglect its security responsibility.

First of all, it should be emphasized that the soft target security plan shall only be processed after a **threat assessment** of the given soft target is **elaborated** and the soft target representative knows what the soft target is facing, what are the threats and thus has **clarified the priority threats**. **Guidelines on how to elaborate a threat assessment**

**are available in the methodology** on the [website of the Ministry of the Interior](#). Appropriate security measures are applied based on a threat assessment that identifies violent threats and risks the soft target faces. It is good to formulate these measures clearly in a security plan that is unique to each soft target.

The security plan is developed especially so that the soft target representative knows precisely how they will protect their soft target. It is, therefore, essential to describe clearly how the soft target representative wants specific situations to be addressed. Both preventive measures and routine procedures, and procedures during incidents that may occur at a given location should be included.

The security plan is, therefore, a manual containing all the information and measures that need to be known and applied to the security of the soft target. It also provides a guarantee that the implementation of measures will not be disrupted even in the case of personnel changes. Finally, the security plan systematizes adopted security measures into one system. During its elaboration, it also verifies their compatibility and coherence within the whole soft target security system.

The following summary contains the types of data that should not be omitted in the soft target security plan. However, their processing will be specific to each soft target.

## 1. Soft target typology

Since soft targets are a large and diverse group of different entities, it is practical to include the fundamental characteristics of a soft target at the beginning of each security plan. In addition to the character of the institution, it is also necessary to describe the character of the site/premises, including all maps of the site/premises. It is also advisable to describe the surroundings of the soft target because it is likely that there are other soft targets in the vicinity. It is good to know about them and to include at least some basic information about them in the security plan.

### a. Basic information about the institution/event

- Title of the institution/event:
- Address of the institution/event:
- Contact person in charge of the security of the institution/event and his/her representative:
- Contact the reception/concierge/dispatch (control room)
- Type of the institution/event:
- Organizational structure of the institution/event: Symbolism of the institution/event:
- Opening hours of the institution/event date:
- Number of employees of the institution/event: Maximum capacity of visitors to the institution/event: An average number of visitors to the institution/event:

Etc.

### b. Basic information about the site /venue

- Description of the site/premises:
- Specifics of the site/premises:
- Mode of entry to the site/premises:
  - » without authorization;
  - » authorization of entry (e.g., ticket);
  - » entry with basic control of undesirable objects;
  - » etc.

### Map of the site/premises:

Mark on the map in particular entrances to the facility/area, escape exits, places of greater concentration of people in the facility/area, location of security measures (authorized, controlled entry, location of camera barriers to entry/entry or other equipment, evacuation/evacuation routes, safe haven, lock down areas, i.e., improvised lock down, access routes for police and other IZS units, assembly areas for evacuees, etc.).

## 2. Security features of the institution/event area

Another aspect that should be incorporated into the security plan and that needs a regular update is the summary of resources available to the soft target. These are both physical security measures, i.e., security personnel and their organization, and technical measures, i.e., electronic and mechanical elements. Furthermore, it is also essential to include in the security plan how the security measures should work in terms of prevention, i.e., during routine operation and in case of an incident. These measures should be written down in the form of standardized procedures for various situations that are relevant to the given site/premises.

Likewise, the standard procedures for using technical elements must be stated here. All procedures may be updated in the security plan according to actual needs (e.g., should a new trend of attack methods appear, it is necessary to respond to it by changing the procedure or developing a new one). Finally, this section of the security plan should include types of training sessions on the procedures as well as their frequency.

## a. Physical security

### Presence of security staff

- only non-security staff;
- in-house security staff and security manager or other persons responsible for the security of the soft target (their numbers);
- external security company (their numbers);
- voluntary security or organizing service (their numbers);
- the presence of other security forces (e.g., the police and in what cases – depending on how cooperation is set up)
- none.

### Procedures for routine situations/ incidents

Security staff should work based on standardized procedures that must always be developed for a given facility/area and must be regularly reviewed. It is crucial to standardize procedures both for routine security measures and for incidents. They are detailed for routine activities and include procedures also for less common situations. Procedures for security incidents, on the other hand, tend to be very brief and must

be accompanied by tactical drills. However, it should not be forgotten that communication is an essential security tool. Therefore, training of standardized procedures should also include training of assertiveness and crisis communication. Security procedures both for routine and security incidents must be binding for the security personnel and should be regularly updated as necessary.

# It is necessary to train also the ordinary personnel in safety.

In addition to security staff, there is also need to work with other staff and to train them adequately to increase their security awareness. In order to protect soft targets, it is appropriate to train staff on fundamental security aspects, such as reporting incidents that are out of the routine operation or the RUN- HIDE-FIGHT procedure<sup>1</sup>, which can significantly reduce the impact of an attack.

<sup>1</sup> More about the procedure see a video of the Police of the Czech Republic: <https://www.youtube.com/watch?v=XxkZRze5Pd8>.

Examples of individual situations for which a procedure can be processed:

- in-house standardized procedures for both routine and incident situations
  - » visit verification;
  - » document checking;
  - » security interview;<sup>2</sup>
  - » reaction to a suspicious person;
  - » reaction to a suspicious item;
  - » evacuation out;
  - » evacuation inside;<sup>3</sup>

- » „lockdown“ procedure;<sup>4</sup>
- » etc.

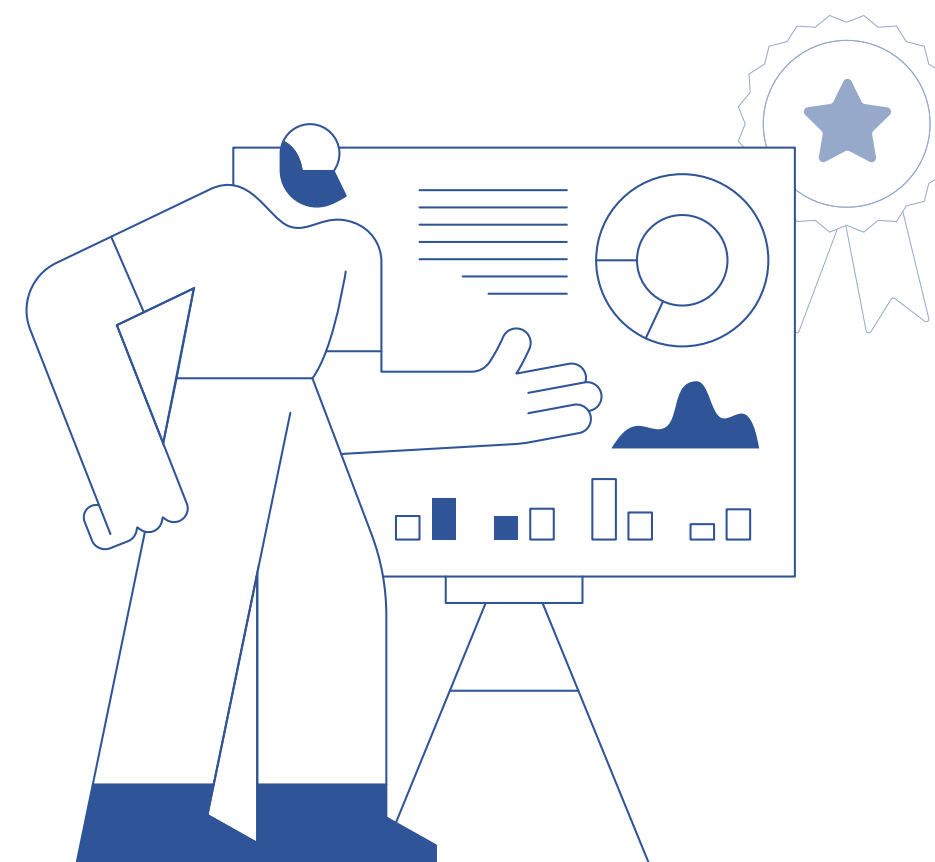
- regular updates of procedures (to be carried out by the security manager or other persons responsible for the security of the soft target as necessary);
- checking/testing compliance with procedures (regularity depends on individual needs of the facility/area)
- etc.

### Examples of procedures for routine situations and incidents

<sup>2</sup> This is a brief, structured dialogue between the security officer and the selected person (suspicious visitor, etc.). It is carried out on-site and aims to confirm or refute the real purpose of the presence of the person at the site. It consists mostly of a few simple, polite questions raised towards the person. If there are discrepancies in the interview, it is possible, for example, to refuse the person to enter the building.

<sup>3</sup> If you have the option, prepare a safe haven for this purpose, which you can equip for temporary survival.

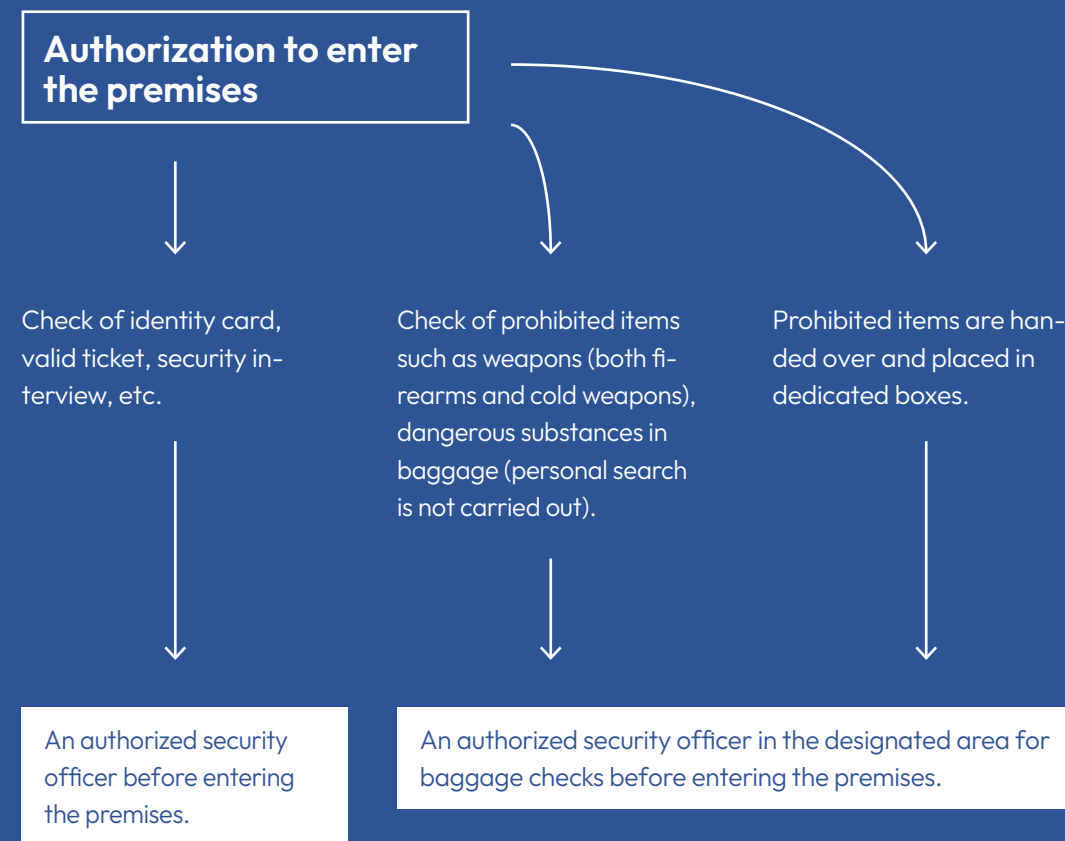
<sup>4</sup> If the soft target is symbolic in nature, it is necessary to consider specific methods of attack of particular extremist groups in the security procedures.



# 1. Example of a routine procedure:

- entrance to the festival grounds

## Routine procedures



# 2. Example of incident procedure:

- deferred baggage;
- threatening phone call;
- shooting.

## Telephone notification of the set-up of an explosive system

1. Enable call recording/record exact statement of the caller.
2. Find out more information: where the explosive system is stored, when the explosion is about to happen, what it looks like, what kind of explosive, how the detonation occurs, who put the bomb in place, why, who are you, where are you, try to use the knowledge of the premises to verify if the person was there and knew it.
3. Record the telephone number from which the person called, their sex, age and nationality estimate.
4. Write down all the details that can help in the search (background sounds, caller status – stress, nervousness, spoken quietly /loud, speech defects, accent, etc.).
5. Contact the Police of the Czech Republic.

## Incident procedures

### Shooting

1. Nemanipulovat s objektem, uzavřít perimetr, nenechat žádné osoby v bezprostřední blízkosti.
2. Pokusit se najít majitele.
3. V případě, že věc nikomu nepatří, kontaktovat Policii ČR.

### Deferred baggage/item

1. Do not handle the item, close the perimeter, and leave no one in the immediate vicinity.
2. Try to find the owner.
3. In case the item does not belong to anyone, contact the Police of the Czech Republic.

Security of the leading shift: XXX XXX XXX  
Police of the Czech Republic: 158  
Next steps, according to the established procedure (e.g., direct superior).

### Training of security staff

In addition to writing the procedures, write down a training plan. It is necessary to train all relevant actors and to develop a thematic plan for staff training in the security procedures for this purpose. The frequency of training is at the discretion and capacity of the security manager or other persons responsible for the security of the soft target. In general, however, it is good to train frequently and regularly. Outside the planned training sessions, brief reminders during briefings or meetings before the start of the shift can be carried out. Also, in the case of a security incident, it is good to convene a meeting and evaluate the concrete solution of the situation.

For example:

- regular training of procedures;
- regular training of security interviews;
- regular training to detect suspicious items, person consignments, vehicles;
- regular training of assertiveness and crisis communication;
- regular training of coordination plan;
- regular legal training for professional staff;
- etc.

### Training of other staff

- increasing security awareness;
- reporting of non-standard situations (e.g., foreign person or object at the site, etc.);
- basic procedures (e.g. RUN-HIDE-FIGHT);
- etc.

Management training (beyond the basic security awareness, see above):

- coordination plan

### b. Technical security measures

In addition to a simple inventory of the technical elements of the security system, it is also necessary to know what the technical security measures are for, who and how they will use them and who will control their operation. Therefore, as in the case of physical security, it is necessary to set up standardized procedures for their use and evaluation of knowledge.

#### Electronic elements

List of specific electronic elements placed at the facility/area:

- camera system;
- alarm security and emergency systems;
- X-ray;
- Internal radio;
- etc.

#### Mechanical elements

List of specific mechanical elements placed at the facility/area:

- double door security system;
- fences/walls;
- security windows;
- roadblocks;
- etc.

# An example of processing a procedure on using technical security measures

- An example of an X-ray procedure to check the mail:

## Procedure using X-ray

### Use of X-ray for the check of delivered mail

When receiving mail from a postman, first ask them to wait on the spot while incoming mail is checked:

- first, make a visual check of the delivered mail for suspicious signs (e.g., liquid leakage, suspect sender address, etc.):
  - » if the mail shows suspicious signs during a visual check, notify the present deliverer and security manager;
  - » if the mail does not show any suspicious signs during the visual inspection, the X-ray inspection follows;
- individual pieces of delivered mail are placed in X-ray for inspection against metallic and chemical/biological elements that:
  - » may be okay if they are, for example, paper clips – in this case, the security check was all right, and the mail can be forwarded to the addressee;
  - » may indicate the presence of an explosive device – in this case, reduce handling, call the security manager, call the police;
  - » may indicate the presence of chemicals – in this case, limit manipulation, call the security manager, call the police.

Security of the shift leader: XXX XXX XXX  
Police of the Czech Republic: 158  
Next steps, according to the established procedure (e.g., direct superior).



# Evidence incident logging helps to improve protection and detect threats.



## Training in technical security measures

The use of technical security measures in such a way that it is a purposeful and compatible part of the security system must always be supplemented by training for their qualified operation and evaluation of the knowledge gained by the security staff. It is therefore important that security staff receive regular training in this case as well. The regularity of the training again depends on the needs and capabilities of the security manager or other people responsible for the security of the soft target.

Training can focus on:

- training of staff on the use of CCTV systems;
- training of staff on the use of X-rays;
- etc.

## 3. Notification and recording of security incidents

Recording of security incidents can help in several ways in the future. Firstly, existing measures and procedures may be improved based on the evaluation of incidents. Incident evaluation and the subsequent conclusions can also be a good lesson for the soft target's security system. Secondly, it can also assist the police in identifying offenders. At the same time, it can help to detect the culprit who causes security incidents repeatedly and thus can prevent further incidents. In addition to the police, it is recommended to share information about past incidents with other relevant partners (e.g., other soft targets in the area). Such information may be important and indicate, e.g., the collection of information, which may be a harbinger of an upcoming major or terrorist attack.

Records:

- in the event of a security incident, the security officer present shall make a record;
- they shall provide the record to the security manager, who will evaluate the incident and update the procedures based on the evaluation;
- they shall share incident information with other relevant partners:
  - » the police;
  - » institutions/events nearby;
  - » management of the institution/event.

Example of Incident Records Table:

Date:	Time:	Place:
Description of the incident:	What happened, who was present, what was the procedure	
Description of the person:	Age, stature, hair and eye colour, clothing, special signs such as tattoo, accent, etc.	
Description of the object:	What was that object – its description	
Solution:	What was the solution to the situation	
Next:		
Recorded by:		
Forwarded to:		



4. Contacts

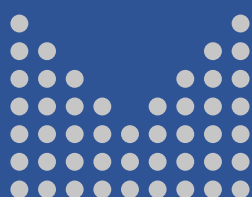
**Communication is the basis of security.** When an incident occurs, it is necessary to know in advance whom to share such information with. In the event of a security incident, a precisely written contact list reduces stress and tension, thus increasing the likelihood that the response will be sufficiently quick to help mitigate the consequences of the incident.

It is important to have a pre-determined procedure for alerting people in the facility or in the event area. Ideally, you should also have a plan for informing people who are outside the building (e.g. at a meeting) not to return to the vicinity of the soft target. This system needs to be tested regularly to ensure that it will work if necessary. Again, we recommend that the procedure for activating the system, including

Contact	Address	Telephone	Mobile	E-mail	Note
Responsible person (e.g., security manager)					
Shift manager (or equivalent)					
Police of the Czech Republic – emergency line					
Contact within the Police of the Czech Republic (if established)					
Press Office					
Etc.					

**Effective communication and clear contacts are key to a quick incident response—warning systems must be prepared and regularly tested.**





MINISTRY OF THE INTERIOR  
OF THE CZECH REPUBLIC

**Soft target security plan**  
or what should not be neglected in its processing

2<sup>nd</sup> revised edition

[www.mv.gov.cz](http://www.mv.gov.cz)