Bijlage 4b
Informatiebeveiligingseisen

Offerteaanvraag ten behoeve van de Europese openbare aanbesteding
“Geodetische meetapparatuur”

Ten behoeve van het Kadaster

Directie	**Personeel en Organisatie (P&O)**
2Agree-kenmerk:	A25-104115
Opdrachtgever	Directie Operatie, Dienstverlening en Registratie (ODR).
Versie	Definitief
Versiedatum	25-02-2026

1 Inleiding

In deze bijlage zijn de informatiebeveiligingseisen opgenomen die het Kadaster stelt aan de gevraagde leveringen en bijbehorende dienstverlening. Aan deze eisen moet bij uitvoering van de overeenkomst, indien van toepassing, worden voldaan.

2 Informatiebeveiligingseisen

Eis	Omschrijving	Categorie
Eis 1.	Datadragers met data van het Kadaster worden na beëindiging van gebruik of bij een defect aantoonbaar, middels een bewijs van een derde partij of eigen vernietigingsprocedure, ontoegankelijk gemaakt. De leverancier is verantwoordelijk voor het voorkomen van datalekken of ongeautoriseerde toegang tot de datadragers.	Data
Eis 2.	De MSS, CERT-Retainer en SOC van het Kadaster kunnen te allen tijde toegang krijgen tot relevante (security) configuraties en audit logs van alle in de Kadaster CMDB opgenomen CI's t.b.v. triage, analyse, forensisch onderzoek en/of threat hunting.	Detectie
Eis 3.	Alle vormen van logs dienen minimaal 6 maanden te worden bewaard om forensisch onderzoek mogelijk te maken in het geval (security)incidenten.	Detectie
Eis 4.	Inhoud en bescherming van logs voldoet aan de eisen van de BIO	Detectie
Eis 5.	De leverancier heeft aantoonbaar maatregelen genomen tegen cyberrisico's op basis van een risico-inschatting die gedeeld is met het Kadaster.	Detectie
Eis 6.	Het Kadaster heeft het recht om securitytesten (zoals pentesten, red-teaming, ethical hacking) uit te (laten) voeren op de door de leverancier geleverde diensten. Een leverancier kan ervoor kiezen om securitytesten zelf uit te laten voeren indien deze voldoet aan de door het Kadaster gestelde scope, reikwijdte, frequentie en kwaliteit. Alle daaruit voortvloeiende relevante bevindingen en benodigde maatregelen worden gerapporteerd aan het Kadaster met, indien van toepassing, een plan van aanpak voor de implementatie.	Detectie
Eis 7.	De leverancier voert wijzigingen gecontroleerd en beheerst door, zonder daarbij afbreuk te doen aan de continuïteit van de geboden dienstverlening. Hiervoor maakt de leverancier gebruik van een representatieve test- en/of acceptatie-omgeving.	Continuïteit
Eis 8.	Kritische kwetsbaarheden (met CVSS-score 9.0 en hoger) worden zo snel mogelijk gemitigeerd, securitypatches hiervoor worden binnen een week geïnstalleerd. Dit gebeurt op basis van een risicoanalyse. In het geval van in-house ontwikkeling moet de leverancier zo spoedig mogelijk, binnen één dag, belangrijke patches kunnen aanleveren. Voor overige termijnen verwijzen we naar de standaard Patchmanagement.	Continuïteit

Eis 9.	De leverancier heeft zelf gedragsregels voor acceptabel gebruik van eigen bedrijfsmiddelen en alle medewerkers worden hier minimaal jaarlijks aantoonbaar op gewezen.	Personeel
Eis 10.	De leverancier stelt zijn medewerkers minimaal jaarlijks op de hoogte van de procedure waarop zij beveiligingsincidenten en datalekken moeten aanmelden.	Personeel
Eis 11.	Binnen de organisatie van de leverancier zijn de verantwoordelijkheden, taken en bevoegdheden voor het risicobeheer, Informatiebeveiliging en compliance vastgesteld en belegd.	Personeel
Eis 12.	Medewerkers van de leverancier hebben enkel toegang tot Kadaster data op need-to-know basis. De lijst met medewerkers van de leverancier met toegang tot Kadaster data wordt minimaal ieder kwartaal aantoonbaar beoordeeld door de leverancier en de leverancier koppelt de resultaten terug aan het Kadaster. De leverancier zorgt ervoor dat de medewerkers die toegang hebben tot Kadaster data voldoende zijn getraind en geïnstrueerd over de geldende regels en procedures.	Personeel
Eis 13.	De gangbare principes rondom Security-by-design (zoals vastgelegd in 'Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software' van het NCSC op https://www.ncsc.nl) zijn uitgangspunt voor de ontwikkeling van software en systemen	Ontwikkeling
Eis 14.	Voor acceptatietesten van software worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Ontwikkeling
Eis 15.	Ten behoeve van de afgenomen dienstverlening dient de leverancier gebruik te maken van een gescheiden ontwikkel-, test-, acceptatie- en/of productieomgeving. Deze omgevingen zijn strikt gescheiden.	Ontwikkeling
Eis 16.	Bij het ontwikkelen en testen wordt bij voorkeur gebruik gemaakt van synthetische gegevens. Gebruik van data van het Kadaster voor ontwikkel/testen is enkel toegestaan na expliciete toestemming.	Ontwikkeling
Eis 17.	De leverancier heeft aantoonbaar effectieve patch- & lifecycle- managementprocessen t.a.v. alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan het kadaster. Waarbij alle onderdelen onder actieve contractuele (security) support vallen van de leveranciers en zo binnen gestelde SLA tijden van de security patches worden voorzien.	Ontwikkeling
Eis 18.	De volgende eisen zijn van toepassing voor zover Kadaster gebruikers op IT-componenten kunnen inloggen die onderdeel zijn van de geleverde dienst, of voor zover deze IT-componenten toegang geven tot Kadaster data en/of functionaliteit. Van deze eisen mag enkel worden afgeweken na een risicoafweging door Kadaster conform de procedure Uitzondering op beleid. (a) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden	Digitale toegang

aangesloten op de Kadastervoorziening(en) voor authenticatie, gebaseerd op open standaarden (lijsten ‘verplicht’ en ‘aanbevolen’ van Forum voor Standaardisatie).

(b) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden aangesloten op de Kadastervoorziening voor autorisatiebeheer, gebaseerd op open standaarden (lijsten ‘verplicht’ en ‘aanbevolen’ van Forum voor Standaardisatie). De wijze van aansluiten dient zodanig te worden vormgegeven dat het toekennen, wijzigen of intrekken van toegangsrechten automatisch plaatsvindt.

(c) De leverancier maakt het mogelijk dat de geleverde IT-componenten worden aangesloten op de Kadastervoorziening voor beveiligen van kritieke toegang, gebaseerd op open standaarden (lijsten ‘verplicht’ en ‘aanbevolen’ van Forum voor Standaardisatie). De wijze van aansluiten dient zodanig te worden vormgegeven dat de inloggegevens door de Kadaster voorziening automatisch kunnen worden gewijzigd.

Eis 19.	Voor zover medewerkers van de leverancier toegang nodig hebben tot IT-componenten van Kadaster die de leverancier zelf niet levert, worden de autorisaties beheerd middels het leverancierssportaal dat onderdeel is van de Kadastervoorziening voor autorisatiebeheer. Van deze eisen mag enkel worden afgeweken na een risicoafweging door Kadaster conform de procedure Uitzondering op beleid.	Digitale toegang
Eis 20.	Devices die data willen versturen naar of uitwisselen met Kadaster-werkplekken moeten zich voorafgaand aan de sessie identificeren en authenticeren.	Digitale toegang
Eis 21.	Authenticatie van devices gebeurt op basis van robuuste authenticatie-methoden, die passen bij het vastgestelde beveiligingsniveau van de dienst en die algemeen geaccepteerd zijn als best practice in het werkveld.	Digitale toegang
Eis 22.	Devices die onderdeel willen worden van een door het Kadaster opgezet (wireless) netwerk, waaronder (maar niet beperkt tot) een piconet, moeten zich identificeren en authenticeren.	Digitale toegang
Eis 23.	Niet openbare gegevens inclusief persoonsgegevens worden zo veel mogelijk versleuteld in transport en bij opslag. Versleuteling in transport en opslag voldoet aan de hedendaagse geaccepteerde standaarden voor versleuteling in opslag (waaronder minimaal de richtlijnen van NCSC).	Cryptografie
Eis 24.	Communicatie vindt plaats via protocollen zonder bekende vulnerabilities. Protocollen die worden afgeraden vanuit best practices worden niet gebruikt voor versleuteling.	Cryptografie
Eis 25.	API’s die de oplossing bieden om het systeem te integreren met Kadaster systemen gebruiken protocollen die zijn aanbevolen door Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen).	Standaarden
Eis 26.	De oplossing voldoet aan de verplichte standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/verplicht).	Standaarden

Eis 27.	De leverancier versleutelt bij communicatie met het Kadaster alle berichten en bestandsuitwisselingsmogelijkheden.	Standaarden
Eis 28.	Indien cookies nodig zijn, dienen deze versleuteld te worden.	Standaarden
Eis 29.	Gegevensuitwisseling wordt gedaan via gangbare protocollen, die zijn beschreven in openbare standaarden	Standaarden
Eis 30.	Beveiligingsincidenten en datalekken die impact hebben op de aan het Kadaster aangeboden dienstverlening en/of data worden zo snel mogelijk (maar uiterlijk binnen 24 uur) gemeld door de leverancier aan het Kadaster. Het meldpunt is de ServiceDesk. Telefoon: +31 (0)88- 183 21 00, KSD@kadaster.nl.	Rapportage
Eis 31.	Om de effectiviteit van de maatregelen, compliance aan het beleid en voldoen aan wet- en regelgeving te kunnen waarborgen, heeft het Kadaster de mogelijkheid om dit te verifiëren middels een formele audit. De leverancier kan dit ook zelf aantonen middels een onafhankelijke audit door een gecertificeerd auditor met inachtneming van de juiste scope en reikwijdte. Het niet voldoen aan de mogelijkheid om een audit te laten uitvoeren dan wel het niet opleveren van de juiste assurance verklaringen kan leiden tot het voortijdig beëindigen van de overeenkomst.	Rapportage
Eis 32.	Het algemene niveau van de informatiebeveiliging blijkt uit één van het volgende: (a) Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISO27001 inclusief Verklaring van Toepasselijkheid, ISAE3000 (ookwel SOC T2)); (b) Een Assurance rapport van een auditor die is aangesloten bij NOREA én in het bezit is van de RE certificering; De eventuele kosten voor het aantonen van de toereikendheid en/of het opvolgen van eventuele adviezen zijn voor de leverancier. De adviezen dienen te worden uitgewerkt in een plan van aanpak en te worden overlegd met het Kadaster. Na akkoord van het Kadaster, voor het uitvoeren van het plan van aanpak, dienen de maatregelen binnen 2 maanden geïmplementeerd te zijn tenzij anders overeengekomen. Indien de leverancier niet kan of niet wenst te voldoen aan de aanbevelingen en adviezen in het auditrapport, heeft het Kadaster de mogelijkheid tot opzeggen van de te sluiten overeenkomst	Rapportage
Eis 33.	De leverancier heeft een vastgestelde procedure voor beveiligingsincidenten (CVD) en datalekken, waarin de taken en verantwoordelijkheden staan beschreven. De beschreven taken en bevoegdheden zijn belegd in de organisatie.	Rapportage
Eis 34.	De leverancier is verantwoordelijk voor de beveiliging van de eigen organisatie en dienstverlening conform de door het Kadaster te stellen eisen, aangevuld met het volgen van branche-richtlijnen en standaarden.	Rapportage
Eis 35.	De leverancier is verantwoordelijk voor het leveren van veilige diensten aan het Kadaster, en regelt daartoe een adequaat systeem in (processen, medewerkers, tooling, monitoring) voor de eigen dienstverlening	Rapportage

Eis 36.	De leverancier rapporteert minimaal elk kwartaal schriftelijk over informatiebeveiligingsrisico's (inclusief kans en impact, genomen beheersmaatregelen en eventuele restrisico's) aan het Kadaster.	Rapportage
Eis 37.	De leverancier voert jaarlijkse een BIO self-assessment uit, waarbij hij aantoont dat de informatiebeveiliging voldoet aan het gestelde normenkader. In het kader van het Pas toe of Leg uit principe dient de leverancier afwijking van het genoemde normenkader toe te lichten	Rapportage