



GRONINGEN SEAPORTS

Beleid voor informatiebeveiliging in
leveranciersrelaties

CONCEPT

Versiebeheer

Versie	Wijziging	Datum	Auteur
0.1	Initieel document	8 december 2022	Thijs Kromhout
0.2	Review en aanvullingen	15 december 2022	Pieter Meulenhoff
0.3	Opmerkingen verwerkt	27 januari 2023	Thijs Kromhout
0.4	Verwerken opmerkingen	15 mei 2023	Thijs Kromhout

Inhoudsopgave

Versiebeheer	2
Inhoudsopgave.....	3
1 Inleiding en achtergrond.....	4
1.1 Toepassingsgebied en reikwijdte.....	4
1.2 Leeswijzer	4
1.3 Definities.....	4
2 Voorwaarden voor gebruik of afname van product of dienst.....	5
2.1 Voorwaarden voor leveranciers aan Groningen Seaports	5
3 Voorwaarden voor tijdens het gebruik van product of dienst	6
3.1 Voorwaarden voor leveranciers aan Groningen Seaports	6
4 Voorwaarden na beëindiging gebruik product of dienst	7
4.1 Voorwaarden voor leveranciers aan Groningen Seaports	7
5 Beheer van veranderingen in dienstverlening van leveranciers	8

1 Inleiding en achtergrond

Dit document heeft als doel om er voor te zorgen dat het juiste niveau van informatiebeveiliging van diensten en bedrijfsmiddelen, geleverd of toegankelijk voor leveranciers, van de organisatie wordt gewaarborgd.

Het beschrijft de uitgangspunten en voorwaarden die Groningen Seaports stelt aan haar leveranciers en aan de eigen organisatie. Om toegang voor leveranciers tot informatie verwerkende faciliteiten te beheren heeft Groningen Seaports deze beheersmaatregelen vastgesteld en toegepast.

Groningen Seaports maakt dan ook alleen gebruik van leveranciers die een adequaat informatiebeveiligingsniveau kunnen aantonen.

De voorwaarden die Groningen Seaports met betrekking tot dit aspect stelt aan leveranciers en aan Groningen Seaports, staan in dit document beschreven. Om de voorwaarden met leveranciers te delen dient gebruik gemaakt te worden van een ander document daar dit document als bedrijfsvertrouwelijk is gemarkeerd. Het openbaar te delen document is in dezelfde locatie te vinden.

1.1 Toepassingsgebied en reikwijdte

De geïmplementeerde beheersmaatregelen hebben betrekking tot alle door Groningen Seaports vastgestelde processen en procedures, en op de processen en procedures waarvan Groningen Seaports eist dat de leveranciers van Groningen Seaports deze implementeren.

1.2 Leeswijzer

De opbouw van het document is terug te vinden in de inhoudsopgave. Verder worden er de volgende rollen en definities gebruikt.

1.3 Definities

- Software Bill of Materials (SBOM): Een SBOM is een geneste inventaris, een lijst met ingrediënten waaruit softwarecomponenten bestaan;
- ISO/IEC 27001: Internationale erkende norm voor het opzetten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging binnen de context van de organisatie;
- SOC2 Type 1 / Type 2: Rapport opgesteld volgens ISAE 3000-standaard. Een SOC 2 spitst zich toe op de uitbestede IT-processen van IT-serviceorganisaties;
- Service level agreement (SLA): Een SLA is een overeenkomst tussen twee of meer partijen, waarbij de ene de klant is en de andere de dienstverlener.

2 Voorwaarden voor gebruik of afname van product of dienst

2.1 Voorwaarden voor leveranciers aan Groningen Seaports

- Een leverancier beschikt over een geldig ISO/IEC27001 certificaat.
 - De bijbehorende Verklaring van Toepasselijkheid (VVT) dient ook overlegd te worden.
- Indien een leverancier niet over een geldig ISO/IEC27001 certificaat beschikt is een ISAE3000 – SOC2 type 1 + 2 rapport (TPM) ook akkoord.
 - Indien een leverancier geen ISAE3000 rapport heeft maar wel een ISAE3402 rapport, dan is dit ook akkoord.
- Leveranciers hebben een wijzigingsbeheerproces welke zorgt voor voorafgaande kennisgeving aan Groningen Seaports en de mogelijkheid voor Groningen Seaports om wijzigingen niet te accepteren;
- Het recht van Groningen Seaports om een bijgewerkte “Software Bill of Materials” op te vragen bij de leveranciers waarin alle gebruikte software onderdelen staan. Dit om een goede risico inschatting te kunnen maken;
- Indien een leverancier gebruik maakt van een toeleverancier voor haar eigen dienstverlening, dan regaderen alle contractuele verplichtingen die op basis van de overeenkomst met leverancier zijn overeengekomen, ook haar toeleveranciers. De leverancier dient aan te tonen dat deze verplichtingen zijn doorvertaald in haar eigen overeenkomst met betreffende toeleverancier;
- Indien van toepassing laat de leverancier periodiek (minimaal jaarlijks) een technisch beveiligingsonderzoek (penetratietest) uitvoeren en rapporteert daarover aan Groningen Seaports;
- De te leveren applicatie of dienst heeft bij voorkeur een functie om de automatische installatie van security updates mogelijk te maken;
- Leveranciers welke data van Groningen Seaports beheren dragen zorg voor een back-up van deze data zodat de data te allen tijde teruggezet en gebruikt kan worden zonder dat er dataverlies optreedt.

3 Voorwaarden voor tijdens het gebruik van product of dienst

3.1 Voorwaarden voor leveranciers aan Groningen Seaports

- Leveranciers hebben de verplichting tot het actief melden van beveiligingsincidenten en datalekken bij Groningen Seaports. Afspraken over hoe en waar leveranciers dit melden dienen in overeenkomsten vastgelegd worden;
- Leveranciers welke data van Groningen Seaports beheren voeren periodieke restore tests uit en leveren het bewijs hier van aan Groningen Seaports. Dit laat overigens onverlet dat Groningen Seaports ook zelf hier initiatief voor kan starten;
- De directie van Groningen Seaports verwacht van haar leveranciers dat de eisen van de overeenkomst, in het bijzonder de informatiebeveiligingseisen, foutloos worden nagekomen;
- Het recht van Groningen Seaports op het uitvoeren van een audit bij de leverancier, ter zake het nakomen van contractueel vastgelegde afspraken en security-audits;
- Groningen Seaports kan minimaal jaarlijks een rapportage over de kwaliteit van de dienstverlening bij haar leveranciers opvragen waarin staat beschreven of de dienstverlening op het niveau is overeenkomstig de gemaakte afspraken.

4 Voorwaarden na beëindiging gebruik product of dienst

4.1 Voorwaarden voor leveranciers aan Groningen Seaports

- Bij beëindiging van het gebruik van het product of de dienst stelt de leverancier de aanwezige data aan Groningen Seaports beschikbaar. De data dient op een dusdanige manier aangeboden te worden zodat deze in een andere applicatie eenvoudig geïmporteerd en uitgelezen kan worden.
- Na acceptatie en akkoord van Groningen Seaports voor het ontvangen van de leesbare data zal de leverancier de data, conform de gemaakte afspraken verwijderen.

5 Beheer van veranderingen in dienstverlening van leveranciers

Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.

- Groningen Seaports beoordeelt, indien nodig, de veranderingen in de dienstverlening van haar leveranciers. Dit kan door evaluatiemomenten met de leveranciers te organiseren. Groningen Seaports controleert en monitort, in die gevallen, de veranderingen in de dienstverlening van haar leveranciers.
- Groningen Seaports houdt rekening mee met de volgende aspecten, indien de dienstverlening, scope of doelstellingen van de leverancier zijn veranderd:
 - Handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging;
 - Noodzakelijke veranderingen in de leveranciersovereenkomsten;
 - Herbeoordeling of de nieuwe situatie voldoet aan de beveiligingseisen van Groningen Seaports en draagt bij het behalen van de doelstellingen van Groningen Seaports.