Informatiebeveiligingseisen voor leveranciersrelaties

Eigenaar	CISO ProRail
Auteurs	Afdeling Cybersecurity

Kenmerk	IPP-O.04
Versie	1.92
Datum	Juni 2024
Bestand	Informatiebeveiligingseisen voor leveranciersrelaties ProRail
Status	Definitief
Informatieclassificatie	Openbaar

Inhoudsopgave

1	Doel document, toepassingsgebied en gebruikers	3
2	Eisen	3
Bijlage A	Zorgplicht vanuit de NIS2	8
Bijlage B	Afkortingen en termen	9

1 Doel document, toepassingsgebied en gebruikers

In dit document worden de eisen voor informatiebeveiliging in leveranciersrelaties beschreven.

De eisen zijn toe te passen op het Informatie en Communicatie Technologie (ICT) - en Operationele Technology (OT)-domein en richten zich op:

- Leveranciers, uitbestedingspartners en ketenpartners (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 zijn gestelde (dochter)ondernemingen.

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

In bijlage B zijn de gebruikte afkortingen toegelicht.

Daarnaast kan dit document ter beschikking gesteld worden aan leveranciers In het kader van inkoop en aanbestedingstrajecten en de uitvoering van de gecontracteerde dienstverlening. Hiervoor is een aparte versie beschikbaar met de classificatie Openbaar.

2 Eisen

In onderstaande tabel zijn de eisen weergegeven die ProRail stelt aan een formele leveranciersrelatie.
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 assurance zoals in IBPO.04 (Beleid voor leveranciersrelaties, bijlage A) beschreven zijn. 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.

De bronnen voor deze eisen zijn:

- De Wet beveiliging netwerken en informatiesystemen (Wbni);
- De tweede Europese richtlijn Netwerken en Informatiesystemen (NIS2);
- De ISO27002 norm voor Informatiebeveiliging;
- De ISO22301 norm voor Bedrijfscontinuïteit en de sub normen;
- De Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen (BIACS);
- De Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT2022);
- De handreikingen van de Informatiebeveiligingsdienst.

IB-eis	Omschrijving
A. Awareness	• De leverancier wordt vooraf bewust gemaakt van risico's m.b.t. informatiebeveiliging en het belang hiervan voor de bedrijfsprocessen van ProRail. De relevante informatie uit het informatiebeveiligingsbeleid wordt aangereikt in de aanbestedingsfase, relevantie wordt bepaald in overleg met de afdeling Cybersecurity. • Iedere medewerker van de leverancier, met toegang tot de IT- of OT-systemen van ProRail, krijgt bij aanvang van de

	werkzaamheden schriftelijke informatie over de belangrijkste en relevante punten van het geldende informatiebeveiligingsbeleid, de security baselines en de Gedragscode ProRail, net zoals dit geldt voor ProRailmedewerkers. • De leverancier zorgt ervoor dat gedurende de uitvoering van het contract zijn medewerkers regelmatig en aantoonbaar op het belang van informatiebeveiliging worden gewezen (security awareness).
B. Bedrijfscontinuïteit	• De leverancier heeft BCM-beleid opgesteld t.a.v. zijn continuïteitsdoelstellingen, - organisatie en -strategie en deelt dit met ProRail • De leverancier heeft aantoonbaar en actueel inzicht in de risico's in zijn bedrijfsprocessen die een bedreiging zouden kunnen vormen voor de continuïteit en/of veiligheid van de bedrijfsprocessen van ProRail. • De leverancier heeft aantoonbaar adequate maatregelen genomen om de continuïteitsrisico's voor de eigen en de bedrijfsprocessen van ProRail te voorkomen (preventie), dan wel de impact op de bedrijfsvoering te beperken (repressie). Deze maatregelen zijn opgenomen in bedrijfscontinuïteitsplannen. • Minimaal dient voor elke ICT- of OT-asset conform een ingericht back-up proces na elke (functionele) systeemwijziging of na een vastgesteld periodiek termijn een back-up te worden gemaakt. Indien het om welke reden dan ook niet mogelijk is om een back-up te maken, dan wordt dit vastgelegd en, op basis van een risicoanalyse, een alternatieve werkwijze gekozen en beschreven. • De genomen maatregelen worden actueel en effectief gehouden door het uitvoeren van hiervoor geschikte tests en oefeningen. • De leverancier is aantoonbaar in staat een ernstige crisis te managen doordat deze een crisis/BCM-organisatie heeft ingericht en onderhoudt. • Indien relevant en mogelijk, wordt ProRail betrokken bij oefeningen en testen.
C. Configuratiemanagement	Alle ICT/OT-componenten en –diensten, inclusief de onderlinge relaties en classificaties, worden vastgelegd en dit overzicht wordt onderhouden (indien van toepassing) door de leverancier. De registratie voldoet aan de eisen die ProRail stelt aan configuratiemanagement.
D. Contactpersoon	Zowel ProRail als de leverancier hebben een contactpersoon voor informatiebeveiligingsaspecten, vastgelegd in de SLA. Deze zijn adviserend en ondersteunend aan het contract- en leveranciersmanagementproces. Afstemming vindt altijd plaats onder regie van de contracteigenaar.
E. Escrow	De leverancier draagt zorg voor een escrow regeling, indien relevant. Zo heeft ProRail in voorkomend geval de mogelijkheid om bij het in vervulling gaan van één of meer in de escrow genoemde voorwaarden, software die onderdeel is van het contract, eigenmachtig te (laten) gebruiken voor het herstellen van fouten en anderszins het onderhouden en beheren van de standaardprogrammatuur.
F. Exit clausule	De leverancier beschikt over een expliciete uitwerking van een exit-strategie, die goedgekeurd is door ProRail. Deze strategie omvat minimaal afspraken over hoe de data overgedragen en daarna verwijderd/vernietigd wordt bij wisseling van leverancier of overname van de dienst door ProRail.

G. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een standaard- en beveiligde manier. Verbindingen zijn ingericht en worden onderhouden conform de standaarden van ProRail.
H. Gegevensverwerking	• De leverancier maakt alleen gebruik van de verstrekte en gegenereerde gegevens voor het uitvoeren van de gecontracteerde werkzaamheden. • De websites, servers en databasesystemen met alle daarop opgeslagen informatie bevinden zich fysiek binnen de Europese Economische Ruimte (EER) en deze mogen alleen vanuit een locatie buiten de EER toegankelijk zijn en/of bewerkt worden vanaf een beveiligde verbinding met multi-factor authenticatie. De data mogen de EER niet verlaten. • Indien informatie opgeslagen wordt binnen de infrastructuur van de leverancier, dan 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 de verwerking van persoonsgegevens houdt de leverancier zich aan de eisen uit de Algemene Verordening Gegevensverwerking.
I. Incidenten	• Er dient een vaste procedure voor het melden van (ICT en OT) beveiligingsincidenten en kwetsbaarheden te zijn afgesproken. • 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. • De leverancier beëindigt (beveiligings-)incidenten en kwetsbaarheden zo spoedig mogelijk en rapporteert daarover aan ProRail.
J. 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 over de maatregelen die hij genomen heeft om de aan hem opgelegde eisen ook door te vertalen naar derden. • Het is de leverancier verboden, 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 over er zwaarwegende risico's bestaan (bv. uitbesteding aan onveilige landen) en tevens inzicht verkrijgen door ProRail 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.
K. Personeel	• Medewerkers van de leverancier overleggen voor aanvang van de werkzaamheden bij ProRail een recente Verklaring Omtrent

	het Gedrag (VOG) conform de eisen uit het ProRail beleid. De leverancier stemt met ProRail voorafgaand de noodzaak en de wijze van overleggen en beheren af. • ProRail kan het personeel van de leverancier dat voor de uitvoering van het contract is of wordt ingeschakeld, aan een veiligheidsonderzoek, overeenkomstig de bij ProRail gebruikelijke regels, (doen) onderwerpen. De leverancier verleent aan dat onderzoek zijn volledige medewerking. ProRail kan op grond van de uitkomsten daarvan de inzet van het betrokken personeelslid bij de uitvoering van de overeenkomst weigeren. • De leverancier toont aan dat het personeel voldoende kennis en kunde heeft om de werkzaamheden binnen ProRail te verrichten. Dit hangt samen met beveiligingseisen, die bijvoorbeeld door scholing en/of voldoende kennis en kunde gebruikersfouten beperken. • Extern personeel dient zich net zo goed te houden aan de gedragsregels van ProRail als een ProRail medewerker. • Indien een medewerker van de leverancier, die door zijn werkzaamheden op locatie van ProRail komt en/of toegang heeft tot infrastructuren en gegevens, uit dienst gaat, wordt dit minimaal twee weken van tevoren gemeld aan de contractmanager van ProRail. • Toegangsrechten tot informatie van ProRail van medewerkers van de leverancier die geen diensten (meer) verlenen aan ProRail worden per direct geblokkeerd.
L. 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.
M. Risicomanagement	• De gecontracteerde leverancier dient gedurende de looptijd van het contract te beschikken over een actuele, gedocumenteerde en door zijn management geaccordeerde risicoanalyse, uitgevoerd voor de te leveren ICT-en OT-diensten. Bij deze risicoanalyse moeten de bedreigingen voor de bedrijfsmiddelen, kwetsbaarheden en de invloeden op de continuïteit van de bedrijfsprocessen van ProRail zijn vastgesteld en het bijbehorende risiconiveau te zijn bepaald. • Beheersmaatregelen die voortkomen uit de risicoanalyse en waar ProRail een aandeel in heeft, zijn afgestemd met ProRail.
N. Security en BCM by Design	De gangbare principes rondom Security by design en BCM by Design zijn uitgangspunt voor de ontwikkeling van software en systemen. Over wat dit concreet inhoudt worden afspraken gemaakt tussen ProRail en de leverancier.
O. 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 het geteste asset goed- of afkeurt.

Bijlage A Zorgplicht vanuit de NIS2

Onder de NIS2 is sprake van een zorgplicht van organisaties voor informatiebeveiliging. Deze komt neer op het uitvoeren en actueel houden van een risicomanagement. Op basis hiervan dienen organisaties passende maatregelen te nemen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en hun informatie te beschermen.

Deze zorgplicht geldt voor ProRail, maar wordt door ProRail ook gevraagd van zijn leveranciers. Onderstaande tabel bevat de tien punten van de zorgplicht (bron: NCSC) en de eisen waarmee ProRail deze in zijn leveranciersrelatie geborgd heeft. **Het is van belang om te beseffen dat niet alleen de eisen uit dit document voor die borging zorgen, maar ook ander beleid, security baselines, afspraken, richtlijnen, e.d.**

Deze tien punten zijn per definitie onderwerp van gesprek bij het verkrijgen van assurance van kritieke leveranciers.

NIS2 eisen	Borging door
1. Een risicoanalyse en beveiliging van informatiesystemen	M. Risicomanagement
2. (Beleid en procedures over) incidentenbehandeling	I. Incidenten
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen	B. Bedrijfscontinuïteit F. Exit clausule
4. Beveiliging van de toeleverancierskeketen	Dit document en het bijbehorende beleid.
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden	E. Escrow H. Gegevensverwerking N. Security en BCM by Design
6. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen	O. Security testing
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging	A. Awareness
8. Beleid en procedures over het gebruik van cryptografie en encryptie	G. Gegevensuitwisseling
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa	C. Configuratiemanagement J. Onderaanneming en toeleveranciers K. Personeel L. Retour/vernietiging bedrijfsmiddelen en informatie
10. Het gebruik van multifactor-authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit	G. Gegevensuitwisseling

Bijlage B 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
BIACS	Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen
CSIR	CyberSecurity Implementatie Richtlijn (Rijkswaterstaat)
IBP	InformatiebeveiligingsBeleid ProRail
ICT	Informatie en Communicatie Technologie
IPP	InformatiebeveiligingsProcedure ProRail
ISO	International Organization for Standardization
NIS2	Verordening Network and Information Systems
OT	Operationele Technology
SLA	Service Level Agreement
Wbni	Wet beveiliging netwerken en informatiesystemen