

Informatiebeveiligingsbeleid voor leveranciersrelaties

Eigenaar Executive Committee (ExCo)
Auteurs Afdeling Cybersecurity

Kenmerk IBP-O.04
Versie 1.93

Datum November 2024

Bestand Informatiebeveiligingsbeleid voor leveranciersrelaties ProRail

Status Definitief

Informatieclassificatie Intern

Inhoud

1	Doel document, toepassingsgebied en gebruikers	4
2	Beleidsuitgangspunten informatiebeveiliging in leveranciersrelaties	4
3	Verantwoordelijkheden van ProRail in de leveranciersrelatie	6
4	BIO/ISO	7
	Bijlage A Afkortingen en termen	8
	Bijlage B Categorisering leveranciers	9

Versiebeheer en distributie

Versiebeheer			
Versie	Datum	Wijziging	Auteur
1.9	21-04-2024	Nieuwe opzet	Afdeling Cybersecurity
1.91	7-05-2024	Reviewcommentaar verwerkt van J-P. van Eekelen, M. de Heuvel, J. Petit, R. Rensman	Afdeling Cybersecurity
1.92	14-06-2024	Reviewcommentaar verwerkt van A. Westendorp, M. de Heuvel, H. Taibi	Afdeling Cybersecurity
1.93	11-11-2024	Structuur document aangepast, herziening/verplaatsing beleidsitems die in feite eisen zijn.	Afdeling Cybersecurity

Distributie		
Versie	Datum	
1.9	21-04-2024	ISM's afdeling Cybersecurity, J-P. van Eekelen, A. Westendorp, E. Hilgenga, R. Boot, M. de Heuvel, R. Rensman
1.91	7-05-2024	Interne versie afdeling Cybersecurity
1.92	14-06-2024	Afdeling Cybersecurity, J-P. van Eekelen, A. Westendorp, E. Hilgenga, R. Boot, M. de Heuvel, R. Rensman, H. Taibi, M. Lacomblé
1.93	11-11-2024	J. Petit, S. van der Aa, C. de Jong, E-J Korving, H. Taibi

1 Doel document, toepassingsgebied en gebruikers

In dit document worden doelstellingen, het toepassingsgebied, basisregels en uitgangspunten voor informatiebeveiliging in relatie tot leveranciersrelaties beschreven.

De scope van dit beleid omvat het Informatie Technologie (IT)- en Operationele Technologie (OT)-domein en richt zich op leveranciers en uitbestedingspartners (in dit document verder genoemd: leverancier),

- die toegang hebben tot en/of diensten verlenen ten behoeve van informatiesystemen, OT-objecten en informatie/data/gegevens(verzamelingen),
 - die gebruikt, verstrekt of bewaard wordt door of namens ProRail,
 - door medewerkers van deze partijen in de breedste zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Met ProRail wordt bedoeld de ProRail organisatie en de onder haar gestelde (dochter)ondernemingen.

Interne doelgroepen van dit document zijn op de eerste plaats de ProRail medewerkers die het beleid en eisen voor informatiebeveiliging in relatie tot leveranciersrelaties toepassen en beheren, zoals tendermanagers, contractmanagers, juristen, information security officers en security coördinatoren, projectleiders, product owners, etc.

Voor extern gebruik is een apart document beschikbaar 'Informatiebeveiligingsbeleid en– eisen voor leveranciersrelaties', met de classificatie Publiek/Openbaar. Dit document kan ter beschikking gesteld worden aan leveranciers in het kader van inkoop en aanbestedingstrajecten en de uitvoering van de gecontracteerde dienstverlening.

2 Beleidsuitgangspunten informatiebeveiliging in leveranciersrelaties

In het kader van informatiebeveiliging in leveranciersrelaties hanteert ProRail de volgende algemene uitgangspunten:

1. **ProRail is en blijft eindverantwoordelijk** voor de informatiebeveiliging van de producten en dienstverlening die binnen de organisatie ingezet worden. ProRail draagt daarom zorg voor de toetsing van de dienstverlening en ziet actief toe op een goede bescherming van de informatie door de leverancier.
2. **Het informatiebeveiligingsbeleid van ProRail is leidend.** Over onderwerpen waar ProRail geen beleid heeft of waar de leverancier ander beleid heeft wordt overleg gepleegd en gemaakte afspraken worden gedocumenteerd. De voor de dienstverlening relevante onderdelen van het informatiebeveiligingsbeleid worden verwerkt in plannen van eisen en contracten.
3. Het beleid en de eisen die ProRail stelt zijn in lijn met de voor ProRail **vigerende wet- en regelgeving** op het gebied van informatiebeveiliging.

Dit zijn:

 - Wet Beveiliging Netwerken en Informatiesystemen (WBNI) - tot in werkingtreding van de Cyberbeveiligingswet in 2025;
 - NIS2 – in werkingtreding per 17 oktober 2024;
 - Cyberbeveiligingswet, wetgeving op basis van NIS2 - per medio 2025;
 - ISO27001/2 - Informatiebeveiliging, met de BIO als Nederlandse verbijzondering voor de Overheid;
 - ISO22301 – Bedrijfscontinuïteit;
 - Algemene Verordening Gegevensbescherming (AVG);
 - IEC 62443, met de CSIR en BIACS als Nederlandse verbijzondering.

4. Informatiebeveiligingseisen worden door ProRail gespecificeerd voor **alle fasen van de levenscyclus** van een leveranciersrelatie: van aanbestedingsfase tot beëindiging van het contract.
5. Te stellen eisen, te nemen maatregelen en toetsing daarvan **zijn toegesneden op de risico's** die de gecontracteerde dienstverlening met zich mee brengt. ProRail hanteert daartoe het principe 'Pas toe of leg uit' en brengt leveranciers onder in risicocategorieën.

Pas toe of leg uit

Niet elke eis is toe te passen op elke leverancier en dienstverlening. Een ingenieurbureau is niet hetzelfde als een leverancier van cloudapplicaties. Daarom wordt bij de start van het inkoopproces door de eerste lijn een beredeneerde keuze gemaakt voor de te stellen eisen uit beleid en baselines. De afdeling Cybersecurity adviseert hierbij de eerste lijn en toetst in het proces op toepassing van beleid.

Risico categorieën

ProRail hanteert vier criteria waarmee het risiconiveau van de leveranciersrelatie gedefinieerd wordt en een risicocategorie wordt toegekend. Zie bijlage B.

- Business impact: de mate waarin de uitval of slecht functioneren van het product, dienst of de leverancier zelf een grote negatieve impact heeft op de bedrijfsprocessen van ProRail (beschikbaarheids-/continuïteitsrisico). Hiermee wordt ook een 1-op-1 relatie gelegd met het bedrijfscontinuïteitsbeleid.
- Werken aan/met missie- of businesskritieke systemen: de leverancier heeft als gebruiker/ontwikkelaar/beheerder toegang tot die systemen die een belangrijke rol spelen in de bedrijfsvoering van ProRail (beschikbaarheids- en integriteitsrisico).
- Toegang tot/verwerken van vertrouwelijke of geheime informatie: de leverancier heeft toegang (digitaal of papier) tot vertrouwelijke of geheime bedrijfsinformatie (incl. persoonsgegevens) en kan deze eventueel ook aanmaken, veranderen of wijzigen (vertrouwelijkheidsrisico).
- Verplichtingen vanuit wet- of regelgeving: de dienstverlening valt onder specifieke/aanvullende eisen die vanuit Europese of nationale wet- en regelgeving gesteld worden.

Afhankelijk van de 'score' op de vier criteria wordt de leverancier ingedeeld in een risicocategorie Hoog, Midden of Laag. De hoogste score bepaalt de categorie. Elke risicocategorie kent een eigen aanpak en frequentie bij de toetsing van de eisen gedurende de uitvoering van het contract en de afronding ervan.

Op hoofdlijnen:

Hoog	Jaarlijkse toetsing van de informatiebeveiligingseisen (persoonlijk contact, bedrijfsbezoek).
Midden	Tweejaarlijkse toetsing van de informatiebeveiligingseisen (schriftelijk)
Laag	Driejaarlijkse toetsing op basis van self-assessment

Indien de contractduur korter is dan drie jaar, dan worden specifieke afspraken gemaakt over het moment en frequentie van toetsing tussen de contractmanager en de afdeling Cybersecurity.

6. De eisen aan de leveranciersrelatie, zoals gespecificeerd in IPP-O.04, de IT en Ot Security Baselines en security architectuur en, indien van toepassing, de uitkomsten van een eventuele risicoanalyse vormen het minimale niveau van beveiliging voor de dienstverlening. Gezamenlijk vormen ze de input voor programma's van eisen en contracten.

3 Verantwoordelijkheden van ProRail in de leveranciersrelatie

Het beheersen van risico's in de toeleveringsketen is meer dan eisen stellen aan leveranciers. ProRail neemt in dit kader ook de verantwoordelijkheid om, naast het specificeren van passende informatiebeveiligingseisen, zelf actief toe te zien op en bij te dragen aan de uitvoerbaarheid en uitvoering van deze eisen. Dit vertaalt zich in onderstaande verantwoordelijkheden en acties voor de eerste lijn. Daar waar de afdeling Cybersecurity een (tweedelijns) taak heeft, is dat expliciet aangegeven.

A. Awareness	Iedere medewerker van de leverancier, met toegang tot de IT- of OT-systemen van ProRail, krijgt bij aanvang van de werkzaamheden door ProRail (afdeling Cybersecurity) schriftelijke informatie uitgereikt over de belangrijkste en relevante punten van het geldende informatiebeveiligingsbeleid, de security baselines en de Gedragscode ProRail, net zoals dit geldt voor ProRail medewerkers.
B. BIV-Classificatie (Informatiebeveiliging)	- Het vereiste niveau en de aard van beveiligingsmaatregelen wordt vastgesteld met een Beschikbaarheids-, Integriteits- en Vertrouwelijkheid- en Privacy (BIVP)-classificatie, en, bij hoge BIVP-classificatie, een risicoanalyse. - De BIVP-classificatie en, indien relevant, de risicoanalyse wordt periodiek door ProRail herijkt of wanneer interne of externe ontwikkelingen daar aanleiding toe geven. Indien de herijking dit vereist, worden de risico's en benodigde maatregelen herijkt in afstemming met de leverancier.
C. Business Impact Analyse (Bedrijfscontinuïteit)	- Met een Business Impact Analyse (BIA) of vergelijkbare methode is door ProRail vastgesteld: a. Welke processen van de leverancier (en eventuele onderaannemers) noodzakelijk zijn voor de levering/dienst aan ProRail en wat de mogelijke impact is van uitval van deze processen (na hoeveel tijd worden de gevolgen voor ProRail onacceptabel). b. Welke resources van de leverancier (en eventuele onderaannemers) noodzakelijk zijn (gebouwen, IT/OT systemen, machines, personeel, data, nutsvoorzieningen etc.). Welke risico's de beschikbaarheid of kwaliteit hiervan zodanig zouden kunnen bedreigen dat voor ProRail onacceptabele gevolgen kunnen optreden.
D. Controles vereist vanuit Rijksoverheid	- Bij het besluit om een leverancier wel of niet in te schakelen: a. worden De Cybercheck¹ en de Quickscan Nationale Veiligheid bij Inkoop en Aanbesteding² van de Rijksoverheid uitgevoerd; b. wordt van zowel leveranciers als hun onderaannemers nagegaan of er issues zijn met economische veiligheid (aandeelhouders uit China/Rusland/etc.).
E. Voorwaarden leverancier	In situaties waarin (technische en/of organisatorische) beveiligingseisen of contractvoorwaarden m.b.t. informatiebeveiliging worden opgelegd door een leverancier, wordt door ProRail door middel van een risicoafweging duidelijk gemaakt wat hiervan de consequenties zijn voor ProRail. Er wordt expliciet gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd dienen te zijn bij het aangaan van de overeenkomst.

¹ [Cybercheck voor risico's in supply chain - Digitale Overheid](#)

² [Toolbox veilig inkopen \(2024\) | Economische veiligheid | Nationaal Coördinator Terrorismebestrijding en Veiligheid](#)

F. Toetsing eisen en prestaties	• Met leveranciers zijn door ProRail eenduidige en gedocumenteerde afspraken (contract, SLA, etc.) gemaakt over veilige dienstverlening en eisen aan informatiebeveiliging en bedrijfscontinuïteit. • ProRail beoordeelt periodiek de naleving van de informatiebeveiligingseisen en bedrijfscontinuïteitseisen, als onderdeel van het contractmanagement. <u>Over de praktische uitvoering (wie doet wat plus inhoud toetsing) van de beoordeling worden afspraken gemaakt tussen contractmanager en de afdeling Cybersecurity.</u>
G. Monitoren en loganalyse	• Indien leverancier onbegeleid toegang heeft tot IT/OT en/of locaties van ProRail, voert ProRail regelmatige monitoring en/of loganalyse uit op deze toegang.
H. Toegang tot digitale infrastructuur en gegevens	• Periodiek wordt door ProRail een review uitgevoerd van de persoonlijke toegangsrechten van medewerkers van de gecontracteerde leverancier (en de derden die de leverancier inschakelt) voor de systemen bij ProRail en de leverancier die binnen de scope van de dienstverlening vallen. • Toegangsrechten tot informatiesystemen, OT-objecten en informatie/data/gegevens(verzamelingen) van ProRail van medewerkers van de leverancier die geen diensten (meer) verlenen aan ProRail worden per direct geblokkeerd. • Na beëindiging van de gecontracteerde werkzaamheden toetst ProRail of de rechten van de medewerkers van de leverancier ook daadwerkelijk zijn ingetrokken en bedrijfsmiddelen en gegevens zijn geretourneerd.
I. Security posture scanning	• De (internetfacing) infrastructuur van SaaS leveranciers en kritieke leveranciers wordt door ProRail periodiek geautomatiseerd gescand ter beoordeling van de kwaliteit van beveiliging (open poorten, verouderde protocollen, etc.), ook wel de 'security posture' genoemd.

4 BIO/ISO

Dit beleidsdocument beschrijft de invulling van de volgende beheersmaatregelen van de BIO:

- 5.19 Informatiebeveiliging in leveranciersrelaties
- 5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten
- 5.21 Beheren van informatiebeveiliging in de ICT-keten
- 5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
- 5.23 Informatiebeveiliging voor het gebruik van clouddiensten
- 6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten
- 8.30 Uitbestede systeemontwikkeling

Een aantal van deze beheersmaatregelen wordt verder ook uitgewerkt in de IT- en OT Security baselines van ProRail.

Bijlage A Afkortingen en termen

Assurance	Het bewijs dat afspraken, eisen e.d. ook daadwerkelijk in de praktijk zijn gebracht zoals ze zijn bedoeld c.q. het proces om daartoe te komen.
AVG	Algemene Verordening Gegevensverwerking
BCM	BedrijfsContinuïteitsManagement
BCMS	BedrijfsContinuïteitsManagementSysteem
BIACS	Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
CSIR	CyberSecurity Implementatie Richtlijn (Rijkswaterstaat)
IBP	InformatiebeveiligingsBeleid ProRail
IT	Informatie Technologie
IPP	InformatiebeveiligingsProcedure ProRail
ISMS	Information Security Management System
ISO	International Organization for Standardization
NIS2	Verordening Network and Information Systems
OT	Operationele Technologie
SLA	Service Level Agreement
Wbni	Wet beveiliging netwerken en informatiesystemen

Bijlage B Categorisering leveranciers

ProRail hanteert vier criteria waarmee het risiconiveau van de leveranciersrelatie gedefinieerd wordt en een risicocategorie wordt toegekend. Zie tabel 1.

Afhankelijk van de 'score' op de vier criteria wordt de leverancier ingedeeld in een risicocategorie (tier). De hoogste score bepaalt de categorie.

Classificatie	Business impact	Toegang tot gegevens	Werken aan systemen	Verplichtingen in de wet- en regelgeving
Hoog (Tier 1)	Veiligheid komt in het geding bij uitvallen leverancier/dienst. Cruciaal voor de operationele continuïteit (A + B) Moeilijk vervangbaar	Toegang tot gevoelige of vertrouwelijke/geheime gegevens	Beheer of ontwikkeling van missiekritieke of businesskritieke IT-systemen of infrastructuur	Regelgeving of wetgeving vereist een hoog niveau van beveiliging.
Midden (Tier 2)	Veiligheid komt niet direct in het geding bij uitvallen leverancier/dienst Ondersteunende rol in belangrijke maar niet-kritieke bedrijfsprocessen (C)	Toegang tot interne gegevens die niet als gevoelig of vertrouwelijk worden beschouwd.	Beheer of ontwikkeling van niet-kritieke systemen.	Wet- en regelgeving vereist naleving van standaard beveiligings- en onderhoudsnormen.
Laag (Tier 3)	Veiligheid komt niet in het geding bij uitvallen leverancier/dienst Geen invloed op de kritieke bedrijfsprocessen of de continuïteit ervan (D)	Enkel toegang tot openbare gegevens.	Werkt met ProRail systemen als Gebruiker.	Verplichtingen vanuit wet- en regelgeving zijn minimaal

Tabel 1. Risico categorieën