GRONINGEN SEAPORTS

Information security policy

Classification: corporate confidential
Version: 3.0

Contents

Contents 2

1. Version and approval management 4

2. The importance of information security 5

3. Groningen Seaports information security policy 6

3.1 What is our target level? *6*

3.2 Detailing of the ambitions *6*

3.3. Familiarity with the information security policy *7*

Article 3.4 Confidentiality *7*

3.4.1 Authentication of data 7

3.5 Removable media *7*

3.6 Employees instructions *8*

3.7 Awareness regarding information security *8*

3.8 Relationship with the information security manual *8*

3.9 Detailing of policy in standards and instructions *8*

4. Information security process 9

4.1 PDCA cycle *9*

4.2 Risk assessment and handling process *9*

4.2.1 Scope of the risk management process 9

4.2.2 Risk evaluation criteria 10

4.2.3 Risk handling options 11

4.2.4 Representation of risk assessment and handling process 11

4.4 Internal audits *11*

4.5 Owners of applications, systems and processes *12*

4.5.1 Agreements with suppliers *12*

5. Organisation of information security 13

5.1 Information security organigram *13*

5.2 Rolls *14*

5.2.1 Groningen Seaports RACI model *16*

5.3 Where can information be found regarding information security? *17*

5.4 Co-operation *17*

5.4.1 Samenwerking Noord 17

5.4.2 Seaports in the Netherlands 17

6. Communication regarding security incidents 18

6.1 Distinction between security leaks and security incidents *18*

6.2 When do we refer to a data leak? *18*

6.3 Communication regarding security incidents *18*

6.4 Registration of security leaks and incidents *19*

7. Rights and access to information 20

7.1 Need to know *20*

7.2 Least privilege *20*

8. Periodic assessment 21

8.1 Targets and Key Performance Indicators (KPIs) *21*

8.2. Reporting *21*

Glossary 22

Reference list 22

List of figures 22

1. Version and approval management

Version management		
Version	**Status**	**Date**
1.0	Signing of final version by board	November 2018
2.0	Overall revision. The password policy has become an integral component of the information security policy.	February 2020
3.0	Update of the policy following new requirements and developments.	May 2023

Approval				
Name	**Role**	**Approved**	**Date of document**	**Version**
Cas König - CEO	Approved	Yes in MT November 2018	19 November 2018	April 2018
Harold Sanders - CFO	Approved	Yes in MT February 2020	25 February 2020	2.0
Harold Sanders - CFO	Approved	Yes in OO May 2023	1 June 2023	3.0

2. The importance of information security

At Groningen Seaports, the processing and exchange of information is an extremely important factor for the achievement of strategic targets.
Security within the seaport and the financial returns are dependent upon it. Think in terms of correct shipping registration and the confidentiality of sales information, for example Information and communication technology is continuously creating new opportunities for the processing and exchange of information, but at the same time also entails new risks.

The Groningen Seaports organisation is a so-called government NV (private law legal entity). The commercial tasks are conducted by the NV. The designated public tasks which are conducted by the organisation, such as the processing of shipping traffic, are covered by the government part. These public tasks are subject to other requirements by the government and maritime organisations with regard to (information) security, which are not described in this document for the time being. When information and resources are required to conduct the public tasks and are made available by the NV, these are covered by the minimum requirements and conditions set by the NV for that purpose.

Any risks pose a threat to the functioning of Groningen Seaports, and Groningen Seaports therefore requires adequate security of its information. Adequate is defined as the measures to be taken being suitable for the intended purpose. In this case, Groningen Seaports will take suitable measures to guarantee the availability, integrity and confidentiality [1]of the information supply, both digitally, orally and in writing. For that matter, such measures are not only based on a conscious risk consideration in keeping with the state of technology and working field at Groningen Seaport. They must also take account of the (compulsory) legislation and regulations applicable to Groningen Seaports. Examples of such legislation are:

- General Data Protection Regulation (GDPR) as of 25 May 2018;
- Port Security Act;
- Network and information security guideline 2 (as of 17 October 2024).

Groningen Seaports applies the information security policy to determine when and to what degree information security is implemented at the required ambition level. Moreover, the policy enables assessment of the practical situation versus the principles, with timely adjustment where necessary.

[1] Glossary

3. Groningen Seaports information security policy

3.1 What is our target level?

In the world of information security, the international standards of NEN-ISO/IEC 27001 and NEN-ISO/IEC 27002 generally serve as the reference framework. The first of these standards (NEN-ISO/IEC 27001) offers a guideline for the implementation and scheduled safeguarding of Information security within the organisation. The second standard (NEN-ISO/IEC 27002) contains an extremely extensive collection of guidelines for a practical and concrete approach to information security within the organisation.

Groningen Seaports has opted to use these reference frameworks (NEN-ISO/IEC 27001 / NEN-ISO/IEC 27002) as a general guide. In order to set a clear level, Groningen Seaports uses the *COBIT 2019* maturity model *(COBIT).* The model has six (6) levels: Excellent (5), good (4), defined (3), managed (2), inadequate (1), critical (0).

The level which Groningen Seaports wishes to achieve for information security is in line with COBIT level 4 (good). COBIT describes this level as follows: “Groningen Seaports is data driven with quantitative performance improvements. Security measures achieve their purpose, security is well-defined and performance is monitored up to a certain degree.”

Once Groningen Seaports has achieved this level, this will represent a major step towards compliance with the NEN-ISO/IEC 27001 standard. This may result in much less effort being required to gain certification for the NEN-ISO/IEC 27001 standard (or comparable), if necessary.

3.2 Detailing of the ambitions

The NEN-ISO/IEC 27001 standard includes a component of the availability of a Statement of Applicability (Verklaring van Toepasselijkheid - VVT). In a Statement of Applicability (VVT), an organisation indicates which business components of this standard apply to the organisation, and why. Business components may be applicable, or not, due to commercial requirements, statutory obligations or both, for example.

Due to Groningen Seaports using the NEN-ISO/IEC 27001 standard as the general guide, a VVT is not directly needed. A comparable document [2]has therefore been formulated. This document shows the current status level as well as the required level. The document is accessible for board members and the members of the Information security team.

[2] plan-level of information security-1

3.3. Familiarity with the information security policy

The information security policy applicable within Groningen Seaports and the accessory guidelines, instructions and protocols apply to all employees (internal / external / temporary). The policy also applies to processes. One example is the process followed when entering and leaving employment, and the actions required to do so. On entering employment, new employees are informed by Human Resources / Personnel Affairs (HR) of the location of this information security policy document in the CISO environment, accessible via the intranet. All employees must be familiar with the contents of the documents made available.

Whenever a new main version of a policy document is released, the CISO team will inform all employees.

Article 3.4 Confidentiality

All information processed by or at Groningen Seaports is automatically designated as corporate confidential, unless otherwise indicated. This means that information may generally not be shared with external parties, unless there is a valid reason or agreement to do so. Sharing can take place digitally, physically or by word of mouth.

This corporate confidential data is also subject to a separate classification, which is based on four (4) levels. These levels and the related requirements are described in the data classification document [3]which can be found in the CISO portal.

3.4.1 Authentication of data

Authentication data, such as user names, passwords and pin codes are encrypted and safely saved and stored as standard. Groningen Seaports provides a password safe for this purpose, which must be used. Employees are generally not permitted to write down or email passwords, nor to share or save non-encrypted (text) files.

If there is any reason to handle this type of data in any other manner, this must be reported to the CISO team. They will assess what is necessary and why, together with the person making the request. If a deviating action is approved, this will be described and registered by the CISO team.

3.5 Removable media

In order to prevent loss of confidential Groningen Seaports information as much as possible, employees are not permitted to save Groningen Seaports information on removable media. Removable media is taken to understand USB flash drives and external hard drives.

If there is an important reason to deviate from this decision, it must be reported to the CISO team. They will assess whether the removable medium is necessary for business purposes, together with the person making the request. Following approval, this will be described and registered by the CISO team.

[3] policy-data classification-1

3.6 Employees instructions

For detailed information on employees instructions, please refer to the employees instruction document[4]. It can be found in the CISO portal on the intranet.

3.7 Awareness regarding information security

It is of great importance to Groningen Seaports that all employees gain and maintain an appropriate level of awareness regarding information security. The CISO works with HR to design an adequate awareness programme, whereby a general basic level is defined and extended with specific additions per role and/or responsibility.

3.8 Relationship with the information security manual

The manual [5]for information security can be consulted to offer guidance, to store practical information and to describe any agreements and processes which have been made. It is available in the Sharepoint environment of the members of the CISO team and the Information security team. The members of this team are described in paragraph 5.2.

3.9 Detailing of policy in standards and instructions

Subjects covered in this information security policy are eventually translated into (technical) standards and instructions. One such example is a patch / update policy which describes how and when Groningen Seaports resources must be updated, or the baseline information security[6] which describes how the use of multi-factor authentication is always compulsory regardless of the location from which employees log in.

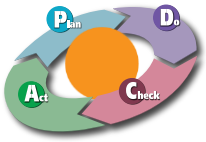
These standards and instructions are generally accessible to all employees via the CISO portal on the intranet. Should any of these documents contain (process) confidential information, they will only be shared with those employees authorised for that purpose, in accordance with the requirements of the data classification policy referred to earlier.

[4] manual-information security employees-1
[5] manual-information security-1
[6] standard-baseline information security-1

4. Information security process

4.1 PDCA cycle

Groningen Seaports strives to continuously maintain information security at the required level. However, information security is a continuously changing process. 'Plan, Do, Check and Act' together form the management system for information security. This quality cycle is described below:



- **Plan**: the cycle starts with the information security policy, based on legislation and regulations, national standards and best practices. This policy is detailed in guidelines for the use of information, corporate continuity and compliance (information security plan). Planning takes place annually and can be adjusted in the meantime when necessary.
- **Do:** The policy framework forms the basis for risk management, execution of (technical) measures and promotion of security awareness. It is implemented on a daily basis and is an integral component of the working process.
- **Check**: check is a part of the working process whose purpose is to safeguard the quality of information, ICT and compliance with legislation and regulations. External control refers to the control by an auditor (outside of the primary process). This takes the form of a random check.
- **Act**: the cycle is completed upon implementation of improvement actions based on the check and (possible) external control. The cycle is a continuous process, whereby the findings of checks form the import for the annual planning and security plans. The findings are in principle reported to the board; an improvement proposal is made in the event of more drastic improvement actions.

4.2 Risk assessment and handling process

Just like many other processes, the risk assessment and handling process is a cyclical one. At Groningen Seaports, the standard cycle duration is one (1) year. This paragraph describes the process applied by Groningen Seaports.

4.2.1 Scope of the risk management process

The scope of the risk management process for information security is limited to all online and off-line processes, systems and applications with which Groningen Seaports information is processed.

4.2.2 Risk evaluation criteria

The aforementioned information security risks must be weighed in order to be able to determine priority, among other things. The diagram below is used for that purpose. This diagram is in line with the criteria applied by Groningen Seaports for the general risk analysis. **All** risks must at all times be maintained in the risk register[7], regardless of their status. This register is available for the CISO team, internal auditor and members of the Information security team. Risks can only be closed in (and removed from) the register, if there is no longer any indication that they will actively influence the organisation (objectives).

	Chance	**<20%**	**>= 20% and < 40%**	**>= 40% and < 60%**	**>= 60% and < 80%**	**>=80%**
Impact (cost in Euro)						
>= 10,000,000						
>= 1,000,000						
>= 400,000						
>= 200,000						
>= 100,000						

Legend:
Dark green: We accept risks which fall within the bandwidth of the risk willingness.
Light green: Risks are in line with the risk willingness of Groningen Seaports (partly due to mitigating measures in place). Further risk limitation is assessed on the basis of effort/costs versus (further) reduction of the risk.
Orange: Action is required to reduce this risk to an acceptable level. Paragraph 4.2.3 describes the actions to be taken.
Red: Immediate action is required in order to directly mitigate the risk and then to reduce it to an acceptable level. Paragraph 4.2.3 describes the actions to be taken.

Chance: the chance that the risk will occur within 5 years

Almost certain	>=80%
Very likely	>= 60% and < 80%
Likely	>= 40% and < 60%
Unlikely	>= 20% and < 40%
Very unlikely	<20%

[7] inventory-infosec risk register-1

4.2.3 Risk handling options

- **Mitigating a risk:** This involves implementing a solution to reduce or remove (the level of) the detected risk. An example is installation of an (improved) anti-malware solution.
- **Risk transfer:** The organisation can opt to transfer the risk to another entity. An example is that the organisation takes out cyber security insurance. Risk transfer often only applies to part of the risk in question. The organisation then needs to determine how much risk remains following transfer.
- **Risk avoidance:** The organisation opts to completely remove the cause of the risk. Or to no longer strive for a certain form of business which entails too much risk.
- **Risk acceptance:** An organisation accepts and acknowledges the existence of a risk. Action is no longer taken against this risk. Risk acceptance can also relate to the residual risk of an already mitigated risk.

4.2.4 Representation of risk assessment and handling process

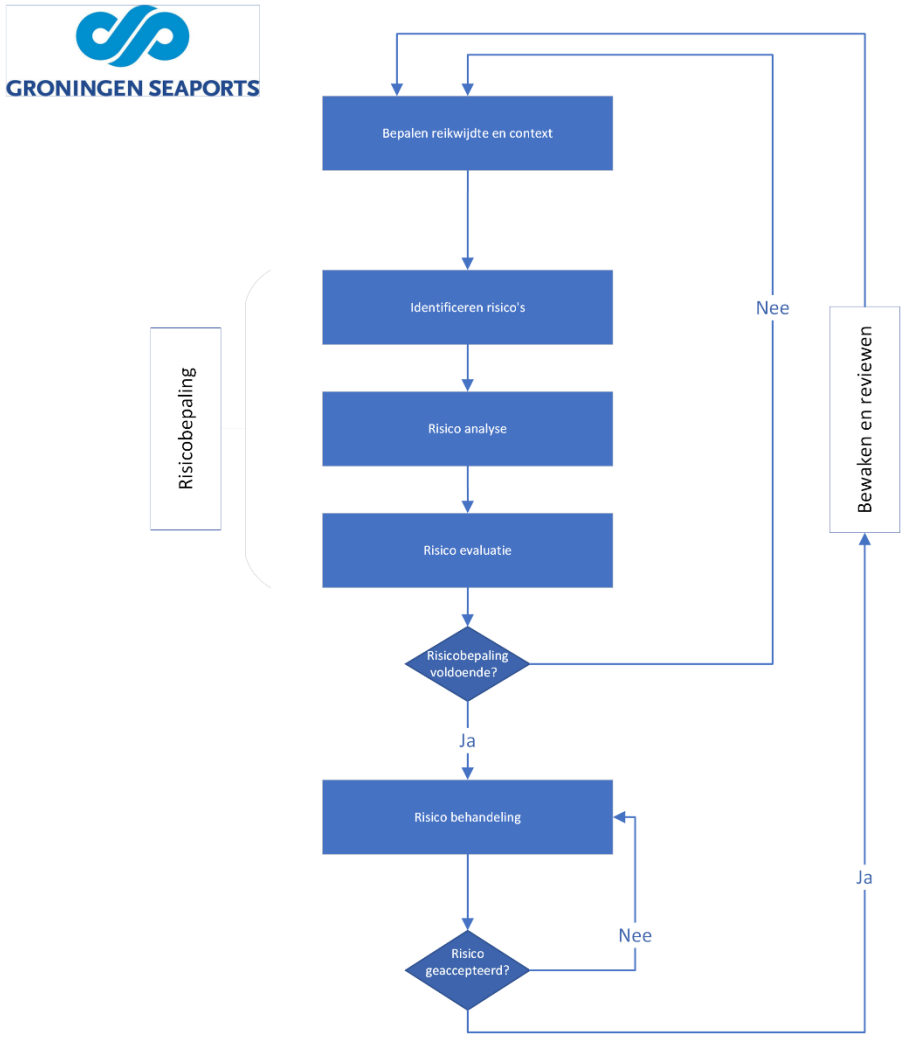


Figure 1 - Risk assessment and handling process

4.4 Internal audits

The organisation of periodical internal audits is a method which allows effective insight into the current situation within the organisation. Groningen Seaports has its own internal audit department which functions independently. These periodical audits render Groningen Seaports well prepared for possible (compulsory)

external audits. The internal audit department of Groningen Seaports has included information security as a compulsory subject in the audit programme.

4.5 Owners of applications, systems and processes

Within Groningen Seaports, it is compulsory for each application, system or process in which Groningen Seaports information is processed, to have an official owner. This owner is responsible for reaching agreements with suppliers in accordance with the requirements of the document referred to in 4.5.1. This ensures, among other things, that the Groningen Seaports information remains as available, sound and confidential as possible.

The owners inform the CISO team regarding those matters for which they are responsible. When purchasing applications and systems, or initiating new processes, the CISO team is actively requested to provide advice. They also comply with the requirements made of suppliers by Groningen Seaports. Furthermore, they are responsible for ensuring that applications and systems always remain up to date. This is done according to the requirements of Groningen Seaports[8].

End users of information must treat such information with great care and must always act in accordance with this information security policy and the accessory process descriptions.

4.5.1 Agreements with suppliers

Relevant information regarding agreements with suppliers is given in the policy for information security within supplier relationships. This document[9] can be found in the CISO portal.

[8] policy-patch and release-1
[9] policy-infosec requirements suppliers-1

5. Organisation of information security

5.1 Information security organigram

The illustration below is a visual representation of the roles currently defined in the information security organisation of Groningen Seaports.

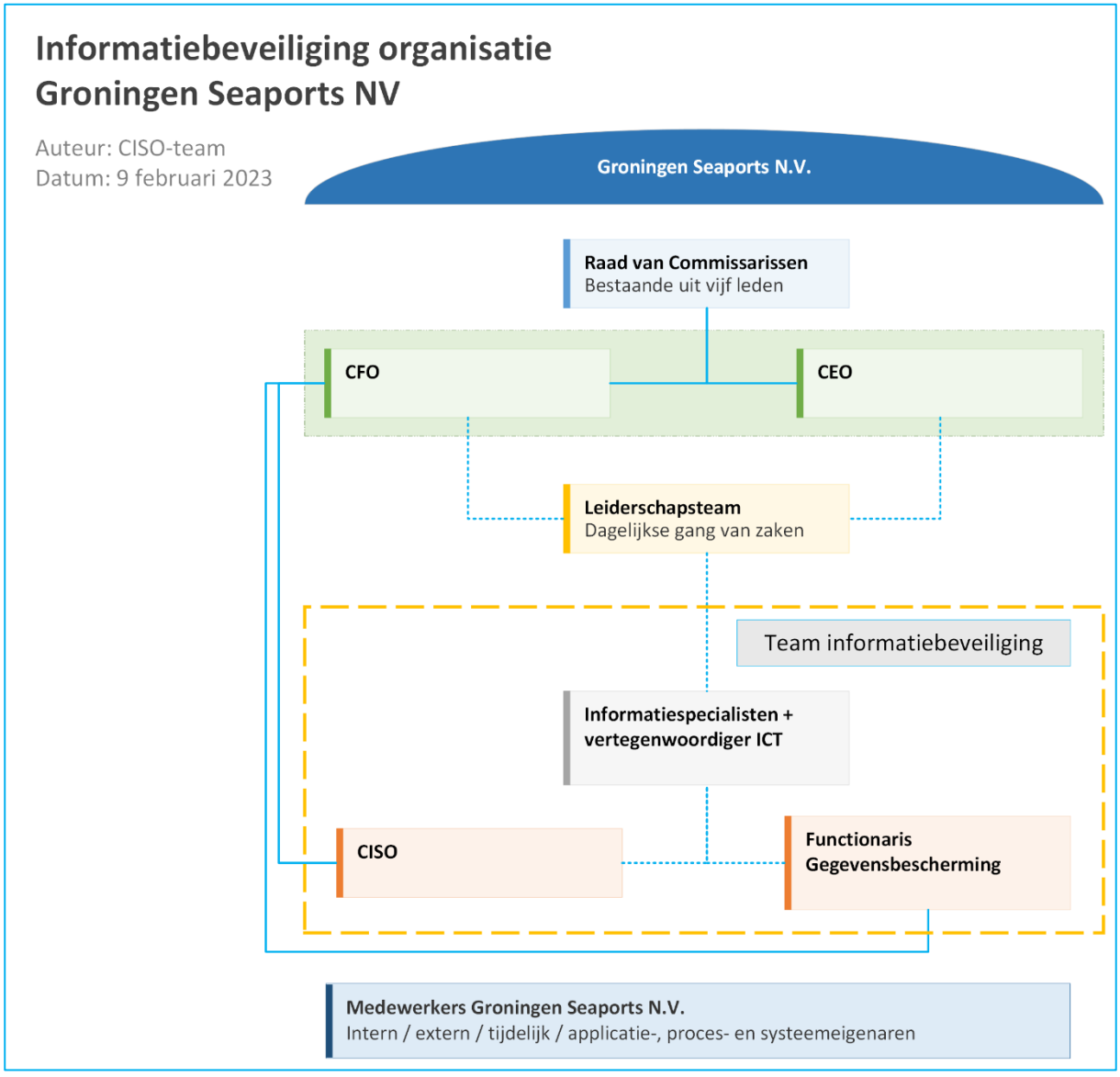


Figure 2 - Visual representation of InfoSec organisation

5.2 Rolls

The following roles exist within information security at Groningen Seaports:

Employees (internal / external / temporary)
Each employee at Groningen Seaports works with information, both digital and non-digital. Each employee in the organisation is responsible for correct and sound handling of this information. Furthermore, each employee at Groningen Seaports is responsible for detecting and reporting any (suspected) security incidents to the CISO. See also paragraph 6.1.

Board of Directors
The Board of Directors, comprising the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) of Groningen Seaports, formulates the information security policy and holds final responsibility for its safeguarding and compliance. The Board of Directors determines the level of ambition, along with the timeline and necessary administration of measures to gain and maintain the required level.

Supervisory Board (SB)
The Board of Directors is accountable to the SB, which comprises five members. Conversely, the SB may also offer (unsolicited) advice to the Board of Directors.

Chief Financial Officer (CFO)
The CFO is the portfolio holder of information security within the Board of Directors. The CISO team reports to the CFO and will confer on any matters concerning information security.

Corporate Information Security Officer (CISO)
The authorities to implement the information security policy are delegated to the CISO. The CISO is responsible for formulating and promoting the information security policy of Groningen Seaports, and for monitoring of compliance. Should the information supply be affected, the CISO also has an advisory role in the crisis and calamity organisation.

Data Protection Officer (DPO)
The General Data Protection Regulation (GDPR) requires public government bodies to appoint a Data Protection Officer who monitors compliance with the regulation on behalf of the Authority for Personal data (AP). This includes creating awareness regarding privacy for all employees, and management of a processing register[10] for any processes which handle personal data, et cetera.

The task package of approximately one (1) day per month is combined with the CISO role. The DPO, who is also a member of the CISO team, falls under the responsibility of the CFO.

Human Resources (HR or Personnel Affairs)
HR is responsible for the correct supply of information to new employees, employees changing jobs and employees leaving Groningen Seaports. HR works closely with the CISO team to gain and maintain the required level of awareness with regard to information security.

[10] Refer to the reference list for the location.

Information security team

The CISO team is basically responsible for determining, managing and implementing the information security policy at Groningen Seaports. This policy and all resultant actions and tasks are discussed with the Information security team.

This team comprises:

- CISO team;
- Information specialists from the departments:
    - Business Support;
    - Shipping.
- Representative of the ICT team.

Application, system and process owners

Owners are designated for each application, system or process which handles Groningen Seaports information. They are responsible for safe processing and use of the information in their particular application, system or process.

5.2.1 Groningen Seaports RACI model

RACI is an acronym derived from the four main responsibilities, which are most commonly applied: **R**esponsible, **A**ccountable, **C**onsulted and **I**nformed. The RACI matrix is used to define and clarify roles and responsibilities within Groningen Seaports.

	Role							
Task:	Supervisory Board	Board of Directors	CFO	CISO	DPO	HR	InfoSec Team	Employees
Identification of the requirements regarding information security and stakeholders.	C	A	A	R	R	C	C	I
Definition of basic frameworks (e.g. policy, etc.)	I	A	A	R	R	C	C	I
Development of the risk assessment and handling methodology.	I	I	A	R	R	I	C	I
Execution of the risk assessment and formulation of the risk handling plan.	I	I	A	R	R	I	C	I
Monitors the execution process.	C	I	A	R	R	I	C	I
Training personnel and raising awareness.	I	I	A	R	C	R	C	I
Manages the detailing and functioning.	I	I	A	R	C	C	C	I
Performance monitoring and measurement.	I	I	A	R	R	I	C	I
Execution of internal control regarding policy.	I	I	A	R	R	C	C	I

5.3 Where can information be found regarding information security?

Final (policy) documents with regard to information security of importance to all employees are made available via the intranet.

5.4 Co-operation

There are mutual dependencies between the parties operating within the seaports, with regard to continuity and safety. Disruption suffered by any one party can have far-reaching consequences for other parties within the seaports. Groningen Seaports strives for cooperation with other parties, to enable rapid sharing of experience and know-how with regard to information security.

5.4.1 Samenwerking Noord

The co-operative alliance known as "Samenwerking Noord" (cooperation of Northern Netherlands' government bodies and companies in the ICT field) includes an information security expertise group, to which both government bodies and specialist security companies are affiliated. Members of the CISO team will join the privacy and security working group[11].

5.4.2 Seaports in the Netherlands[12]

The Netherlands is home to other seaports besides Groningen Seaports. The main four (4) are described here:

- Port of Rotterdam;
    - Also includes the ports of Dordrecht and Vlaardingen.
- Port of Amsterdam;
    - Also includes the ports of Velsen/IJmuiden, Beverwijk and Zaanstad.
- Port of Moerdijk;
- North Sea Port (Vlissingen and Terneuzen, excluding Ghent).

While Groningen Seaports may be 'the smallest' of the five (5) seaports located in the Netherlands with regard to the transshipment tonnage, it is certainly not the least important. Groningen Seaports is also an extremely important organisation within in the Netherlands due to the presence of the LNG terminal. Groningen Seaports believes strongly in sharing any experience but at the same time learning from others.

For example, the experience gained in Rotterdam with regard to improving information security in collaboration with all seaport parties has proven to be very useful for Groningen Seaports. The ambition is therefore to give structural shape to the collaboration between Groningen Seaports and the other seaports, with regard to information security aspects.

[11] https://samenwerkingnoord.nl/kennisnetwerken/privacy-security/
[12] https://www.cbs.nl/nl-nl/visualisaties/verkeer-en-vervoer/vervoermiddelen-en-infrastructuur/zeehavens

6. Communication regarding security incidents

6.1 Distinction between security leaks and security incidents

A *security leak (vulnerability)* is not by definition a *security incident* and therefore also not equal to a *data leak*. A security leak is the discovery that there is a vulnerability within the security system. This should be taken very broadly. An example is anti-virus software which has not been updated. While it poses a risk, it has not yet caused an incident. The leak must of course be *rectified as quickly as possible* via the regular procedure. **Any employee** (internal/external) who detects a leak must report this immediately to the ICT Service desk and the CISO team. This can be done via the email addresses **servicedeskict@groningen-seaports.com** and **ciso@groningen-seaports.com**.

A security leak can of course result in a security incident. A security incident is therefore an undesirable or unexpected event which *can* result in a breach in the security of the availability, integrity or confidentiality of information at Groningen Seaports.

All employees (internal/external) are expected to **report** (possible) security incidents **without any delay** to the ICT Service desk and the CISO team. This can be done via the email addresses **servicedeskict@groningen-seaports.com** and **ciso@groningen-seaports.com**.

Together with the CISO team, the service desk will determine what actions are required and will call in any other (external) parties who may be required. The full process with regard to security and privacy incidents is described in the document titled "security and privacy incidents[13]" which can be found in the CISO portal, accessible via the intranet.

6.2 When do we refer to a data leak?

A lost USB flash drive containing personal information, a lost or stolen laptop, or personal information being sent to the wrong email address. These are all examples of a (possible) data leak. The definition of a data leak therefore concerns whether there is unauthorised or unintended access to personal information. Extended lack of access to personal information is also included in this.

A data leak is therefore not necessarily preceded by a security leak and/or security incident.

In the unfortunate event of this happening, it must be **reported without delay** via **datalek@groningen-seaports.com**.

6.3 Communication regarding security incidents

The communication regarding security incidents is the responsibility of the CISO team. The CISO team coordinates with the various stakeholders on how and with whom to communicate. This process is described in more detail in the 'security and privacy incidents' document.

[13] manual-security and privacy incidents-1

6.4 Registration of security leaks and incidents

All security leaks and incidents are registered by the CISO team in the ‘security and privacy reporting’ register. Here, all information regarding such a report is stored. Access to this register is limited to the CISO team, the Information security team and the board of directors.

7. Rights and access to information

7.1 Need to know

As indicated earlier, all information processed by or at Groningen Seaports is designated as corporate confidential, unless otherwise classified. Access is therefore limited to authorised persons.

This does not mean that all information within Groningen Seaports is then accessible to all persons. Only that information required to execute a particular task is accessible. Exceptions can be made in the event that sharing or providing limited access to information is in the best interests of the organisation. The owner of the information determines whether information specifically relevant to the task may be shared or access be granted.

7.2 Least privilege

Furthermore, Groningen Seaports applies the 'Leased Privilege' principle. Employees are only granted the rights necessary to execute their designated tasks.

8. Periodic assessment

8.1 Targets and Key Performance Indicators (KPIs)

Groningen Seaports believes strongly in continuous improvement of the quality of information security. Information security targets are therefore defined in order to determine that such improvement indeed occurs. By coupling KPIs to this improvement process, it becomes possible to monitor whether Groningen Seaports is on the right road to achieving the set targets. The targets and KPIs with regard to information security are described in the manual for information security.

8.2. Reporting

The CISO will provide the board of directors with a quarterly report, giving the progress of the set KPIs for information security, along with a general picture regarding information security over the past three months.

Once every three months, the CISO team will meet with the Board of Directors to discuss the report and to look ahead to the coming period.

This will provide the Board of Directors with adequate information at all times, allowing for adjustment when necessary.

Glossary

- Availability: accessibility and usability of information at the time at which it is required.
- Integrity: the correctness, currency and comprehensiveness of information.
- Confidentiality: only authorised access to information.

Reference list

- CISO portal on the intranet: https://groningenseaportsnv.sharepoint.com/sites/CISO
- Generally available information security documents: https://groningenseaportsnv.sharepoint.com/sites/CISO/Gedeelde%20documenten/Forms/AllItems.aspx
    - plan-level of information security-1
    - policy-data classification-1
    - manual-information security employees-1
    - policy-infosec requirements suppliers-1
- Secure environment for the CISO team, Information security team and board of directors: https://groningenseaportsnv.sharepoint.com/sites/Informatiebeveiliging
    - manual-information security-1
    - inventory-infosec risk register-1
    - Processing register (based on Microsoft Lists)
- GDPR text: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&rid=1
- Samenwerking Noord: https://samenwerkingnoord.nl/kennisnetwerken/privacy-security

List of figures

Figure 1 - Risk assessment and handling process 11
Figure 2 - Visual representation of InfoSec organisation 13