091 – Norwegian Oil and Gas Recommended guidelines for securing supplies and materials in the oil and gas industry

Translated version

FOREWORD

These guidelines have been subject to consultation with and are recommended by the Norwegian Oil and Gas Security Forum, HSE Managers Forum, and Operations Committee. They have also been subject to consultation with base specialists. In addition, the government – represented here by the Petroleum Safety Authority Norway (PSA) and the Norwegian Coastal Administration (NCA) – have been consulted. The guidelines are also approved by the director general of the Norwegian Oil and Gas Association.

The responsible manager in Norwegian Oil and Gas is the HSE manager, who can be contacted via the Norwegian Oil and Gas switchboard at +47 51 84 65 00.

These guidelines have been prepared with broad-based participation from interested parties in the Norwegian petroleum industry and are owned by the Norwegian petroleum industry, represented by the Norwegian Oil and Gas Association. Norwegian Oil and Gas is responsible for their administration.

Norwegian Oil and Gas Association
Vassbotnen 1, NO-4313 Sandnes
P O Box 8065
NO-4068 Stavanger
Phone: +47 51 84 65 00
Fax: +47 51 84 65 01
Website: www.norskoljeoggass.no
E-mail: firmapost@norog.no

CONTENTS

1 INTRODUCTION

1.1 Purpose

The purpose of these guidelines is to prevent unauthorised materials or personnel reaching offshore petroleum facilities via the supply chain (including supplier, transport chain, supply base, sea areas, vessel and facilities). The guidelines do not cover the supply chain for air transport (including helicopters, heliports and so forth, which are covered by guidelines 003). This purpose is accomplished by establishing coordinated and uniform practice of the companies' requirements for securing supplies and materials for offshore petroleum operations.

The guidelines represent the industry's common foundation for securing supplies used in oil and gas activities on the Norwegian continental shelf (NCS).

Emphasis will be placed on coordination and on cost-effective measures to detect, delay and, if possible, deter threats or criminal acts, while also laying the basis for the efficient flow of goods.

1.2 Definitions and abbreviations

Asset:	Resource where exposure to an undesirable influence would have a negative consequence for its owner, manager or beneficiary (such as life, health, money, infrastructure, information and reputation). *(NS 5830)*
Base company:	Company which offers or coordinates base services to licensees and suppliers in the oil and gas industry. *(description)*
Baseline security:	Measures/barriers which meet an entity's security requirements under normal conditions. *(NS 5830)*
Entity:	A physical object, individual, organisation, public-sector grouping, enterprise or other unit which fits the context. *(NS 5832)*
Facility:	Installation, plant and other equipment for petroleum activities, however, not supply and support vessels or ships which transport petroleum in bulk. Facility also comprises pipeline and cable unless otherwise provided. *(Petroleum Act)*
Freight documentation:	Waybill, hazardous goods documentation, packing list or manifest accompanying goods arriving at the base. *(description)*

ISPS code:	International ship and port facility security code, adopted by the International Maritime Organisation (IMO) on 12 December 2002. *(NCA guidelines for regulations on port security)*
ISPS area:	Port area regulated in accordance with the international ship and port facility security code to protect against deliberate undesirable actions. *(NCA abbreviations and key terms – in Norwegian only)*
Load container:	All types of containers, baskets, trailers, tanks and frames used for transporting consignments. The term includes associated slings. (*Norsok R-003 2017)*
Load container's security integrity:	The load container is intact and has the correct seal number specified in the delivery documentation. *(description)*
NCA:	Norwegian Coastal Administration *(abbreviation)*
NCS:	Norwegian continental shelf. *(abbreviation)*
Operator company:	Company with the right to explore for oil and gas in a block and to develop a possible commercial discovery. Usually acts on behalf of a licensee partnership. *(PSA's definitions – terms and expressions)*
Pisas:	Petroleum industry security alert system. *(abbreviation)*
Port facility:	The area where contact occurs between ship and port. It covers such areas as anchorages, waiting berths and access from the sea side, where relevant. *(NCA guidelines for regulations on port security)*
PSA:	Petroleum Safety Authority Norway *(abbreviation)*
Restricted area:	The term used by the ISPS for a controlled area. *(description)*
Security:	Application of security measures to deal with the risk associated with deliberate undesirable incidents. *(NS 5830)*

Security level:	The sum of human, technical and organisational (HTO) measures/barrier elements for meeting a defined threat. *(description)*
Security manager:	The enterprise's formal contact on security issues related to the Norwegian Oil and Gas guidelines. The base company's security manager at the supply bases may also play the role of port facility security officer (PFSO) pursuant to the ISPS code. *(description)*
Security measure:	Barrier actions intended to reduce the risk associated with deliberate undesirable incidents. Such actions can be defined as human, technical or organisational (HTO) measures. *(NS 5830)*
Security plan:	A set of routines and procedures regulating the establishment and maintenance of security and emergency preparedness measures at baseline and heightened threat levels for one or more enterprises. Where more than one enterprise is involved, the security plan must be formalised through agreements between the parties. *(description)*
Security risk analysis:	Security risk assessment plus assessment of strategy and measures. *(NS 5831)*
Security risk assessment:	An overall assessment based on assessments of the value, impact on, threats to and vulnerability of assets with the aim of specifying an entity's risk in a defined security context. *(NS 5832)*
Security seal:	A locking device in metal or plastic used to seal closed load containers. A security seal cannot be unlocked, but can only be broken. It must carry a unique number. *(description)*
Supplier:	Enterprise which delivers supplies, materials and/or base services to operating companies or another supplier/ company serving facilities in the oil and gas industry. *(description)*
Supply base:	In this context, "supply base" is understood to mean logistical hubs used for packing, securing and transporting load containers to/from facilities via vessels. *(description)*

Threat:	Possible deliberate undesirable incident which could have negative consequences for the entity's security. *(NS 5830)*
Vulnerability:	Inability to cope with/withstand a deliberate undesirable action or to establish a new stable condition should an asset be subject to an undesirable influence. *(NS 5830)*
Vulnerability assessment:	Assessment of an entity's vulnerability in relation to identified threats. *(NS 5830)*

1.3 References

References in this document refer to documentation which must be read in connection with, and which set relevant requirements for, securing supplies/ materials sent out to the facilities. These references are:

- NCA (in Norwegian only)
  https://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Regelverk/
- Regulation no 538 of 29 May 2013 on security of port facilities (in Norwegian only)
  https://lovdata.no/dokument/SF/forskrift/2013-05-29-538
- Regulation no 539 of 29 May 2013 on port security (in Norwegian only)
  https://lovdata.no/dokument/SF/forskrift/2013-05-29-539
- Guidelines to the regulations on port security (in Norwegian only)
  https://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Veiledning-/
- ISPS code
  https://www.kystverket.no/contentassets/ee9c5d41826343d3ac2d0ccebb7d7fd2/konsolidert-forordning-725-2004.pdf
- Norwegian Oil and Gas guideline 116 – Recommended guidelines for packing, securing and transport as well as user inspection of load containers (in Norwegian only)
  https://www.norskoljeoggass.no/contentassets/a9b7533b85504134a0fbc58c4e95662b/116---retningslinjer-for-pakking-sikring-og-transport-av-last-samt-kontroll-av-lastbarere.pdf

1.4 Simplified diagram

Figure 1 seeks to clarify the principles for the flow of materials in the petroleum industry supply chain.

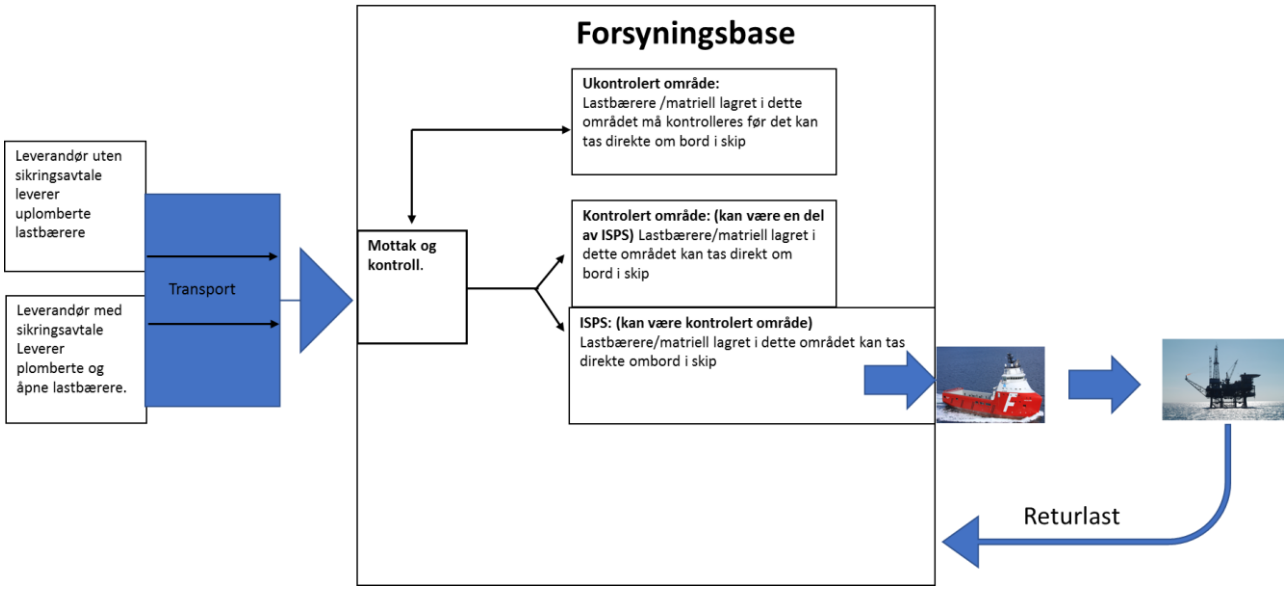

Figure 1 – Simplified diagram

Key

Supplier without security agreement delivers unsealed load containers
Supplier with security agreement delivers sealed load containers

Transport

Supply base
Reception and control
Uncontrolled area:
Load containers/materials stored in this area must be checked before they can be loaded directly onto ships
Controlled area (can be part of ISPS):
Load containers/materials stored in this area can be loaded directly onto ships
ISPS (can be controlled area):
Load containers/materials stored in this area can be loaded directly onto ships

Return cargoes

2 SECURING THE SUPPLY CHAIN

2.1 Security risk analysis and plan

Good risk understanding is crucial for a good security regime. A security risk analysis must therefore be performed. This corresponds to the NCA's "vulnerability assessment" concept.

The security risk analysis will describe operations as well as assessing and determining the system for baseline security. It will also assess and describe possible supplementary security measures for all threat levels – as covered by appendix 2 to this 091 guideline.

A security plan must be established on the basis of a security risk analysis. This plan will describe the security system intended to prevent unauthorised personnel and/or materials reaching facilities on the NCS from the supply bases. The system must comprise a baseline security level and possible supplementary security measures in the event of a heightened security level (appendix 2).

The requirement to conduct a security risk analysis and establish a security plan applies to supply bases and to all suppliers with a security agreement.

The NCA's requirements for vulnerability assessments build almost entirely on the NS 5830 series. Its requirement that such assessments be carried out for port facilities (or similar) can be utilised to meet the requirement specified in these guidelines for a security risk analysis and plan. See the link below to a template (in Norwegian only): https://www.kystverket.no/Nyheter/2016/desember/ny-mal-for-sarbarhetsvurdering-av-havneanlegg/.

Where packing, securing and transport as well as user inspection of load containers are concerned, Norwegian Oil and Gas recommended guideline 116 (in Norwegian only) must be complied with.

2.2 Open load containers

Control routines must be established for open load containers arriving at the supply base. These must ensure that freight documentation accords with the actual goods delivered. After reception and control, open load containers must be stored in an area with controlled access and monitoring (ISPS or controlled area) until they are loaded onto the vessel for shipment to the facility.

Tubulars are taken to be open load containers in this context. Tubulars readied and inspected before being taken directly to the supply base's controlled area are considered to be checked. This also applies when tubulars are readied, inspected and loaded into load containers driven directly to the supply base. The previous sentence applies only when the supplier readying and inspecting tubulars has a security agreement with an operator company.

2.3 Closed load containers

A system for secure packing and sealing of closed load containers must be established at enterprises which enter into a security agreement with an operator company. This must be done on the basis of a security risk analysis at the enterprise which does the packing.

Only operator and base companies with security agreements may pack and seal closed load containers from third-party suppliers without a security agreement.

Closed load containers must be sealed with security seals.

Control routines must be established for closed, sealed load containers on arrival at the supply base to check that the container and security seal numbers accord with the freight documentation. Random checks to ensure that the contents of load containers accord with the freight documentation must be conducted in line with the port facility's security plan (ISPS). If closed, sealed load containers are stored in areas without controlled access or monitoring (ISPS or controlled area), the load container's security integrity as well as container and seal numbers must be checked against the manifest before the load container is loaded onto the vessel.

2.4 Storage at the supply base

After reception and control, the load containers will be stored until they are loaded onto the vessel.

Open load containers stored in a controlled area with security measures able to prevent manipulation of container contents can be sent from the controlled area to the vessel without further checks.

When open load containers are stored outside a controlled area, their contents must be verified and checked before they are loaded onto the vessel.

2.5 Controlled area

A controlled area is one at the disposal of the operator company or a supplier with a security agreement. This area can be used to store load containers which have been subjected to full checking. At a minimum, the security system for the controlled area must correspond to one for a restricted area in an ISPS-approved port facility.

3 SECURITY AGREEMENTS

3.1 Suppliers with security agreements

To ensure acceptable and efficient control over the security of supplies and materials, operator companies can enter into security agreements with key suppliers and base companies. A security agreement has a standardised format and content, which must not be altered (see appendix 1 to this guideline 091).

To ensure the quality of compliance with the requirements in security agreements, efforts should be made to confine these to suppliers of a certain size.

The operator companies are responsible for entering into and following up security agreements with key suppliers. An overview of suppliers with valid security agreements is available at www.norskoljeoggass.no.

Base companies with security agreements can undertake packing, checking, sealing and storing of consignments on behalf of suppliers without security agreements.

A security agreement is valid for up to three years, and the supplier itself is responsible for ensuring its renewal by contacting the operator company pursuant to the contact details in the agreement.

In connection with establishing and renewing an agreement, the operator company is responsible for verifying the supplier's compliance with its terms. Such verification will include the restricted area. Unannounced verifications can also be conducted.

Operator companies may award a temporarily approved security agreement for up to three months in cases where identified non-conformities must be closed before a final agreement can be entered into.

Should the terms of an agreement be breached, it can be cancelled by the operator company with immediate effect.

3.2 Suppliers without security agreements

For all consignments from suppliers without a security agreement where delivery is to be made directly to the supply base or the operator company, the supply base or operator company must be contacted in order to avoid delivery delays.

4 SECURITY SEALS

Use of security seals

Security seals must be used to seal closed load carriers for transport to offshore facilities on the NCS. Only operator and base companies, plus suppliers with valid security agreements, are allowed to seal consignments with these security seals. Further procedures for using security seals are detailed in chapter 5.

Requirements for security seals, and requisitioning and returning these

Security seals used must be produced by a manufacturer designated by the operating companies. Only one such manufacturer can produce security seals at any given time. Old OLF seals must not be used.

Only the security manager at the base or supplier company with a security agreement can requisition security seals from the manufacturer.

Seals must be kept under lock and key, and inaccessible to unauthorised people.

Should the security agreement be cancelled or expire, unused seals and logs must be handed over to the operator company which entered into the security agreement.

Requirements for the manufacturer

The manufacturer of security seals is responsible for logging the number series which have been manufactured and delivered to the operator companies, to the base companies and to suppliers with security agreements.

5 REQUIREMENTS FOR PARTIES ENTERING INTO SECURITY AGREEMENTS

5.1 Requirements for suppliers with a security agreement

On the basis of a security risk analysis, the minimum requirements for a supplier's security system are as follows.

a) Security must be an integrated part of the supplier's security system, which must:
- be well entrenched with the management in that targets are set for security, the necessary resources are allocated, and the security status is evaluated annually by management
- have satisfactory security documentation with clear guidance for security work
- establish clear responsibilities and organisation
- ensure that personnel responsible for receiving and checking piece goods and load containers, packing, securing consignments, and locking and sealing load containers have received documented training
- set requirements for annual security reviews with all personnel involved in packing and dispatch pursuant to the security agreement. During these reviews, a reminder must be given that the purpose of the agreement is to prevent unauthorised materials and/or personnel reaching facilities via the supply chain. The review must be appropriate for motivating vigilance and identifying the need to enhance expertise
- ensure that security reviews carried out are documented
- ensure that at least one security exercise is conducted annually with varying scenarios, and that these exercises are documented
- provide a structured method for work on security management, such as a management plan which includes evaluation and revision.

b) The supplier must appoint a contact person for matters relating to security (security manager). One of their duties will be to ensure compliance with the security agreement.

c) Safety seals must be kept under lock and key, and access to them must be restricted. Withdrawal of seals must be logged, with seal number, date and signature. At the end of the working day, unused seals must be returned to locked storage and logged in the same way as for withdrawal. Unused withdrawn seals must be kept under control and secured against theft. The supplier must ensure an overview of the stock of seals.

d) The security manager can delegate responsibility for storing and issuing seals, and for checking and sealing consignments, to selected personnel in their own company, providing sufficient training has been given.

e) Load containers (containers, tanks, etc) must be checked for internal and external foreign objects before being taken into use.

f) Only goods specified in the manifest and/or freight documentation can be packed in load containers.

g) The seal number must be entered on the freight documentation.

h) The load container must be under continuous observation during packing/filling. If the supplier must interrupt packing and temporarily leave the packing site, the load container must be locked and sealed. The seal must be checked and found to be unbroken before packing/filling resumes, and/or the load container is finally locked and sealed. If an unlocked and unsealed load container has not been under continuous observation, or the seal has been manipulated/broken, it must be rechecked before it is resealed and dispatched from the supplier.

i) Before leaving the supplier, the load container must be checked to see that the seal is unbroken (with the correct seal number), that it is free of foreign bodies and that it otherwise conforms with the Norwegian Oil and Gas checklist for user control (see Norwegian Oil and Gas guideline 116 – Recommended guidelines for packing, securing and transport as well as user inspection of load containers (in Norwegian only)).

j) If a load container's seal is removed or broken before dispatch, it must be halted and all content checked before dispatch from the supplier. The same applies if the seal number does not accord with the freight documentation/ delivery information from the supplier.

k) The supplier will be notified by the supply base if the seal is broken or removed, or if its number does not match the manifest on arrival or while at the base. The supplier must then check the load container together with the base before it is locked and sealed again. Supplier checks can be carried out on site or on the basis of information from the base in the form of photographs, videos and/or a verbal description.

l) If a break-in occurs or is suspected in the warehouse or in areas where security-sealed load containers are stored, these must be specially checked for broken seals and foreign bodies.

m) The responsible operator company must be notified immediately in the event of such irregularities as the loss/theft of security seals, the discovery of foreign bodies in or on load containers, removed or broken seals on load containers, or other conditions which arouse suspicion that irregular activities have occurred.

n) The supplier must not undertake packing, checking or sealing with security seals for other suppliers, except in the case of its own sub-suppliers.

o) Where packing, securing and transport as well as user inspection of load containers is concerned, the supplier must comply with the content in the Norwegian Oil and Gas recommended guideline 116 with associated documents.

p) Suppliers of chemicals or other liquids are themselves responsible for verifying the contents before onward dispatch to the supply base.

5.2 Requirements for base company with security agreement

On the basis of a security risk analysis, the minimum requirements for the supply base's security system are as follows.

a) Security must be an integrated part of the base company's security system, which must:
- be well entrenched with the management in that targets are set for security, the necessary resources are allocated, and the security status is evaluated annually by management
- have satisfactory security documentation with clear guidance for security work
- establish clear responsibilities and organisation
- ensure that personnel responsible for receiving and checking piece goods and load containers, packing, securing consignments, and locking and sealing load containers have received documented training
- set requirements for annual security reviews with all personnel involved in packing and dispatch pursuant to the security agreement. During these reviews, a reminder must be given that the purpose of the agreement is to prevent unauthorised materials and/or personnel reaching facilities via the supply chain. The review must be appropriate for motivating vigilance and identifying the need to enhance expertise
- ensure that security reviews carried out are documented
- ensure that at least one security exercise is conducted annually with varying scenarios, and that these exercises are documented
- provide a structured method for work on security management, such as a management plan which includes evaluation and revision.

b) The base company must appoint a contact person for matters relating to security (security manager). One of their duties will be to ensure compliance with the security agreement.

c) Safety seals must be kept under lock and key, and access to them must be restricted. Withdrawal of seals must be logged, with seal number, date and signature. At the end of the working day, unused seals must be returned to locked storage and logged in the same way as for withdrawal. Unused withdrawn seals must be kept under control and secured against theft. The base company must ensure an overview of the stock of seals.

d) The security manager can delegate responsibility for storing and issuing seals, and for checking and sealing consignments, to selected personnel in their own company, providing sufficient training has been given.

e) Load containers (containers, tanks, etc) must be checked for internal and external foreign objects before being taken into use.

f) Only goods specified in the manifest and/or freight documentation can be packed in load containers.

g) The seal number must be entered on the freight documentation.

h) The recipient must check the seal number against the freight documentation.

i) The load container must be under continuous observation during packing/filling. If the base company must interrupt packing and temporarily leave the packing site, the load container must be locked and sealed. The seal must be checked and found to be unbroken before packing/filling resumes, and/or the load container is finally locked and sealed. If an unlocked and unsealed load container has not been under continuous observation, or the seal has been manipulated/broken, it must be rechecked before it is resealed and dispatched from the base company.

j) Before leaving the base company, the load container must be checked to see that the seal is unbroken (with the correct seal number), that it is free of foreign bodies and that it otherwise conforms with the Norwegian Oil and Gas checklist for user control (see Norwegian Oil and Gas guideline 116 – Recommended guidelines for packing, securing and transport as well as user inspection of load containers (in Norwegian only)).

k) If a load container's seal is removed or broken before dispatch, it must be halted. The base company must notify the original supplier, who must check all content. The same applies if the seal number does not accord with the manifest.

l) If a break-in occurs or is suspected in the warehouse or in areas where security-sealed load containers are stored, these must be specially checked for broken seals and foreign bodies.

m) The supplier will be notified by the base company if the seal is broken or removed, or if its number does not match the manifest on arrival or while at the base. The supplier must then check the load container together with the base before it is locked and sealed again. Supplier checks can be carried out on site or on the basis of information from the base in the form of photographs, video and/or a verbal description.

n) The responsible operator company must be notified immediately in the event of such irregularities as the loss/theft of security seals, the discovery of foreign bodies in or on load containers, removed or broken seals on load containers, or other conditions which arouse suspicion that irregular activities have occurred.

o) A base company with a security agreement is permitted to pack, check and seal load containers.

p) When receiving load containers from suppliers with a security agreement, a minimum of five per cent of all closed load containers must be checked before being admitted to an ISPS or restricted area under a normal threat level. Chemicals are exempted from this check.

q) When reception and control has been carried out with open load containers, these must be stored in an area with access control and surveillance until loaded onto the vessel for shipment to the facility. When open load containers are stored

outside a controlled area, they must be checked before loading onto the vessel.

r) Where packing, securing and transport as well as user inspection of load containers is concerned, the supplier must comply with the content in the Norwegian Oil and Gas recommended guideline 116 with associated documents.

s) Only the base company may pack and seal closed load containers from third-party suppliers without a security agreement.

5.3 Requirements for operator companies

In connection with establishing security agreements, the operator has the following responsibilities.

a) Entering into security agreements with suppliers and base companies which are to send closed, locked and sealed load containers to facilities. These agreements must have a maximum duration of three years.

b) Verifying before entering into a security agreement that the supplier/base company meets the requirements defined in this document.

c) Make announced/unannounced checks of compliance with these requirements.

d) Check that the supplier/base company complies with the security system throughout the duration of the agreement. The operator must seek to apply a coordinated verification practice. An audit of the security system must be conducted during the life of the contract.

e) Make security agreements and audit reports available to operator companies.

f) Approve the right to order security seals.

5.4 Vessels

Provisions pursuant to the ISPS apply during transport on vessels.

5.5 Facilities

Before a load container is opened, the security seal must be checked for damage and to ensure that its number accords with the freight documentation. When the load container is opened, its contents must be verified against the manifest. Discrepancies must be notified, reported and dealt with immediately.

Security seals must not be used on return consignments.

6 RESPONDING TO INCIDENTS

Should the absence of or breaches to security measures be identified, immediate action must be taken to restore the barrier(s). Restricted areas must be inspected, and other compensatory measures must be proportionate to the relevant barrier breach. The operator company must be notified in each case. The incident must be registered.

In the event of breaches to the access provisions, unauthorised activity or activation of perimeter alarms, the private security company must be able to mobilise immediately and verify the relevant area manually. Controlled areas must be checked in order to re-establish security barriers.

Closed load carriers where security seals are damaged or missing, or where the seal number does not correspond with the freight documentation, must be quarantined. The supplier must be notified. The latter must verify that the contents of the load carrier conform with the freight documentation before the load carrier can be resealed. New freight documentation must then be issued with the updated seal number.

Nonconformities identified between the stock of seals and the log must be reported to the operator company. The missing seal numbers must be declared invalid.

The operator company must be notified immediately should any unauthorised use of safety seals or illegal and/or unauthorised objects be discovered.

The operator company can issue a notification via Pisas in the event of incidents which could be significant for other operator companies.

7 REVISION HISTORY

Revision no 4 to the guidelines of01.03.2019 has been significantly amended compared with revision no 3 of 1 September 2015. The most important changes can be summarised as follows.

- Revision no 4 has been built up as a performance-based (functional) guideline, unlike revision no 3, which was more prescriptive.

- Revision no 4 sets stricter requirements for the players on conducting security risk analyses and the description of their own risk.

- Revision no 4 is harmonised with the ISPS code. In other words, the guidelines reflect a level of security corresponding with the international standard/code for securing port facilities.

- Descriptions of various security incidents have been removed from revision no 4 because each entity must conduct risk analyses to identify their own vulnerability and risk, and dimension their own preparedness and security measures in relation to these.

- References to the supply base network in Norwegian Oil and Gas have been removed because this network no longer exists.

- The structure of revision no 4 has been amended in line with the new construction of the document. See the items above.

- The definition of “controlled area” has been amended. Revision no 4 builds on the ISPS code as a minimum requirement, and safety risk analyses will result, where relevant, in additional security measures.

- It is assumed that security risk analyses will be conducted as the basis for preparing security plans. These will accord with accepted standards.

- The description of access control in revision no 3 has been amended in revision no 4. This is one of several security measures which can be implemented to reduce risk. This will emerge through analysis and be described in the security plan.

- Specific training requirements, as described in revision no 3, have been removed and replaced in revision no 4 with a requirement that relevant personnel must be able to document the appropriate training.

- Appendix 1 in revision no 3 on baseline security requirements has been removed since the security risk analysis will determine the level of baseline security.

- Appendix 2 in revision no 3 becomes appendix 2 in revision no 4 on heightening the security level, emergency response measures and notification procedures (state of alert). *Confidential.*

- Appendix 3 in revision no 3 becomes appendix 1 in revision no 4: security agreement for suppliers and supply bases.

- Appendix 4 in revision no 3 on the decision table has been removed and is replaced by figure no 1 in revision no 4.

APPENDICES

Appendix 1 — Security agreement for suppliers and supply bases
Appendix 2 — Heightening the security level, emergency response measures and notification procedures