

Informatiebeveiligingsbeleid en -eisen voor leveranciersrelaties

Eigenaar	Executive Committee (ExCo)
Auteurs	Afdeling Cybersecurity
Kenmerk	IPP-O.04a
Versie	1.93
Datum	November 2024
Bestand	Informatiebeveiligingsbeleid voor leveranciersrelaties ProRail

Status	Definitief
Informatieclassificatie	Publiek/Openbaar

Inhoud

1	Doel document, toepassingsgebied en gebruikers	3
2	Beleidsuitgangspunten informatiebeveiliging in leveranciersrelaties	3
3	Verantwoordelijkheden van ProRail in de leveranciersrelatie	4
4	Eisen aan de leveranciersrelatie	6
	Bijlage A Afkortingen en termen	9
	Bijlage B Categorisering leveranciers	10

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.

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.
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 ingenieursbureau 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.

- De eisen aan de leveranciersrelatie, zoals gespecificeerd in dit document, de IT en OT Security Baselines, 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.
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

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

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

	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 Eisen aan de leveranciersrelatie

In onderstaande tabel zijn de eisen weergegeven die ProRail stelt aan een formele leveranciersrelatie.

Toepassing van de eisen volgt het principe 'Pas toe of leg uit', aangezien niet alle eisen op iedere leveranciersrelatie betrekking (kunnen) hebben. Bij het bepalen van het programma van eisen, de inkoopvoorwaarden en/of het contract wordt deze afweging gemaakt in overleg met de afdeling Cybersecurity.

De omschrijving van de eis geeft de essentie weer, niet de letterlijke verwoording zoals die in een contract e.d. opgenomen zou moeten zijn. Deze eisen zijn onderwerp van toetsing zoals in IBP-O.04 (Beleid voor leveranciersrelaties) beschreven is. Algemene eisen aan het product of dienst komen voort uit de Security baselines IT en OT en de toe te passen security architectuur. Specifieke eisen worden gesteld op basis van risicoanalyses.

A. AVG	Bij de verwerking van persoonsgegevens houdt de leverancier zich aan de eisen uit de Algemene Verordening Gegevensverwerking.
	Leveranciers dienen zich te conformeren aan de procedure Melding Datalekken van ProRail. Tijdlijnen, voorwaarden, contactpersonen, etc. worden opgenomen als onderdeel van de verwerkersovereenkomst.
	Met alle derde partijen die als verwerker voor of namens ProRail persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
	De leverancier verwerkt persoonsgegevens in voorkomende gevallen uitsluitend in opdracht en op basis van schriftelijke instructies van ProRail, tenzij er sprake is van andersluidende wettelijke voorschriften.
D. Certificeringen en normenkaders	Relevante certificaten (bv. ISO 27001/22301/IEC62443/BIACS) en/of assurance verklaringen (bv. SOC2, ISAE 3400/2) worden ter beschikking gesteld aan ProRail. De scope en inrichting van het ISMS en BCMS worden door ProRail getoetst op relevantie en effectiviteit.
E. Contactpersoon	Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in bijvoorbeeld de SLA. Deze contactpersonen zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contractmanager.

H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.
I. Gegevensverwerking en -opslag	De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden.
	Indien informatie opgeslagen wordt binnen de infrastructuur van de leverancier, dient deze beveiligd te worden conform het beveiligingsniveau dat bij deze informatie is overeengekomen. Dit betekent dat persoonsgegevens per definitie minimaal Vertrouwelijk geclassificeerd zijn. (Bij bijzondere persoonsgegevens : Geheim)
	De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligd werkstation waarbij lokale opslag niet mogelijk is en een beveiligde verbinding en multi-factor authenticatie gebruikt wordt. De data mogen de EER niet verlaten.
K. Incidenten	Er wordt een vaste procedure voor het melden van (IT en OT) beveiligingsincidenten en kwetsbaarheden afgesproken tussen ProRail en de leverancier. Deze dient aan te sluiten bij de bestaande incidentmanagementprocessen binnen ProRail.
	De leverancier meldt (beveiligings-)incidenten en kwetsbaarheden direct aan ProRail, en als dat wettelijk noodzakelijk is, ook aan de Autoriteit Persoonsgegevens. Bij niet-gemelde incidenten waar persoonsgegevens bij betrokken zijn, kan ProRail de leverancier in gebreke stellen.
L. Monitoren en loganalyse	Monitoring is ingericht voor alle IT- en OT-systemen. Wanneer monitoring niet mogelijk is of niet rendabel is, dan dient hiervoor een risico gebaseerde redeneerlijn te worden opgesteld. Monitoring van de remote toegang en beheer op afstand dient altijd te worden ingericht.
	Activiteiten van gebruikers en beheerders dienen ten behoeve van audittrailing passend beveiligd vastgelegd te worden in logboeken.
M. Onderaanneming en toeleveranciers	De leverancier dient inzicht te geven in welke derden mogelijk toegang kunnen hebben tot ProRail data. Denk aan hosting providers, softwareleveranciers, support partijen, subverwerkers, etc.
	Alle voorwaarden en eisen op het gebied van informatiebeveiliging die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
	De leverancier moet desgevraagd inzage geven in de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden.
	Het is de leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ProRail, de uitvoering van een contract geheel of gedeeltelijk aan derden over te dragen of uit te besteden, dan wel gebruik te maken van ter beschikking gestelde of ingeleende arbeidskrachten. Deze toestemming zal niet op onredelijke gronden geweigerd worden.

	ProRail wordt zo snel mogelijk op de hoogte gebracht indien de leverancier wijzigingen aanbrengt bij het uitbesteden van zijn eigen (deel)processen. Hierdoor kan ProRail bepalen of er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen in de wijze van beheersing van de door de leverancier uitbestede (deel) processen. Deze inzet, beheersing en wijziging van sub verwerking wordt opgenomen in de overeenkomst met de leverancier.
P. Retour/vernietiging bedrijfsmiddelen en informatie	Op verzoek retourneert of vernietigt de leverancier, dit naar keuze van ProRail, onverwijld alle door ProRail ter hand gestelde documenten, boeken, bescheiden en andere zaken (waaronder begrepen gegevensdragers en back-ups). Dit geldt ook voor alle gegevens, inclusief persoonsgegevens, ook in cloudomgevingen.
	Voorafgaand aan hergebruik of verwijdering van apparatuur dienen alle gegevens op de daarin aanwezige opslagmedia op betrouwbare wijze te worden verwijderd. Dit gebeurt door een hiertoe gecertificeerde organisatie. Als bewijs van verwijdering dient een certificaat door het vernietigingsbedrijf te worden aangeleverd.
S. Security en BCM by Design	De gangbare principes rondom Security by Design/Default en BCM by Design zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet binnen de opdracht inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
T. Security testing	ProRail kan een security test, zoals een penetratietest, laten uitvoeren als onderdeel van de acceptatie en/of validatie om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Een security test is niet nodig als de leverancier door middel van rapportages aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke security test heeft plaatsgevonden en de relevante resultaten deelt met ProRail.
	Indien ProRail in het kader van acceptatie of validatie een security test (laat) verricht(en), stelt ProRail zo spoedig mogelijk een testverslag op en zendt dat ondertekend aan Opdrachtnemer. In het testverslag worden geconstateerde bevindingen en gebreken vastgelegd alsook of ProRail de geteste asset goed- of afkeurt. Afspraken worden tussen ProRail en de leverancier gemaakt over de opvolging van de bevindingen.
U. Toegang tot digitale infrastructuur en gegevens	Er wordt een gedocumenteerde formele en actuele procedure afgesproken voor het registreren, verlenen, wijzigen en intrekken van logische toegang tot IT- en OT-systemen. Deze procedure wordt periodiek (minimaal eens per jaar) beoordeeld en geactualiseerd.
W. Wijzigingsbeheer	Substantiële wijzigingen van de leveranciersorganisatie en -processen met impact voor ProRail dienen door de leverancier tijdig kenbaar gemaakt te worden aan ProRail. Dit wordt opgenomen als onderdeel van de overeenkomst met de leverancier.

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