

Awareness | B | B.1

Alle personeel en derden van leverancier die betrokken zijn bij de uitvoering van het contract worden periodiek, tenminste eenmaal per jaar, getraind op security awareness.

Wet- en regelgeving, certificeringen en normenkaders | D | D.1

De leverancier voldoet aan alle toepasselijke wet- en regelgeving op het gebied van informatiebeveiliging en privacy, waaronder, maar niet gelimiteerd tot, de Cyberbeveiligingswet, de Cyber Resilience Act en de Algemene Verordening Gegevensbescherming (AVG).

Wet- en regelgeving, certificeringen en normenkaders | D | D.2

De leverancier dient gedurende de looptijd van het contract te voldoen aan de normen inzake kwaliteitsbewaking NEN-ISO 27001 of een gelijkwaardig informatiebeveiligingsmanagementsysteem en dient te beschikken over een geldig certificaat dat is afgegeven door een onafhankelijke instantie die voldoet aan de Europese normenreeks NEN/ISO 27001 (of een gelijkwaardig certificaat, afgegeven door een instituut binnen de EU; dit naar het oordeel van ProRail). De leverancier deelt het certificaat met bijbehorende verklaring van toepasselijkheid met ProRail.

Contactpersoon | E | E.1

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 ProRail contractmanager.

Gegevensuitwisseling | H | H.1

Digitale gegevensuitwisseling vindt plaats via beveiligde verbindingen die voldoen aan actuele en algemeen geaccepteerde beveiligingsstandaarden en richtlijnen, zoals de relevante richtlijnen van het NCSC.

Gegevensverwerking en -opslag | I | I.1

De leverancier gebruikt door ProRail verstrekte en tijdens de dienstverlening gegenereerde gegevens uitsluitend voor het uitvoeren van de gecontracteerde werkzaamheden en niet voor andere doeleinden. De leverancier treft aantoonbaar passende technische en organisatorische maatregelen om ongeoorloofd gebruik, toegang, wijziging, verstrekking of verlies van gegevens te voorkomen.

Gegevensverwerking en -opslag | I | I.2

De leverancier mag ProRail-informatie uitsluitend verwerken met behulp van AI-tools indien wordt gewaarborgd dat deze informatie niet wordt gebruikt voor

trainingsdoeleinden van de AI-aanbieder, niet wordt gedeeld met derden buiten de overeengekomen dienstverlening en wordt verwerkt binnen de EER, conform de geldende informatiebeveiligingseisen van ProRail.

Gegevensverwerking en -opslag | I | I.3

Informatie die wordt opgeslagen binnen de infrastructuur van de leverancier, beveiligt de leverancier deze conform het met ProRail overeengekomen classificatieniveau.

Persoonsgegevens worden minimaal als ‘Vertrouwelijk’ geclassificeerd en bijzondere persoonsgegevens als ‘Geheim’. De leverancier treft aantoonbaar passende technische en organisatorische maatregelen die aansluiten bij deze classificatie. Hierbij kan onder meer worden gedacht aan toegangsbeveiliging, versleuteling, logging en monitoring, autorisatiebeheer, backup voorzieningen en periodieke controlemaatregelen.

Gegevensverwerking en -opslag | I | I.4

Gegevens van ProRail worden uitsluitend verwerkt en opgeslagen binnen de Europese Economische Ruimte (EER) en mogen de EER niet verlaten.

Toegang tot deze gegevens vanuit locaties buiten de EER is uitsluitend toegestaan indien dit plaatsvindt via beveiligde werkstations waarbij lokale opslag is uitgesloten.

De leverancier borgt dat deze toegang plaatsvindt via een beveiligde verbinding en met toepassing van multi-factor authenticatie en kan op verzoek aantonen dat aan deze eisen wordt voldaan.

Geheimhouding | J | J.1

Ter waarborging van de vertrouwelijkheid van als ‘Vertrouwelijk’ en/of ‘Geheim’ geclassificeerde informatie wordt tussen ProRail en de leverancier een geheimhoudingsverklaring (NDA) of gelijkwaardige overeenkomst gesloten. De leverancier verplicht medewerkers die betrokken zijn bij de uitvoering van de overeenkomst tot naleving van deze geheimhoudingsverplichting.

Incidenten | K | K.1

Bij constatering van een kwetsbaarheid, beveiligingsincident of datalek dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail en de betreffende contractmanager.

Incidenten | K | K.2

De leverancier geeft (beveiligings-)incidenten volgens gemaakte afspraken opvolging en rapporteert daarover aan ProRail.

Monitoren en loganalyse | L | L.1

De leverancier richt monitoring in voor alle software die onderdeel uitmaken van de dienstverlening aan ProRail, inclusief onderliggende infrastructuur, netwerkcomponenten en beheertoegang. Deze monitoring is gericht op het detecteren van beveiligingsincidenten, afwijkingen en ongeautoriseerde activiteiten.

Indien monitoring voor specifieke systemen aantoonbaar niet mogelijk of proportioneel is, stelt de leverancier een risico-gebaseerde onderbouwing op en treft passende compenserende maatregelen.

Monitoring van remote toegang en beheer op afstand wordt altijd ingericht en omvat minimaal logging en controle op authenticatie, autorisatie en uitgevoerde handelingen.

Monitoren en loganalyse | L | L.2

De leverancier legt relevante activiteiten van gebruikers en beheerders vast in logbestanden ten behoeve van audittrails. Deze loggegevens worden passend beveiligd tegen ongeautoriseerde toegang, wijziging en verwijdering. De logging omvat, voor zover relevant voor de dienstverlening, gebeurtenissen zoals authenticatiepogingen, toegangsverlening, wijzigingen in autorisaties, beheerdershandelingen en beveiligingsrelevante gebeurtenissen.

De leverancier stelt op verzoek passende loggegevens, auditinformatie of managementinformatie beschikbaar aan ProRail.

Onderaanneming en toeleveranciers | M | M.1

De leverancier draagt de uitvoering van de overeenkomst geheel of gedeeltelijk niet over aan derden, waaronder onderaannemers en ingeleende arbeidskrachten, zonder voorafgaande schriftelijke toestemming van ProRail. ProRail zal deze toestemming niet op onredelijke gronden weigeren.

Onderaanneming en toeleveranciers | M | M.2

De leverancier verstrekt inzicht in alle derden die (mogelijk) toegang hebben tot gegevens van ProRail, waaronder hostingproviders, softwareleveranciers, supportpartijen en subverwerkers. De leverancier houdt een actueel overzicht bij van deze partijen, inclusief de aard van de toegang en de verwerkingsactiviteiten, en stelt dit overzicht voor contractering aan ProRail beschikbaar.

Onderaanneming en toeleveranciers | M | M.3

De leverancier informeert ProRail voorafgaand aan voorgenomen wijzigingen in de uitbesteding van (deel)processen, waaronder wijzigingen in subverwerkers of onderaannemers. De leverancier verstrekt daarbij inzicht in de aard van de uitbesteding, de betrokken partijen en de getroffen beheersmaatregelen.

Onderaanneming en toeleveranciers | M | M.4

De leverancier borgt dat alle informatiebeveiligingseisen en -voorwaarden die op hem van toepassing zijn, onverkort worden doorgelegd aan derden die in opdracht van de leverancier diensten verrichten voor ProRail. De leverancier legt deze verplichtingen contractueel vast en deelt deze op verzoek met ProRail.

Personeel | O | O.3

De leverancier toont aan dat personeel dat werkzaamheden verricht voor ProRail beschikt over aantoonbare kennis en vaardigheden die passend zijn bij de aard van de werkzaamheden en de geldende informatiebeveiligingseisen. De leverancier draagt zorg voor passende opleiding en training, gericht op het beperken van gebruikersfouten en het waarborgen van veilig handelen.

Personeel | O | O.5

Personeel van de leverancier dat werkzaamheden verricht voor ProRail houdt zich aan de geldende gedragsregels van ProRail, zoals opgenomen in de Gedragscode van ProRail (beschikbaar via de website van ProRail), en handelt in lijn met de daarin opgenomen principes, waaronder integriteit, onafhankelijkheid en zorgvuldige omgang met informatie. De leverancier borgt dat het personeel voorafgaand aan de werkzaamheden over deze regels is geïnformeerd.

Retour/vernietiging bedrijfsmiddelen en informatie | P | P.1

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.

Retour/vernietiging bedrijfsmiddelen en informatie | P | P.2

Voorafgaand aan hergebruik, afvoer of verwijdering van apparatuur zorgt de leverancier ervoor dat alle gegevens op aanwezige opslagmedia op betrouwbare en onherstelbare wijze worden verwijderd, conform een erkende standaard (zoals NIST SP 800-88 of gelijkwaardig). Afhankelijk van het classificatieniveau van de gegevens wordt gekozen voor passende methoden, zoals logisch wissen of fysieke vernietiging.

Auditrecht | Q | Q.1

ProRail kan op enig moment een audit (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit is niet nodig als de leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, dan wel aantoont dat een onafhankelijke audit heeft plaatsgevonden en de relevante resultaten deelt met ProRail.

Auditrecht | Q | Q.2

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.

Risicomanagement | R | R.1

De leverancier vult direct na contractering een self-assessment in waaruit de mate van beveiliging blijkt, met als kader het beveiligingsbeleid van ProRail.

Risicomanagement | R | R.2

De leverancier beschikt gedurende de looptijd van de overeenkomst over een actuele, gedocumenteerde en door het management geaccordeerde classificatie en risicoanalyse voor de geleverde software.

In deze risicoanalyse worden relevante bedreigingen, kwetsbaarheden en risico's met betrekking tot de geleverde dienstverlening geïdentificeerd en beoordeeld. Op basis hiervan wordt het bijbehorende risiconiveau vastgesteld en worden waar nodig passende beheersmaatregelen getroffen. De leverancier dient op verzoek aan te tonen dat deze risicoanalyse actueel is en wordt toegepast.

Risicomanagement | R | R.3

Beheersmaatregelen die voortkomen uit de risicoanalyse en waar ProRail een aandeel in de implementatie heeft, worden afgestemd met ProRail.

Risicomanagement | R | R.4

De leverancier verstrekt op verzoek van ProRail volledig en actueel inzicht in de getroffen beheersmaatregelen die van toepassing zijn op de dienstverlening, inclusief relevante documentatie en bewijs van implementatie en werking. De leverancier licht desgevraagd toe hoe deze maatregelen zijn ingericht, toegepast en gemonitord.

Risicomanagement | R | R.5

De leverancier beschikt over een gedocumenteerd patchmanagementproces waarbij beveiligingsupdates en patches risicogebaseerd worden beoordeeld, geprioriteerd en geïmplementeerd binnen passende termijnen. Indien een patch niet direct kan worden geïmplementeerd, treft de leverancier passende mitigerende maatregelen om het risico te beheersen. Op verzoek van ProRail kan de leverancier aantonen hoe kwetsbaarheden, patches en mitigerende maatregelen worden beheerd.

Security en BCM by Design | S | S.1

De leverancier heeft beleid voor veilig ontwikkelen. Bij het ontwikkelen, implementeren en beheren van software past de leverancier aantoonbaar principes toe zoals Security by Design, Security by Default en BCM by Design om de beveiliging van software en gegevens van ProRail te waarborgen.

Hierbij wordt gebruikgemaakt van relevante secure development standaarden en richtlijnen, zoals bijvoorbeeld de OWASP Application Security Verification Standard (ASVS).

Digitale toegangsbeveiliging | T | T.2

De leverancier dient ProRail in staat te stellen toegangsrechten in te richten volgens het 'least privilege'-principe. De oplossing ondersteunt ten minste rolgebaseerde autorisaties, waarbij toegangsrechten centraal kunnen worden beheerd, toegewezen en ingetrokken. ProRail moet gebruikersrechten kunnen documenteren, beheren, periodiek kunnen beoordelen en waar nodig kunnen aanpassen, zodat gebruikers uitsluitend toegang hebben tot functies en gegevens die noodzakelijk zijn voor de uitvoering van hun werkzaamheden.

Digitale toegangsbeveiliging | T | T.5

Toegang tot systemen, applicaties en omgevingen die binnen scope van de dienstverlening vallen en waarvoor gebruikers van ProRail authenticeren, dient te worden beveiligd met unieke gebruikersaccounts, sterke authenticatiemechanismen en Multi-Factor Authenticatie (MFA), conform actuele en algemeen geaccepteerde marktstandaarden en beveiligingsrichtlijnen, zoals bijvoorbeeld de relevante richtlijnen van het NCSC, NIST en CIS Controls.

Fysieke toegangsbeveiliging | U | U.1

De leverancier heeft fysieke beveiligingsmaatregelen ingericht voor ruimten en omgevingen waarin ProRail-data en/of IT-bedrijfsmiddelen worden verwerkt of opgeslagen. Deze maatregelen zijn passend bij het risico en zijn gericht op het voorkomen van onbevoegde fysieke toegang, schade of verstoring.

Organisatiewijzigingen | V | V.1

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.