ISPS
& Port Security Standards and Recommendations

A guide for port companies

Introduction

This ISPS guide supports competent authorities and port companies seeking guidance in establishing smooth and secure operations. It gives a clear overview of what is standard practice and needs to be done according to regulations. It provides extra recommendations for those wishing to go the extra mile to secure their premises and leave nothing to chance. Competent ISPS authorities can use this guide during their inspections and/or require certain measures through the Port Facility Security Assessment. It is not intended as a set of hard regulations, but as a practical go-to guide where you find information at a glance, together with a handy checklist. We hope it helps you in securing ports and companies.

International working group ISPS code & regulations

Contents

Security Plan and International Ship and Port Facility Security Code (ISPS) (portofantwerpbruges.com)

1. ISPS Perimeter & fence

1.1 ISPS Perimeter

1.1.1 Aim

Establishing a clear boundary of a secure area where security rules must be observed by all port users and where the port facility is responsible for exercising its security responsibilities.

1.1.2 Standard

ISPS Perimeter

- The competent authority defines the ISPS perimeter in the PFSA.
  - The ISPS perimeter is the entire corporate site, including all adjacent land areas, associated with:
    - the embarkation/disembarkation of passengers;
    - the storage, production, loading and unloading of cargo;
    - storage buildings, manufacturing units, warehouses, etc. *(offices may be located outside of the perimeter);*
- The perimeter is completely closed to prevent unauthorised access.

Exceptions

- Exceptions may include a more limited definition of the ISPS perimeter or the non-closure of the ISPS perimeter.
- Exemptions may only be granted by the competent authority after justification and on the basis of geographical location and/or low risk activities.
  - e.g.: public quays, waiting berths, bulk terminals (type sand, gravel, etc.), interruption of a public road or other very specific situations.
- In this case and particularly in the case of seagoing vessels, other security measures are in place to prevent unauthorised access, intentional unlawful acts and illegal activities.
  - e.g.: cameras, security guards, etc.

1.2 Fence

1.2.1 Aim

The fence is a barrier to prevent unintentional unauthorised access and delay deliberate intrusion.

The fence may also be replaced by an equivalent alternative construction, such as a concrete wall. This alternative construction shall be tested and approved by the competent authority.

Transitional period: this standard applies to new or replacement fencing. The competent authority may also decide that the facility must install new or modified fencing earlier.

1.2.2 Standard

Fence

Minimum

- Overall height: at least **2.40m** (fixed construction). The anti-scaling protection is an extra section on top of the fixed construction.
  - The anti-scaling protection is an extra section on top of the 2.40m fixed construction.
  - The competent authority may grant exemptions for safety reasons.
- Buried or anchored to the ground in several places or fitted with an impenetrable tension wire at the bottom.
- It should be impossible to crawl between the fence and the gates.
  - The fence fits closely to the gates; and/or
  - The access point is permanently manned or under CCTV surveillance.

Recommendations

- Anchorage can be replaced with heavy concrete jersey blocks at the bottom.
- At least 3 rows of barbed wire at the top.
- Detection systems: smart fence, alarm, voltage, etc. (at critical points).
- 2 layers of fencing.
- Cut-resistant fencing.
- Non-corrosive materials.

Mobile Fencing

Minimum

- Each panel is reinforced with concrete blocks or anchored to the ground.
- Panels (fences) are joined together with at least 2 solid bolted clips.
- The use of containers may be an equivalent alternative.
- If fencing or alternatives are not possible due to the work situation, permanent physical surveillance must be organised by your own or other security personnel.

Recommendations

- Additional surveillance through cameras or security personnel (at critical points).
- Additional security measures based on goods, passengers and duration.

Waterside Perimeter

Minimum

- The waterside end of the fence is fitted with:
  - Anti-scaling protection;
  - Barbed wire;
  - Steel plates to prevent grabbing; or
  - Other anti-scaling devices.
- The waterside of the facility (= quay side) is under appropriate human or digital surveillance when seagoing vessels are present.
- The construction takes the tides into account.
  - Use a camera if the infrastructure is not good enough.

Recommendations

- Ships should always be moored within the perimeter of the terminal.
- External bollards must be specially and/or separately secured.
- Additional measures for and/or in cooperation with the ship.
- An agreement should be drawn up (in the PFSP) for mooring lines crossing neighbouring facilities.

Perimeter Control

Minimum

- Procedure with realistic surveillance rounds to check the condition of the fence. The number of surveillance rounds shall be increased in proportion to the number of perimeter breaches or replaced by smart fencing. This may also be determined by the competent authority if necessary.
- Each perimeter check shall be recorded and the PFSO shall review the reports.
- Any deliberate damage shall be reported to the competent authority.

Recommendations

- E.g.:, but to be determined entirely according to the facility and in function of the risks, incidents and security measures in place:
  - High-risk terminals: at least **1×/day**
  - Low-risk terminals: at least **1×/week**
  - Spread the checks throughout the day or each shift
- Smart fence:
  - Daily check that the system is working properly
  - Regular checks on foot to detect minor irregularities that the system doesn't detect or that you can't see from the control room
- The use of fixed tag points and additional control points, possibly with live locator or GPS tracking
- Camera and video surveillance
  - Fixed camera at weak/blind spots
  - Include the perimeter in the 'camera sweep'
  - The use of drones for perimeter patrols
- Additional lighting where visibility is poor to improve camera quality and staff safety.

Repair of Damaged Fencing

Minimum

- Immediate repair with a temporary solution

Recommendations

- Additional surveillance (guard, camera, etc.)
- Establish SLA's with the supplier and/or your own technical service
  - Provide your own (technical) service with repair and spare parts; or
  - Establish a contract with an external company

No Obstacles

Minimum

- No obstacles near or against the fence (e.g.: pallets, vehicles, ladders, etc.).
- Extra suitable barrier for immovable obstacles or trucks on the public road.

Recommendations

- For movable obstacles: a minimum distance of 2m is recommended.
- For immovable obstacles: a higher fence, extra barbed wire, intrusion detection cameras, etc.
- For obstacles on public property: request additional measures from the local authority, such as a parking ban (if possible).
- No natural bushes and trees, except as an additional security barrier (e.g.: thorny bushes).
- Follow the height of the terrain; on a hill the fence must go up.

1.2.3 References

Loss Prevention Standard

There is a recognised certification for physical security products: Loss Prevention Standard LPS 1175
LPCB Attack Testing LPS 1175 - YouTube

Products from European suppliers aren't usually certified by a Loss Prevention Certification Board (LPCB). The technical descriptions of their products include the standards to which the **parts conform** (NEN-EN, etc.). Many European fencing suppliers indicate which standard(s) their business processes comply with.

Relevant EU Guideline

Guideline, building perimeter protection - Publications Office of the EU (europa.eu)
There is a European organisation that deals specifically with perimeter protection: Perimeter Protection Association of Europe.

2. Gates

2.1 Aim

Gates are a point of entry into a closed perimeter where people can gain authorised access (see "Access Control and Authorisation" Standard) and where unauthorised access is prevented.

2.2 Standard

General Principles

Minimum

- Gates and doors are only open for as long as an authorised person or vehicle needs to enter or exit.
- Gates and doors that are permanently open are under physical surveillance or intelligent digital surveillance with an alarm.
- Gates and fences are of the same height *(excluding the anti-scaling protection)*
- It should be impossible to crawl between the fence and the gates because:
  - The fence fits closely to the gates (no gaps between the gates and the fence);
  - The access point is permanently manned or under CCTV surveillance;
  - and/or the barrier boxes must be adequately protected to prevent climbing.
- Gates must be capable of being locked in the closed position
- A clear and visible "ISPS" or "Authorised Persons Only" sign at each operational entry gate/main gate.
- *An anti-passback system for entrances with a badge system*
- *A code system for non-sensitive terminals only*
- A 24/7 surveillance system for each operational entry/exit point; either
  - physical
  - camera
  - alarm with follow-up (linked to a 24/7 dispatch or control room)
- Lighting at each (operational) entry/exit point
- A geographical map in the PFSP showing the:
  - entire perimeter
  - each entry/exit point (even when not in use)
  - gate/door function
  - cameras

- Staff security awareness:
  - The importance of closed access points and awareness of tailgating
  - Be aware of anomalies: deliberate blocking of gates, materials or information to circumvent the use of the gate (e.g.: stones, ladders, visible codes, etc.)
- Report anomalies and changes to the competent authority
  - Report any deliberate damage
  - Report any gate that's out of order for an extended period of time **and** the temporary security measure:
    - Damage is such that intrusion is possible
    - Gates out of service due to damage
    - New temporary gates
- Additional measures for systems with entrances that do not close automatically:
  - Chain and lock with key: the key must be traceable (comprehensive list of users)
  - Code system (not recommended): single use or frequent change of the code

Recommendations

- Visual indication that the gate/door is open
- Anti-tailgating system with 2 barriers or road blocks to stop vehicles
- Gates and doors that close automatically or sound an alarm if left open
- Good practice:
  - *Automatically activating or pointing cameras at specific doors/gates when they open.*
  - *Fast gates that close immediately after a vehicle passes through*
  - *Magnetic contact that triggers an alarm in the access control room when doors/gates are in an abnormal open position*
- Automatic intrusion alarm
- International standard for gates and doors → *See "Loss Prevention" and "US Certification" in the "Fence" standard.*
- Code system: single use or daily/weekly code change, depending on the importance and criticality of the terminal.

Main Access Gates

Minimum

- There is a communication tool and/or a contact number at the main gates that are not manned 24/7.

Recommendations

- Refused trucks, people and cargo can easily leave the main entrance (without entering the site and without obstructing other traffic).

Barriers

Minimum

- Barriers are long enough to prevent entry/exit by foot or car.
- Barriers have access restrictions above and below (sufficiently low and high).
- Barriers are under physical or camera surveillance.
- The entrance/exit is locked with a gate outside of operating hours.
- The barrier control box must be connected directly to the fence.

Turnstiles

Minimum

- An anti-passback system for turnstiles with a badge system
  - *Note: an anti-passback system is not possible on turnstiles with a loop/sluice-gate system that opens the turnstiles*
- Turnstiles must be set up so that only 1 person can enter/exit after identification.
- Prevent the turnstiles from being used as ladders for entry/exit.

Recommendations

- Place a fixed part in the turnstile so that no one can enter and exit at the same time
- The turnstile must be under camera surveillance

Railway Gates

Minimum

- No large opening at the bottom of the railway gate (e.g.: install a metal bar to prevent people from crawling underneath)
- Active monitoring system (see general principles) for the railway gate at all times during operating hours
- Open the gate as late as possible
- Close the gate as soon as the train has passed

Recommendations

- The controls for opening and closing the railway gate are located at the facility (not at the railway operator).

Emergency Gates (Safety Programme)

Minimum

- There is a procedure for the emergency services to gain access
- Emergency gates are marked
- Facilities that are not manned 24/7 must provide the emergency services with a 24/7 contact number.
- The accuracy and accessibility of the contact number should be checked frequently.

Recommendations

- There is an alarm system or light for emergency gates to indicate security.

Doors, etc.

Minimum

- Provide procedures, key management and regular checks on the locking of (other) doors, e.g.: warehouse doors on the outside of the perimeter, pedestrian doors, manual doors, bicycle access, etc.
- Perimeter doors can only be opened by authorised persons.

Gates or Doors That Are Not or Rarely Used

Minimum

- Gates and doors not in use are permanently closed and locked
- Overview of who can open/close (only authorised persons) + key management
- Frequent closure checks

Damaged Gates or Doors

Minimum

- Immediate repair with a temporary solution, depending on the damage

Recommendations

- Establish SLA's with the supplier and/or your own technical service;
  - Provide your own (technical) service with repair and replacement materials; or
  - Establish a contract with an external company
- Physical control or guard at the entry/exit point
- Close the entry/exit point

Exceptions

- Construction zones: arrangements must be made with the competent authority and converted into an addendum or temporary procedure to the PFSP.
- Public quays, waiting quays, bulk terminals (see Perimeter Standard) may be exempted through the PFSA established by the competent authority.

2.3 References

See the ISPS Perimeter and Fence Standard

3. Access Control

3.1 Aim

Port facilities should be entered and exited through controlled entrances. The access control system supports the access control process by distinguishing between 'authorised' and 'unauthorised' persons*, but also by maintaining an accurate and real-time overview of who is currently present in the facility.

Throughout the entire (digital/physical) access control process, it's important to always be vigilant and not accept everyone 'blindly'.

Notes:

- Definition of 'un/authorised': see 'Authorisation' standard.
  Carrying out "access control" is subject to other regulations, in some situations it's better to use "access procedures".
- Performing an "identity check" is also strictly regulated, it is better to use "identity verification".

3.2 Standard

Access Procedure

Minimum

- Pre-registration for all
  - Pre-registration and registration for all types of facilities
  - Exemptions from pre-registration:
    - Special exemption for priority emergency services
    - Exemption for authorities (registration only): in accordance with national policy
    - Exemption for crew and welfare & trade (registration only) cfr. ISPS Code A/16.3.15
    - Exemption for *waiting berths;* based on the PFSA an exemption may be granted for waiting berths. In this case, the responsibility for access is transferred to the ship, in combination with other security measures such as camera surveillance, etc.
  - There is coordination between the facility and the ship regarding pre-registration and access for ship supplies, repairs, visitors, etc.
- Access registration at ENTRY and EXIT for:
  - Persons; incl. co-drivers, own personnel
  - Vehicles (not specific to/owned by the facility)
- An up-to-date attendance list must be available at all times
- Registered data**:** always check national law/GDPR

	Antwerp	Rotterdam	Hamburg
Persons	• Date and time of entry/ exit • Full name • National Registration Number *(Belgians)* • Date of birth, nationality and address *(non-Belgians)* • Email (optional) • Company name • Reason for visit • Biometric data (by law!) • Photo check (optional)	• Date and time of entry/ exit • Full name • Email (optional) • Company name • Reason for visit AIM – Register: ID Number (nationals), Date of birth or passport number (foreign nationals)	• Date and time of entry/ exit • Full name • Email (optional) • Company name • Reason for visit AIM – Register: ID Number (nationals), Date of birth or passport number (foreign nationals)
Crew	• Mandatory registration when leaving or entering the terminal • The police have the crew list (= Schengen Control) • Seaman's book or passport	• Mandatory registration when leaving or entering the terminal • The police have the crew list (= Schengen Control) • Seaman's book or passport	• Mandatory registration when leaving or entering the terminal • The police have the crew list (= Schengen Control) • Seaman's book or passport
Authorities	**Access at all times!** • Date and time of entry/ exit • ID number issued by a government agency (= unique staff number) • Full name (optional) • Photo check (optional)	**Access at all times!** • Date and time of entry/ exit • Full name • Company/Agency name • Email (optional) • Reason for visit	**Access at all times!** • Date and time of entry/ exit • ID number issued by a government agency (= unique staff number) • Check agency badge • Full name (optional)
Pilots/Nautical Service Providers	**Access at all times!** **(Defined group)** Registration on ENTRY AND/OR EXIT • Date and time of entry/ exit • Full name • Company name • Reason for visit	**Access at all times!** **(Defined group)** Registration on ENTRY AND/OR EXIT • Date and time of entry/ exit • Full name • Company name • Reason for visit	**Access at all times!** **(Defined group)** Registration on ENTRY AND/OR EXIT • Date and time of entry/ exit • Full name • Company name • Reason for visit

	Antwerp	Rotterdam	Hamburg
Vehicles	• **General:** Registration number + country • **Intervention vehicle (emergency):** Registration number + number of persons in vehicle • **Truck:** Registration number + country truck (not trailer)	• **General:** Registration number + country • **Intervention vehicle (emergency):** Registration number + number of persons in vehicle • **Truck:** Registration number + country truck (not trailer)	If required by the PFSA
Exemption for Guided Bus Tours	Simplified process agreed in advance with the tour organiser: • Registration of all required details of the guide and bus attendants • Registration of the name and surname of everyone on the bus, including the driver • Everyone must have their ID with them These rules apply when no one leaves the bus. As soon as any other form of visit takes place, all required data must be registered for everyone.	Simplified process agreed in advance with the tour organiser: • Registration of all required details of the guide and bus attendants • Registration of the name and surname of everyone on the bus, including the driver • Everyone must have their ID with them These rules apply when no one leaves the bus. As soon as any other form of visit takes place, all required data must be registered for everyone.	Simplified process agreed in advance with the tour organiser: • Registration of all required details of the guide and bus attendants • Registration of the name and surname of everyone on the bus, including the driver • Everyone must have their ID with them These rules apply when no one leaves the bus. As soon as any other form of visit takes place, all required data must be registered for everyone.

- Data retention period:
  - Current access data:
    - RTD : 6M, same as for visitors to national government buildings.
    - ANT : max. 10Y, to be included in the PFSP
    - HMB : 14D in accordance with GDPR,
  - Recommendation to follow at least the telecom data retention period:
    - NL : 12M telephone data – 6M internet data
    - BE : 12M telecom data
    - GE: 4-10W telecom data

- ID verification:
  - Identification is done by means of government-recognised identification documents.
  - Badges are issued after an ID verification
  - Ensure unambiguous ID verifications and obtain proof that the person in question is entitled to apply for a badge.

Recommendation

- Examples of identification documents: identity card, passport, seaman's book, etc.
  - A driving licence is an official ID and is accepted in RTD and HMB
  - A driving licence is not an official ID in BE
- If so agreed between the terminal and the authority/emergency services, emergency badges or access cards (badges) with special rights may be used.
  - Badges for intervention services must be requested via the relevant HR department (not personal)
- An automatic link between work schedules and the access control system (e.g.: dock workers)
- Visitors must provide a contact person
- Waiting berths: there is camera control on the waiting quays to monitor the (open) access
- How to carry out an unambiguous ID check:
  - Trained personnel to critically check people and documents
  - Ask for identification
  - Compare name and photo with the person physically registering
  - Use biometrics

Access Tools and Management

There are many different access tools available. As an organisation you choose the system that best suits your operational processes.

General Access Principles

- Use access tools that meet the above-mentioned minimum requirements.
- Use the access tools correctly.
- Badges and codes are for personal use only.

Access Management Principles

- Time and place restrictions must be optimally integrated
  - Use time slots (for badges visitors, trucks etc.)
- The access control system must be current and up to date.
- Implement restrictions to prevent misuse of codes/badges.
- Restricted areas are equipped with a badge system or keys with a controllable key management system.
- It's recommended to connect the access control data to a central database *(in accordance with GDPR)*

Technical Access Principles (recommendations)

- Badges (permanent/temporary):
  - An anti-passback system for entrances with a badge system
  - Visible data on badge: full name, company, photo, expiry date (permanent)
  - Strongly recommended data: biometrics (permanent)
- Codes: renewal process
  - Code system only allowed for **non-sensitive terminals or non-sensitive locations/ opportunities**
  - Single use or change the code daily or weekly, depending on the importance and criticality of the terminal/location
  - Frequency of code changes can be determined by the PFSA
- Manual logbook:
  - Check the details provided by each person
    - Ask for identification
    - Check for correct name, date and time
    - Must be legible
  - Ensure registration is completed on exit.
  - Respect the privacy of the previously registered persons (= GDPR)
- Other tools: ANPR (Automatic Number Plate Recognition) at express gates
  - Who: intervention vehicles and own staff
  - It must be possible to trace the identity of the driver (and passengers).

Access Control Monitoring

Minimum

- The PFSP describes detailed measures for all means of access
  - Additional note: the access procedure in the PFSP and the evacuation procedure are co-ordinated
- Provide a manual with the access control tasks for staff at the entrance.
- Establish a monitoring process; carry out regular checks on:
  - the system, whether it's digital or paper-based;
  - the correct human execution of the access control procedure.
- Monitor the entrances
  - Physical (security guards or other personnel)
  - Cameras
- Create security awareness
  - Organise regular briefings or training sessions
    - Correct use of the access control system and procedures
    - Be aware of and alert to suspicious situations
    - Internal reporting and analysis of all access control violations:
      - E.g.: misuse of the access control system, failures, any unauthorised access, etc.

- Organize 1 quarterly ISPS drill on access control each year .
- Proper access control is everyone's responsibility

Sanctions

Minimum

- Establish house rules *(see references)*:
  - Entry/exit other than through the controlled entrances is an offence
  - Deny access as a sanction (e.g.: no registration is no access)
- Report access control breaches to the competent authority:
  - any serious or suspected breach of access control
  - any deliberate or suspicious failure of the access control system

3.3 References

Set of house rules

Rotterdam has worked out a unified set of house rules between the different companies in the port.

Gatekeeper–Community Code of Conduct:

- I will abide by the applicable house and safety rules at the location.
- I will only enter the terminal for a legitimate and lawful purpose. If I have any doubts about the legality of my stay, I will not proceed and will report this.
- It is my duty to exercise due diligence in the assignments I carry out, and to ensure that an assignment does not or cannot conflict with the applicable rules of conduct at the terminal
- I will not conduct or participate in any criminal activity.
- I will not unlawfully bring people or goods onto the site, transport them across the site or remove them from the site.
- I will cooperate with a visitation request.
- I will immediately follow the instructions of (security) personnel at the terminal I am visiting.
- I will immediately report any suspicious or abnormal situations.

4. Authorisation

4.1 Aim

This guideline is a supplement to the Access Control Standard. It aims to clarify the term "(un)authorised" to avoid misinterpretations in practice and explain why this is so important.

4.2 Definition

What does 'Authorised' mean?

Authorised access is subject to a business purpose, time and place.

- You have to be on site for a professional activity/reason.
- Only within the agreed time frame or the time required for the task/job.
- Entry and exit, which may be restricted to certain locations, is only possible with authorisation via the terminal's access procedure (including registration).
- For ISPS port facilities, this applies only to those with legitimate ship or port facility related concerns.

What does 'Unauthorised' mean?

- When people don't meet the above conditions and don't comply with the terminal's access procedures.
- An additional precaution to prevent unauthorised access: don't give permanent access to people or groups who don't need it for their work.

4.3 Guidelines

Basic Principles

- Register everyone as required by the Access Control Standard.
- Authorisation and access tools must be carefully developed, maintained and kept up to date. This is an important investment to ensure that subsequently your access procedure is as effective as possible.
- When reviewing your access control system/procedure, you should also consider its impact on the users (your own staff, service providers, emergency services, visitors, other port users, etc.):
  - Limit the impact on them as well; one uniform access control system can facilitate this.
  - If possible, involve them in the preparations.
- Think carefully about the practical implementation of the definition of 'authorisation'. This applies to digital and paper applications, as well as to the use of codes.

- This guideline is not intended to prescribe technical details. For this, it's best to consult different suppliers to compare the systems they offer and choose the best one for your organisation.

Pre-/registration

- A pre-registration system can facilitate the effective application, identification and registration. Apply this to all contractors, visitors, staff, etc., not just to visitors to ships.
- It's important from both a security and safety perspective that everyone is registered.
- Pre-registration must include the exact individual person, not a group of possible people (exemption for seaman's mission or approved by the competent authority). The list must be thoroughly checked.

Identification

- Make sure that the person in front of you is who they claim to be.
- The use of biometrics can help in this process.

Identifiers

- Means of identification (see Access Control Standard)
- A badge is a personal resource:
  - Implement physical/technical means to prevent misuse
  - Create awareness about this
- Respond to misuse
  Passing on the badge, co-drivers using the driver's badge, etc. are examples of unauthorised access and are not legal!
- So make sure everyone has individual authorisation. Also take into consideration the ship and its crew when they enter the site.
- Don't underestimate the importance of an up-to-date badge/card system.
  Critical implementation of this can really help you meet all the requirements.

Access Control System

- The importance of an access control system with registration on entry/exit (electronic/paper) for security and safety reasons. Remember that paper is difficult to track and check, and also has privacy issues.
- Many different access control systems make it complex, so make good arrangements with users such as: nautical services, emergency services, governments, etc.
- It's good practice to maintain accounts, e.g.: delete inactive users every 2 months, use short expiry dates for badges, etc.
- Consider various centrally controlled solutions

  - At facility level: pre-registration, application, registration, coordination with the ship's ID system, link with staff and third party time/work schedules, etc.
  - At port level: inter-agency and inter-terminal/company network to synchronise and complete (access control) data.
- Test and update the system frequently to ensure it works. Continue to improve your system as well.

Access Levels

- Differentiate between:
  - internal (staff) and external (people)
  - temporary and permanent
  - natural activities: who should have access where, when, and in what order of priority?
- Consider all possible parties: own staff, contractors, dockers, visitors, inspectors, crew, welfare and trade associations, emergency services, technicians, etc.
- Include all different forms of access levels in a procedure to be added to the PFSP.

Execution Control

- Provide very clear instructions, implement them correctly and review them frequently.
- The PFSP must describe all measures for all means of access (see Access Control Standard)
  - Important: the authorisation levels described in the PFSP must be correctly applied in practice; "no paper security".
- Follow up on misuse, sanction e.g.: by:
  - Refusing access (mandatory in accordance with the Access Control Standard);
  - Notifying the (external) person responsible;
  - Notifying the police (depending on the nature of the incident);
  - Reporting to the competent ISPS authority (ISPS incident report).

Legal Issues

- Consider the legal options
  - Who can check an ID? (Private Security Law)
  - Conditions for collecting and processing personal data? (GDPR/Privacy)
  - Other regulations? E.g.: identification law, code or laws of authorities (like customs, police) that include guaranteeing the access of the authorities.

5. Rail

5.1 Aim

To manage rail access to port facilities to minimise unauthorised use or access.
Note: cooperation and good agreements between the company, the railway manager and the cargo operator are essential. It's strongly recommended that good agreements and a security declaration are signed between the port facility and the rail operator (or other parties involved).

5.2 Standard

Railway Access

Minimum

- No large openings at the bottom of the railway gate (e.g.: install a metal bar to prevent people crawling underneath, use concrete blocks).
- It should be impossible to crawl between the fence and the railway gates. The fence must fit closely to the gate (the fence and the gate must comply with the relevant standards).
- Active surveillance of the railway gate at all times when it's open, in accordance with the general principles.
  - General principles: a 24/7 surveillance system for each operational entry/exit point; either
    - physically; or
    - with cameras.
- Open the gate as late as possible.
- Close the gate as soon as the train has passed.
- If the gate must remain open for longer, additional measures must be taken (camera surveillance with intrusion alarm, physical presence, etc.)
- Lighting at each train gate.
- Staff security awareness when the train gate is open.
- Include the railway gate in the perimeter patrol.
- Report anomalies to the competent authority.

Recommendations

- Visual sign that the gate is open (e.g.: red/orange light or a signal in the operator/security room).
- Automatic closing system when the gate is open and there is no train/wagon.
- Automatic intrusion alarm.

- Implementation of a 'smart' camera system to prevent intruders from gaining access to the terminal site with or along the train.
- For large and wide areas: additional cameras if there are no other surveillance systems.
- Additional solutions/procedures if gates are often left wide open due to heavy traffic (e.g.: smart camera, intrusion detection, physical presence, etc.)
- Take into account that:
  - (New) camera systems are not always technically sufficient.
  - VCA (Video Content Analysis) cameras fail on several levels.
  - Trains easily cause poor visibility and blind spots:
    - Cameras don't show all details in combination with a train; 2 cameras may be needed.
    - Position the camera close enough to the rail entrance to get good image quality.
    - Use additional infrared cameras.
  - VCA (Video Content Analysis) cameras fail on several levels

Access Procedure

Minimum

- Pre-registration of estimated time and wagon/goods information
  - The railway operator is known.
  - The names of persons entering the terminal through the rail gate must be verifiable.
    - By means of a fixed list/approval list of employees provided by the railway operator (including engine drivers, inspectors, supervisors, and others).
    - *Optionally include: function, date of birth, etc.*
  - The date and approximate time of arrival.
  - Wagon/goods information:
    - Number of wagons, which goods/products.
    - Not necessary if arriving/departing empty.
- Organisation of access registration at ENTRY and EXIT:
  - A call or other notification (e.g.: intercom) before arrival (to the terminal, the guard, etc.).
  - The terminal (guard) checks the name against the list *and/or* registers the name in a system (always or randomly).
  - The terminal (guard) checks the reason (planned activity).
  - The terminal (guard) registers the time of ENTRY and EXIT.
  - The terminal is responsible for the access control to the terminals, i.e. also for the opening/closing of the rail gate.
  - The terminal (guard) monitors all access and movements digitally or physically.
  - The automatic rail gate systems (with sensors) must be equipped with additional security measures such as: cameras, an alarm if the system doesn't work, a special access control/registration procedure, etc.

Recommendations

- Schedule train activities at quiet times/at night/at specific hours/on weekends/ on demand, etc.

Others

Minimum

- Inspection of the cargo, e.g.::
  - Container number, seals, damage, integrity of the goods.
  - Visual or manual inspections are checked against the system.
- Random inspections of empty containers for suspicious contents (as they enter/leave the terminal).
- Random inspections of wagons.
- Reporting of anomalies and security incidents relating to rail, rail entry/exit, cargo, trains and loaders, unauthorised access, etc.
- A clear procedure in the PFSP for the access, inspection and handling of goods by rail.

Recommendations

- Prohibit wagons from being left unattended outside the terminal. If this is not possible, alternative solutions/rules must be provided:
  - A holding track with lighting, permanent camera surveillance or physical surveillance. The holding track can be the section of track in front of the entrance.
  - The creation of an enclosed holding track.
- An electronic registration system of the wagons as they pass through the ISPS area (an RFID reader to detect and verify the wagon numbers upon entry).
- A 100% visual inspection of empty containers as they enter/leave the terminal.
- The development of an additional procedure to check the train cargo before and during departure:
  - Additional cargo inspection.
  - Monitoring of the train entering and leaving the facility.
  - Provision of a rapid response procedure when anomalies are detected during exit.
- Also monitor the tracks (at sensitive spots) instead of just the access.
- The agreement between the facility and the operator must include the responsibility of the railway manager, the operator and the train driver in the event of non-compliance (for not following the rules).

6. Standard Vehicle Control

6.1 Aim

To maintain an overview of which (external) vehicles are within the perimeter of the facility and to prevent vehicles from being misused to smuggle unauthorised people or materials in and/or out of the facility.

- IN is mandatory for ISPS
- OUT is mandatory if required by the PFSA

6.2 Standard

Vehicle Access

Minimum

- Compliance with the Access Control Standard – registration on entry and exit: time, driver, registration number + country of each vehicle.
  - Registration number is mandatory if required by the PFSA.
- Add random vehicle checks.

Recommendations

- Basic specification of the vehicle checks at security levels 1, 2 and 3.
  - Frequency of the checks
- Creation of a separate area (vehicle check zone) where vehicles can be checked.
- Control methods:
  - External technical vehicle inspection
  - Use of a mirror
  - Counting of all occupants
  - Search for suspicious materials
- Aim to minimise external vehicle access to the facility.

Truck Access

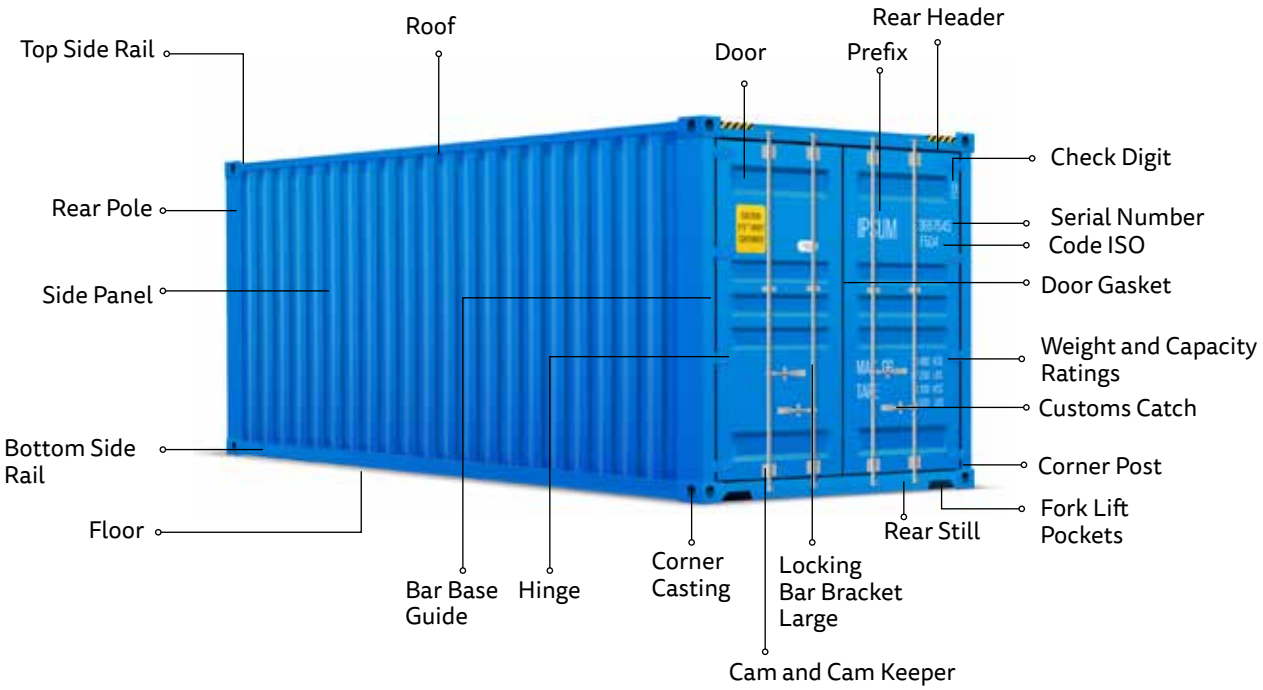
Minimum

- Compliance with the Access Control Standard. Registration on entry and exit: time, driver, registration number + country of each truck (not trailer).
  - Registration number is mandatory if required by the PFSA.
- Check against the loading/unloading documents.
- Check the seals and hinges

Recommendations

- 7-point container inspection: front door, left side, right side, floor, ceiling/roof, interior/exterior doors, bottom

- Extra elements of a container:



- Use detection devices such as:
  - Scanners
  - CO_2 meters
  - Dog control (K9)

Vehicle Repair

Minimum

- Compliance with the Access Control Standard – registration on entry and exit: time, driver, registration number + country of each delivery vehicle.
  - Registration number is mandatory if required by the PFSA.
- Randomly ask to open the cargo/loading space and take a quick look.

Recommendations

- Carry out a detailed check as an ISPS drill in cooperation with the ship security officer and the supplier.

Movements on Site

Minimum

- Monitor the movements on the site.
- Provide clear and pre-defined driving routes and stopping/parking areas on the site.
- Monitor abnormal driving behaviour and stops at abnormal locations.

Recommendations

- Provide guidance for specific vehicles or in specific risk areas of the facility.
- Use detection (cameras) for restricted areas.

7. Practical checklist

7.1 ISPS Perimeter and Fence

7.1.1 Perimeter

7.1.1.1 Aim

The establishment of a clear boundary of a secure area, where security rules must be observed by all port users and where the port facility is responsible for exercising its security responsibilities.

7.1.1.2 Questionnaire

ISPS Perimeter		YES	NO	N/A
1.	Is the ISPS perimeter defined by the competent authority in the PFSA?	☐	☐	☐
	Comment			
2.	Is the entire corporate site defined as an ISPS perimeter?	☐	☐	☐
	Comment			
3.	Is the perimeter completely closed to prevent unauthorised access?	☐	☐	☐
	Comment			

Exceptions		YES	NO	N/A
4.	Is the definition of the ISPS perimeter restricted to part of the corporate site?	☐	☐	☐
	Comment			
5.	Is the restriction of the ISPS perimeter justified by the geographical location of the port facility or its low-risk activities?	☐	☐	☐
	Comment			
6.	Have additional security measures been taken around the restricted ISPS perimeter?	☐	☐	☐
	Comment			

7.1.2 Fence

7.1.2.1 Aim

The fence is a barrier to prevent unintentional unauthorised access and delay intentional intrusion. The fence may also be replaced by an equivalent alternative construction, such as a concrete wall. This alternative construcion must be tested and approved by the competent authority. Transitional period: this standard applies to new or replacement fencing. The competent authority may also decide that the facility must install new or modified fencing earlier.

7.1.2.2 Questionnaire

Fence		YES	NO	N/A
1.	Is the total height of the fence at least 2.40 metres?	☐	☐	☐
	Explanation The anti-scaling protection is an extra section on top of the 2.40m fixed construction. The competent authority may grant exemptions for safety reasons			
	Comment			
2.	Is the fence buried in or anchored to the ground in several places? Or is the fence fitted with an impenetrable tension wire at the bottom?	☐	☐	☐
	Comment			
3.	Is there room to crawl under the fence and/or gate?	☐	☐	☐
	Explanation The fence should be close to the ground and gates. And/or the access point is permanently manned or under CCTV surveillance.			
	Comment			

Fence (recommendations)		YES	NO	N/A
4.	Are there concrete jersey blocks in front of the fence?	☐	☐	☐
	Explanation This security measure can serve as a substitute for anchoring the fence.			
	Comment			
5.	Does the fence have three rows of barbed wire at the top?	☐	☐	☐
	Comment			

6.	Is the fence equipped with detection devices at critical points?	☐	☐	☐
	Explanation For example, smart alarm, voltage, etc.			
	Comment			
7.	Is the fence double-layered?	☐	☐	☐
	Comment			
8.	Is the fence cut-resistant?	☐	☐	☐
	Comment			
9.	Is the fence made of non-corrosive materials?	☐	☐	☐
	Comment			

Mobile Fence		**YES**	**NO**	**N/A**
10.	Is the mobile fence reinforced with concrete blocks or anchored to the ground?	☐	☐	☐
	Comment			
11.	Are the elements of the fence joined together at two points with at least 2 solid bolted clips?	☐	☐	☐
	Explanation The use of containers can be an equivalent alternative.			
	Comment			
12.	If a physical barrier cannot be installed, is there permanent supervision by a (security) employee?	☐	☐	☐
	Comment			

Mobile Fence (Recommendations)		**YES**	**NO**	**N/A**
13.	Is there additional surveillance by means of cameras or security personnel (at critical points)?	☐	☐	☐
	Comment			
14.	Are there additional security measures in place, based on the port facility's business activities?	☐	☐	☐
	Comment			

Perimeter Waterside		YES	NO	N/A
15.	Is the fencing on the waterside secured and equipped with anti-scaling protection?	☐	☐	☐
	Explanation Possible security measures: extended fencing, barbed wire, steel plate or a similar construction.			
	Comment			
16.	Does the physical barrier on the waterside provide sufficient security at low tide?	☐	☐	☐
	Comment			
17.	Is there any supervision (human or digital) of the facility's waterside boundary?			
	Comment			

Perimeter Waterside (recommendations)		YES	NO	N/A
18.	Are ships moored within the port facility's perimeters?	☐	☐	☐
	Comment			
19.	Are external bollards secured when the mooring lines extend beyond the port facility's perimeter?	☐	☐	☐
	Explanation Additional measures for and/or in cooperation with the ship. An agreement must be drawn up (in the PFSP) for mooring lines laid across neighbouring facilities.			
	Comment			

Perimeter Control		YES	NO	N/A
20.	Are the perimeter surveillance rounds proportionate to the port facility's security risks?	☐	☐	☐
	Comment			
21.	Are the surveillance rounds logged and are these logs reviewed by the PFSO?	☐	☐	☐
	Comment			
22.	Does the PFSO report deliberate damage as a security incident to the competent authority?	☐	☐	☐
	Comment			

Perimeter Control (recommendations)	YES	NO	N/A
23. A high-risk port facility checks its perimeter at least once a day, and a low-risk port facility at least once a week.	☐	☐	☐
Comment			
24. If a port facility has smart fencing it is advisable to check the operation of the system on a daily basis, both from the control room and on foot.	☐	☐	☐
Comment			
25. Use of fixed tag points and additional control points, possibly with live locator or GPS tracking.	☐	☐	☐
Comment			
26. Camera & video surveillance: fixed cameras on weak/blind spots; include the perimeter in the 'camera sweep'; the use of drones for perimeter surveillance.	☐	☐	☐
Comment			
27. Extra lighting when visibility is poor to enhance camera quality and staff safety.	☐	☐	☐
Comment			

Repair Damaged Fence	YES	NO	N/A
28. Is there a procedure in place to ensure that damaged fencing is repaired immediately or a temporary solution is put in place?	☐	☐	☐
Comment			

Repair Damaged Fence (recommendations)	YES	NO	N/A
29. Will extra surveillance (guard, camera) be organised if the fence is damaged?	☐	☐	☐
Comment			
30. If a port facility has smart fencing, it is advisable to check the operation of the system on a daily basis, both from the control room and on foot.	☐	☐	☐
Comment			

31.	Does the port facility have Service Level Agreements with a company that will repair the fencing if it's damaged?	☐	☐	☐
	Comment			

No Obstacles		YES	NO	N/A
32.	Is there a procedure in place to ensure that damaged fencing is repaired immediately or a temporary solution is put in place?	☐	☐	☐
	Comment			
33.	Have additional security measures been taken to prevent people from climbing in if there are immovable objects near the fence?	☐	☐	☐
	Comment			

No Obstacles (recommendations)		YES	NO	N/A
34.	For movable obstacles: a minimum distance of 2 meters is recommended	☐	☐	☐
	Comment			
35.	For immovable obstacles: a higher fence, extra barbed wire, intrusion detection camera, etc.	☐	☐	☐
	Comment			
36.	For obstacles in a public space: request additional measures from the local authority, such as a parking ban (if possible)	☐	☐	☐
	Comment			
37.	No natural wild growth and trees; except as an additional safety barrier (e.g.: thorny bushes)	☐	☐	☐
	Comment			
38.	Follow the height of the terrain; on a hill the fence must go up	☐	☐	☐
	Comment			

7.2 Gates

7.2.1 Target

Gates are an entry point in the closed perimeter where people can gain authorized access (cfr. standard "access control and authorization") and where unauthorized access is prevented.

7.2.2 Questionnaire

General Principles Gates	YES	NO	N/A
1. Is it possible to lock the gates in a closed position?	☐	☐	☐
Comment			
2. Do you monitor the authorized acces on gates/doors during opening an closing? How?	☐	☐	☐
Comment			
3. Do you monitor the gates/doors that are constantly open? How?	☐	☐	☐
Comment			
4. Is there a barrier between gate and fence?	☐	☐	☐
Comment			
5. Is there a lighting system close to the access point?	☐	☐	☐
Comment			
6. Do you have visible "ISPS-sign" or "only authorized people" for each entry/exit point? what?	☐	☐	☐
Comment			
7. Do you have a anti-pass back System/ Code system ?	☐	☐	☐
Comment			
8. Do you have a 24/7 monitoring for each entry/exit point? How?	☐	☐	☐
Comment			

9.	Do you have a Geographic map in the PFSP with indication of entire perimeter/ entries / cameras?	☐	☐	☐
	Comment			
10.	Do you monitor the authorised acces on gates/doors during opening an closing? How?	☐	☐	☐
	Comment			
11.	Do you drill the staff on security awareness ?	☐	☐	☐
	Comment			
12.	Do you report anomalies to the competent authority?	☐	☐	☐
	Comment			
13.	Do you report all Doors/ Gates out of service to the competent authority?	☐	☐	☐
	Comment			

General Principles Gates (recommendations)		**YES**	**NO**	**N/A**
14.	Do you have visual sign that the gate/door is open? What kind of sign?	☐	☐	☐
	Comment			
15.	Do you have anti-tailgating locks with 2 barriers or road blocks to stop vehicles (can also be useful for vehicle control)?	☐	☐	☐
	Comment			
16.	Are the gates and doors closed automatically or do they generate an alarm when they stay open?	☐	☐	☐
	Comment			
17.	Do you have an automatic intrusion detection alarm?	☐	☐	☐
	Comment			

Main Access Gates	YES	NO	N/A
18. Do you have a communication tool and/or contactnumber at the main gates where there is no 24/7 attendance?	☐	☐	☐
Comment			

Main Access Gates (recommendations)	YES	NO	N/A
19. Can refused trucks, people & cargo easily leave the main entrance (without entering the site and without causing traffick jam)?	☐	☐	☐
Comment			

Barriers	YES	NO	N/A
20. Are the barriers long enough to prevent entrance/exit by foot or car?	☐	☐	☐
Comment			
21. Do the barriers have over- and under climb protection (low and high enough)?	☐	☐	☐
Comment			
22. Is there a physical or camera monitoring of the barriers?	☐	☐	☐
Comment			
23. Is the entry/exit closed with a gate outside operational hours?	☐	☐	☐
Comment			

Turnstiles	YES	NO	N/A
24. Do you have an anti-pass back system for gates with badge system?	☐	☐	☐
Comment			
25. Are the turnstiles set in such a way that only 1 person can enter/exit after identification?	☐	☐	☐
Comment			
26. Can you prevent that the barriers are being used as ladders to climb in or out?	☐	☐	☐
Comment			

Turnstiles (recommendations)	YES	NO	N/A
27. Is the turnstile designed in such a way that no one can get in or out at the same time?	☐	☐	☐
Comment			
28. Is there already camera surveillance at the turnstile (already mandatory in the surveillance of the operational entrance)?	☐	☐	☐
Comment			

7.3 Access Control

7.3.1 Target

Entry and exit from port facilities should be through controlled entrances. The access control system supports the access control process, in distinguishing 'authorized' and 'unauthorized' persons (*see standard), but also in maintaining an accurate and real-time overview of who is currently at the facility. In the whole (digital/physical) access control process, it's important to be always vigilant and not to accept everyone 'blindly'.

7.3.2 Questionnaire

Access Procedure		YES	NO	N/A
1.	Is everyone registered?			
	Comment			
2.	Is everyone pre-registered?	☐	☐	☐
	Comment			
3.	Are following services exempted from pre-registration?	☐	☐	☐
	→ Special exception for priority emergency services	☐	☐	☐
	→ Authorities (only registration) conform national policy	☐	☐	☐
	→ Crew, welfare and trade (only registration) cfr. ISPS A/16.3.15	☐	☐	☐
	→ Waiting berths (if an exception is motivated by the PFSA)	☐	☐	☐
	Comment			
4.	Is there coordination between facility and ship with regard to pre-registration and access for ship supplies, repairs, visitors?	☐	☐	☐
	Comment			
5.	Is there access registration IN **and** OUT for:	☐	☐	☐
	→ Persons (incl. co-drivers, own personnel)	☐	☐	☐
	→ Vehicles (not specific to or owned by the facility)	☐	☐	☐
	Comment			

6.	Is an actual attendance list available at all times? SHOW							☐	☐ ☐
	Comment								
7.	What data is registered?								
	Persons	Date and hour in/out ☐	Full name ☐	National Register Nr or date of birth ☐	Email ☐	Company ☐	Reason for visit ☐	Biometric data ☐	Photo check ☐
	Crew	Leaving / entering facility ☐	Seaman's book or passport ☐	Police has crew list ☐					
	Authority (always access!)	Date and hour in/out ☐	Unique staff number ☐	Full name ☐	Company / Service ☐	Email ☐	Reason for visit ☐	Check badge service ☐	Photo check ☐
	Pilots/Nautic Service Providers (always access!)	Date and hour in AND/ OR out ☐	Full name ☐	Company ☐	Reason for visit ☐				
	Vehicles	General: license plate + land ☐	Emergency: license plate + number of persons in vehicle ☐	Trucks: license plate + land truck (not trailer) ☐					
	Guided bus tours (simplified) arrangement)	N/A ☐	All data from guide and attendants bus ☐	Sur/name of everyone on the bus incl. driver ☐	Everyone must have their ID with them ☐	All data is registered when people leave the bus ☐			
	Comment								
8.	Is data kept? What is the data retention period (open question)							☐	☐ ☐
	Comment								
9.	How is ID-verification performed?								
	→ By means of ID-documents accepted by the government?							☐	☐ ☐
	→ Are badges issued after ID-check?							☐	☐ ☐
	→ Is unambiguous ID-check ensured? PROOF							☐	☐ ☐
	Comment								

Access Procedure (recommendations)	YES	NO	N/A
10. Is there a list of the official identification documents? EXAMPLE	☐	☐	☐
Comment			
11. Are there agreements between terminal and authority/emergency services to gain access? E.g.: use of general track cards, emergency badges,... (via HR)? EXPLAIN	☐	☐	☐
Comment			
12. Is there an automatic link between work schedules and the access control system?	☐	☐	☐
Comment			
13. Are visitors obliged to provide a contact person?	☐	☐	☐
Comment			
14. Is there camera control on the waiting quays to monitor open access?	☐	☐	☐
Comment			
15. How is unambiguous ID-check performed at the entrance	☐	☐	☐
→ Personnel is trained to check people/documents critically?	☐	☐	☐
→ They ask for the identity	☐	☐	☐
→ They compare name/photo of the people who signs up	☐	☐	☐
→ The port facility uses biometrics	☐	☐	☐
Comment			

Access Tools and Management (principles)	YES	NO	N/A
16. Does the access tools fulfill the above minimum? EXPLAIN	☐	☐	☐
Comment			
17. Is there a correct use of the access tools? PROOF	☐	☐	☐
Comment			

18.	What does the facility do to ensure strict personal use of badges and codes? EXPLAIN and PROOF	☐	☐	☐
	Comment			
19.	Is the access control system actual and up to date?	☐	☐	☐
	Comment			
20.	Are there restrictions implemented to prevent misuse of codes/badges?	☐	☐	☐
	Comment			
21.	Are restricted areas equipped with a badge system/keys with a controllable key management system?	☐	☐	☐
	Comment			
22.	Is the access control data connected with a central database? (recommendation)	☐	☐	☐
	Comment			
23.	Badges (permanent/temporary)			
	→ Is there an anti-pass back system (for entrances with badge system)?	☐	☐	☐
	→ Is there visible data on the badge? Which? EXPLAIN	☐	☐	☐
	→ Does the facility use biometrics? (recommendation)	☐	☐	☐
	Comment			
24.	Codes and renewal process			
	→ Are code-systems only used at *non sensitive* locations?	☐	☐	☐
	→ Is single use of codes assured?	☐	☐	☐
	→ Is longer usage time of codes analyzed according criticality?	☐	☐	☐
	→ Is the frequency of code replacement determined by PFSA?	☐	☐	☐
	Comment			

25. Manual logbook			
→ Is the data that each person writes checked? Name, date, time,...	☐	☐	☐
→ Is there a control on the OUT-registration? PROOF	☐	☐	☐
→ Is the privacy of previous registered persons respected?	☐	☐	☐
Comment			
26. Other tools like ANPR (Number Plate Recognition) at fast gates: is it possible to trace the identity of the driver?	☐	☐	☐
Comment			

Access Control Supervision	**YES**	**NO**	**N/A**
27. Does the PFSP describe detailed measures for all means that provide access?	☐	☐	☐
Comment			
28. Is there a manual with the access control tasks for the personnel at the entrance?	☐	☐	☐
Comment			
29. Is a supervision process implemented, with regular checks on the access control system (digital/paper) and the correct human execution of the access control procedure?	☐	☐	☐
Comment			
30. Are all the entrances monitored?			
→ Physical (security guard or other personnel)?	☐	☐	☐
→ Camera's	☐	☐	☐
Comment			
31. How does the facility create security awareness?			
→ Organisation of regular briefings/trainings? Correct use of systems/procedures, attention for suspicious situations, report and analyze breaches	☐	☐	☐
→ Organization of 1 quarterly drill on access control every year	☐	☐	☐
→ People are reminded on their responsibility for access	☐	☐	☐
Comment			

Sanctions	YES	NO	N/A
32. Does the facility have a set of house rules with:			
→ Entering/exiting through controlled entrances is an offence	☐	☐	☐
→ Sanctions like: no registration = no access; deny access as a sanction in case of misuse	☐	☐	☐
Comment			
33. Does the facility report breaches on access control?			
→ any serious or suspicious breach of access	☐	☐	☐
→ Intentional or strange failure of the access control system	☐	☐	☐
Comment			

7.4 Authorisation

7.4.1 Target

This guideline is an addition to the standard "access control". It aims to create clarity in the term "un/authorised" to avoid misinterpretations in practice and to motivate why this is so important.

7.4.2 Questionnaire

Definition	YES	NO	N/A
1. Are persons only allowed access for professional reasons?	☐	☐	☐
Comment			
2. Is access only granted for the time necessary for the professional activity?	☐	☐	☐
Comment			
3. Can access only be obtained after correct legitimation and registration?	☐	☐	☐
Comment			
4. These professional activities are only ship or terminal related?	☐	☐	☐
Comment			
5. What do you see as unauthorized access? EXPLAIN	☐	☐	☐
Comment			
6. Which persons have permanent access? EXPLAIN	☐	☐	☐
Comment			

Basic Principles	YES	NO	N/A
7. Are tools/systems that provide access well maintained and up to date?	☐	☐	☐
Comment			
8. Did you carry out an analysis of the access procedure and systems before? EXPLAIN and/or PROOF	☐	☐	☐
Comment			

9.	When is someone 'authorised' to use the following tools: digital application, paper registration, use of code, a key.... Explain also how you prevent misuse of (paper) registration.	☐	☐	☐
	Comment			

Pre-/Registration		YES	NO	N/A
10.	Must all people pre-register? Which persons not? EXPLAIN	☐	☐	☐
	Comment			
11.	Does pre-registration contain an individual? Not an entire list of possible people.	☐	☐	☐
	Comment			
12.	Can you assure that everyone is registered? EXPLAIN	☐	☐	☐
	Comment			

Identification		YES	NO	N/A
13.	How do you check that the person in front, is the person who he or she claims to be?	☐	☐	☐
	Comment			
14.	Do you use biometrics?	☐	☐	☐
	Comment			

Identifiers		YES	NO	N/A
15.	Do you guarantee that badges are used personally? HOW?	☐	☐	☐
	Comment			
16.	Do you guarantee that each person has an individual authorisation? Also explain how you deal with ship and crew.	☐	☐	☐
	Comment			

Access Control System		YES	NO	N/A
17.	Are there access control agreements with users like: nautical services, emergency services, governments,...?	☐	☐	☐
	Comment			

18.	Are badges set to inactive? WHEN	☐	☐	☐
	Comment			
19.	Is the access control system centralised? EXPLAIN	☐	☐	☐
	Comment			
20.	Do you test the access control system? How often? EXPLAIN	☐	☐	☐
	Comment			

Access Levels		**YES**	**NO**	**N/A**
21.	Is there a difference in the access level? (in/external) EXPLAIN	☐	☐	☐
	Comment			
22.	What are the different access categories?	☐	☐	☐
	Comment			
23.	Is everything described in detail in the PFSP? PROOF	☐	☐	☐
	Comment			

Execution Control		**YES**	**NO**	**N/A**
24.	Are the access instructions clear? PROOF	☐	☐	☐
	Comment			
25.	Are the access procedure instructions executed correctly? How do you check for it (no paper security)?	☐	☐	☐
	Comment			
26.	What's the consequence of abuse?	☐	☐	☐
	Comment			

Legal		**YES**	**NO**	**N/A**
27.	Did legal check your access control procedure/system? Is it conform with private security law, GDPR, other...?	☐	☐	☐
	Comment			

7.5 Rail

7.5.1 Target

Manage rail accesses of port facilities to minimize unauthorized use or access. Collaboration and good agreements between company, railway manager and cargo operator are essential.

7.5.2 Questionnaire

Railway Access	YES	NO	N/A
1. How many rail gates do you have?	☐	☐	☐
Comment			
2. Do you monitor the gates during opening and closing? How?	☐	☐	☐
Comment			
3. Is there a barrier between gate and rail?	☐	☐	☐
Comment			
4. Is there a barrier between gate and fence?	☐	☐	☐
Comment			
5. Is there a lighting system near the access?	☐	☐	☐
Comment			
6. Did you drill the staff on awareness rail?	☐	☐	☐
Comment			
7. Do you report anomalies to the competent authority?	☐	☐	☐
Comment			

Railway Access (recommendations)	YES	NO	N/A
8. Does the PF control the opening and closing of the gates?	☐	☐	☐
Comment			

9.	Do you have a visual sign showing the opening/closing?	☐	☐	☐
	Comment			
10.	Do you have an automatic intrusion detection alarm?	☐	☐	☐
	Comment			
11.	Do you have additional cameras or other solutions?	☐	☐	☐
	Comment			
12.	Do you have any procedures when gates often remain wide open due to frequent traffic?	☐	☐	☐
	Comment			

Access Procedure	**YES**	**NO**	**N/A**
13. Do you pre-register and which information (operator/ goods/ wagons)?	☐	☐	☐
Comment			
14. Do you registrate data, which one and how?	☐	☐	☐
Comment			

Access Procedure (recommendations)	**YES**	**NO**	**N/A**
15. Do you registrate the names of the rail operators (driver etc.)?	☐	☐	☐
Comment			
16. Do you registrate data, which one and how?	☐	☐	☐
Comment			

Others	**YES**	**NO**	**N/A**
17. Do you check the cargo and which data do you registrate?	☐	☐	☐
Comment			
18. Do you check incoming empty containers and how?	☐	☐	☐
Comment			

19.	Do you report anomalies to the competent authority?	☐	☐	☐
	Comment			

Others (recommendations)		YES	NO	N/A
20.	Do you check outcoming empty containers and how?	☐	☐	☐
	Comment			
21.	Do you have an electronic registration system?	☐	☐	☐
	Comment			
22.	Do you conduct extra checks? Which kind of checks?	☐	☐	☐
	Comment			

7.6 Vehicle Control

7.6.1 Target

Maintain an overview of which (external) vehicles are within the perimeter of the facility and prevent vehicles from being misused to smuggle unauthorized persons or materials in and/or out of the facility. IN is mandatory for ISPS, OUT is mandatory if the PFSA requires it.

7.6.2 Questionnaire

Vehicle Access		YES	NO	N/A
1.	Are vehicles being registered in and out?	☐	☐	☐
	Comment			
2.	Is the following information being registered of vehicles: hour, driver, license plate + land of every vehicle?	☐	☐	☐
	Comment			
3.	Are vehicles being checked on an ad random basis?	☐	☐	☐
	Comment			

Vehicle Access (recommendations)		YES	NO	N/A
4.	Are the specifications for vehicle checks in security level 1, 2 and 3?	☐	☐	☐
	Comment			
5.	Is there a separate area in which vehicles can be checked?	☐	☐	☐
	Comment			
6.	Are different control methods being used for the vehicle checks?	☐	☐	☐
	Explanation External technical vehicle check; use of a mirror; counting of occupants and looking for suspicious materials			
	Comment			
7.	Does the port facility have a policy which limits the vehicle acces to it?	☐	☐	☐
	Comment			

Truck Access		YES	NO	N/A
8.	Is the following information being registered of trucks: hour, driver, license plate + land of every vehicle?	☐	☐	☐
	Comment			
9.	Are the loading and unloading documents being checked at the port facility?	☐	☐	☐
	Comment			
10.	If applicable, are seals being checked?	☐	☐	☐
	Comment			

Truck Access (recommendations)		YES	NO	N/A
11.	Is a seven-point check being carried out on containers?	☐	☐	☐
	Explanation Front door, left side, right side, floor, ceiling/roof, interior/exterior doors, bottom			
	Comment			
12.	Are detection equipment being used during the inspections?	☐	☐	☐
	Explanation For example: CO_2 meters; Scanners; Dog control (K9)			
	Comment			

Vehicles for ship supply or repair		YES	NO	N/A
13.	Is the following information being registered: hour, driver, license plate + land of every vehicle?	☐	☐	☐
	Comment			
14.	Are the vehicles of ship suppliers or repair companies visually being inspected, at the gate and on a random basis?	☐	☐	☐
	Explanation Request to open the cargo/loading space and preform a visual inspection.			
	Comment			
15.	Execute a detailed check as an ISPS drill in cooperation with the ship security officer and the supplier.	☐	☐	☐
	Comment			

16.	Is the movement of vehicles and people at the port facility being monitored?	☐	☐	☐
	Comment			
17.	Are the driving directions clearly indicated at the port facility? Including the areas where vehicles are allowed to be parked?	☐	☐	☐
	Comment			
18.	Will abnormal driving behavior and stopping at non-agreed location be detected at the port facility?	☐	☐	☐
	Comment			

Movements on the facility (recommendations)		**YES**	**NO**	**N/A**
19.	In case of high risk facilities, are visitors guided about the port facility?	☐	☐	☐
	Comment			
20.	Are detection cameras being used to monitor restricted areas?	☐	☐	☐
	Comment			

D/2024/12.443/08

Port of Rotterdam

Port of Antwerp Bruges