Informatiebeveiligingseisen aan NEN Connect v0.91

ProRail heeft cluster overstijgend behoefte aan toegang tot NEN-, EN- en ISO-normen (en afgeleiden daarvan, zoals IEC). Voor het raadplegen van deze normen maakt ProRail gebruik van het online platform NEN Connect, waarmee medewerkers digitaal inzage hebben in de actuele en historische versies van relevante normdocumenten.

De leverancier stelt aan ProRail een "platform" (lees: database) beschikbaar waar medewerkers van ProRail desgewenst de normen, kwaliteitsstandaarden en afgeleiden daarvan kunnen raadplegen.

D. Certificeringen en normenkaders	De leverancier garandeert dat hij voldoet aan alle toepasselijke verplichtingen voortvloeiend uit de komende Cyberbeveiligingswet, inclusief maar niet beperkt tot: 1. Het treffen van passende technische en organisatorische maatregelen ter beheersing van cyberbeveiligingsrisico's; 2. Het melden van betekenisvolle cyberincidenten aan de relevante toezichthoudende autoriteiten en aan de opdrachtgever binnen 24 uur na ontdekking; 3. Het uitvoeren van regelmatige risicoanalyses en het bijwerken van beveiligingsmaatregelen; 4. Het waarborgen van de beveiliging van persoonsgegevens en bedrijfsinformatie van de opdrachtgever; 5. Het faciliteren van audits en inspecties door of namens de opdrachtgever om naleving van deze clausule te verifiëren. Indien de leverancier nalaat te voldoen aan deze verplichtingen, behoudt de opdrachtgever zich het recht voor om het contract per direct te ontbinden en/of schadevergoeding te eisen
H. Gegevensuitwisseling	Digitale gegevensuitwisselingen vinden plaats conform een gestandaardiseerde en beveiligde manier.
K. Incidenten	Bij constatering van een kwetsbaarheid, beveiligingsincident of datalek dient de leverancier onverwijld contact op te nemen met de Centrale Servicedesk van ProRail, bereikbaar op nummer 0882312600, en de betreffende contractmanager.
M. Onderaanneming en toeleveranciers	Alle voorwaarden en eisen van ProRail op het gebied van informatiebeveiliging die gelden voor de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor ProRail.
Q. Auditrecht	ProRail kan op enig moment een audit, waaronder een penetratietest, (laten) uitvoeren om te controleren dat aan beveiligingseisen die van toepassing zijn wordt voldaan. Dit gebeurt in overleg met de leverancier. Een audit hoeft niet nodig te zijn 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. ProRail behoudt zich echter te allen tijde het recht voor om alsnog zelf een audit uit te voeren, indien daartoe aanleiding is.
R. Risicomanagement	De leverancier dient ProRail (op verzoek) te informeren over de getroffen beheersmaatregelen die relevant zijn binnen het kader van de dienstverlening.
U. Toegang tot digitale infrastructuur en gegevens	De leverancier ondersteunt toegang tot de dienst via Single Sign-On (SSO), gekoppeld aan het centrale identiteits- en toegangsbeheersysteem van ProRail.
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.