

Bijlage 14: Eisen met betrekking tot informatiebeveiliging

Let op: Indien Inschrijver zelf niet over de informatiebeveiligingseisen beschikt conform de door het Kadaster gestelde eisen, maar de hostende/beherende partij wel aan de Kadaster informatiebeveiligingseisen voldoet dan is dat ook goed.

1. Er is een informatiebeveiligingsbeleid opgesteld door Opdrachtnemer. Dit beleid is vastgesteld door de leiding van Opdrachtnemer en bevat de volgende onderdelen:
 - (a) De internationaal geaccepteerde norm (minimaal ISO 27001 of vergelijkbaar) die wordt gebruikt voor informatiebeveiliging
 - (b) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd (minimaal jaarlijks).
 - (c) Activiteiten ter bevordering van het informatiebeveiligingsbewustzijn bij de medewerkers (minimaal jaarlijks).
2. Binnen de organisatie van de Opdrachtnemer zijn de verantwoordelijkheden, taken en bevoegdheden voor het risicobeheer, Informatiebeveiliging en compliance vastgesteld en belegd.
3. Medewerkers van Opdrachtnemer die toegang hebben tot data van het Kadaster zijn gescreend voor hun functie (VOG met minimaal functieaspecten 11, 12, 13 of minimaal gelijkwaardig).
4. Opdrachtnemer heeft zelf gedragsregels voor acceptabel gebruik van eigen bedrijfsmiddelen en alle medewerkers worden hier minimaal jaarlijks op gewezen.
5. Data van het Kadaster wordt na beëindiging van gebruik of een defect aantoonbaar middels een bewijs van een derde partij of eigen vernietigingsprocedure ontoegankelijk gemaakt.
6. Opdrachtnemer ondersteunt inloggen middels multi factor authenticatie (MFA) en voldoet minimaal aan het wachtwoordbeleid van het Kadaster:
 - (a) Lengte: Minimaal 12 karakters
 - (b) Wachtwoordhistorie: Wachtwoorden worden niet hergebruikt
 - (c) Complexiteitseis: Minimaal kleine letters, hoofdletters en cijfers
 - (d) Wachtwoordleeftijd: Maximaal 1 jaar
 - (e) Maximale sessieduur: 10 uur
 - (f) Vergrendeling bij inactiviteit: Na 30 minuten.
7. Opdrachtnemer biedt API's (minimaal SAML 2.0, OpenID Connect of OAuth 2.0) t.b.v. het aansluiten op het identity managementsysteem (IDM) van het Kadaster of ondersteunt inloggen middels multi factor authenticatie (MFA).
8. Medewerkers van Opdrachtnemer hebben enkel toegang tot Kadaster data op need-to-know basis. De lijst met medewerkers van Opdrachtnemer met toegang tot Kadaster data wordt minimaal ieder kwartaal aantoonbaar beoordeeld door Opdrachtnemer en Opdrachtnemer koppelt de resultaten terug aan het Kadaster.
9. Klantenomgevingen van Opdrachtnemer zijn logisch gescheiden en kunnen elkaar onderling niet beïnvloeden als gevolg van verstoringen in de klantomgeving.
10. Opdrachtnemer maakt gebruik van versleutelde verbindingen (bijvoorbeeld door middel van HTTPS, IPSEC VPN, SFTP) en voldoet aan de meest recente TLS richtlijn van het NCSC (Zie 'ICT-beveiligingsrichtlijnen voor transport layer security' op <https://www.ncsc.nl/>). Kadaster medewerkers hebben toegang tot de service op basis van een beveiligde verbinding (bijvoorbeeld HTTPS).
11. Niet openbare gegevens inclusief persoonsgegevens worden altijd versleuteld in transport en bij opslag. Versleuteling voor transport is in lijn met de meest recente TLS richtlijn van het NCSC (Zie 'ICT-beveiligingsrichtlijnen voor transport layer security' op <https://www.ncsc.nl/>). Versleuteling in opslag voldoet aan de hedendaagse geaccepteerde standaarden voor versleuteling in opslag.
12. Indien cookies nodig zijn, dienen deze versleuteld te worden.
13. Opdrachtnemer heeft de toegang en toegangsbeveiliging tot beveiligde zones ingericht om gebieden te beschermen die vertrouwelijke of geheime informatie en informatie verwerkende faciliteiten bevatten. Het aantal beveiligde passages of openingen naar een beveiligde zone wordt beperkt. De toegangen tot de verschillende zones zijn zelfsluitend en de zones zijn van elkaar gescheiden.
14. Opdrachtnemer voert wijzigingen gecontroleerd en beheerst door, zonder daarbij afbreuk te doen aan de continuïteit van de geboden dienstverlening.
15. Opdrachtnemer heeft maatregelen tegen malware geïmplementeerd: systemen en media worden als voorzorgsmaatregel routinematig gescand. Bij scanning wordt onderscheid gemaakt tussen scans bij toegang en routinematige scans:

- (a) Bij toegang worden bestanden vooraf gescand, waaronder alle bestanden die een netwerk of opslagmedium zijn ontvangen.
 - (b) Bij het downloaden en openen van bijlagen worden de bestanden gescand, voordat deze definitief opgeslagen en daadwerkelijk geopend kunnen worden.
 - (c) Bestanden worden routinematig gescand, minimaal 1x per week om reeds opgeslagen data alsnog te scannen op nieuwe detectiemogelijkheden. Bijvoorbeeld door aangepaste patroonherkenning van het betreffende antimalware pakket of een verbeterde engine van de antimalware software.
16. Opdrachtnemer heeft een back-up beleid vastgesteld en geïmplementeerd waarin de eisen voor het bewaren en beschermen zijn gedefinieerd. In het back-up beleid wordt minimaal met de volgende eisen rekening gehouden:
- (a) Dataverlies en hersteltijd(en) van een backup in geval van incidenten is afhankelijk van het type dienst en zullen tot een minimum in tijd worden beperkt die nodig is om de bedrijfsvoering weer te continueren.
 - (c) De backups zijn beschermd tegen ransomware aanvallen (zoals bijvoorbeeld een offline backup).
17. Belangrijke patches (bij kwetsbaarheden met CVSS-score 9 en hoger) worden zo snel mogelijk, maar uiterlijk binnen een week, geïnstalleerd. Bij softwareontwikkeling moet Opdrachtnemer zo spoedig mogelijk en binnen 1 dag belangrijke patches kunnen aanleveren.
18. Het in- en uitgaande dataverkeer van Opdrachtnemer wordt bewaakt en geanalyseerd op kwaadaardige elementen (zoals malware).
19. Het bewaken en analyseren van het in- en uitgaande dataverkeer van Opdrachtnemer wordt gemonitord door een SIEM en/ of SOC middels detectie-voorzieningen.
20. Bij elektronische (e-mail)berichten worden de vastgestelde open standaarden tegen phishing en af luisteren op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie toegepast (zie link: <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>).
21. Opdrachtnemer versleutelt bij communicatie met het Kadaster alle berichten en bestandsuitwisselingsmogelijkheden.
22. 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.
23. Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.
24. Opdrachtnemer heeft een vastgestelde procedure voor beveiligingsincidenten en datalekken, waarin de taken en verantwoordelijkheden staan beschreven. De beschreven taken en bevoegdheden zijn belegd in de organisatie.
25. Opdrachtnemer stelt zijn medewerkers minimaal jaarlijks op de hoogte van de procedure waarop zij beveiligingsincidenten en datalekken moeten melden.
26. Beveiligingsincidenten en datalekken die impact hebben op de aan het Kadaster aangeboden dienstverlening worden binnen 24 uur gemeld door Opdrachtnemer aan het Kadaster. Het meldpunt is de ServiceDesk. Telefoon: +31 (0)88- 183 21 00, KSD@kadaster.nl
27. Opdrachtnemer heeft continuïteitsplannen voor systemen die de dienstverlening aan het Kadaster betreffen, die jaarlijks worden getest op geldigheid en bruikbaarheid. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
- a) Identificatie van essentiële procedures voor bedrijfscontinuïteit.
 - b) Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd teruggaan wordt.
 - c) Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
 - d) Prioriteiten en volgorde van herstel en reconstructie.
 - e) Documentatie van systemen en processen.
 - f) Kennis en kundigheid van personeel om de processen weer op te starten.
28. Opdrachtnemer rapporteert minimaal jaarlijks schriftelijk over informatiebeveiliging risico's (inclusief kans en impact en genomen beheersmaatregelen) aan het Kadaster.
29. Significante gebeurtenissen die de dienstverlening aan het Kadaster bedreigen worden geïdentificeerd, geregistreerd en geëvalueerd.
30. De locatie van de verwerking van data (daaronder begrepen maar niet beperkt tot: data in rust, productie, back-ups, etc) vindt plaats binnen de Europese Economische Ruimte waar minimaal Europees recht van toepassing is. Voor zover (sub)verwerking plaatsvindt buiten de EER is dat alleen toegestaan op grond van door een bevoegde toezichthoudende autoriteit goedgekeurde bindende bedrijfsvoorschriften zoals is bedoeld en voor zover die voldoen aan alle eisen zoals genoemd in artikel 47 Algemene Verordening Gegevensbescherming.
31. De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- * Periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3402 T2 of SOC T2);
- * Een Assurance rapport van een auditor die is aangesloten bij NOREA;
- * Een door de Opdrachtnemer ingevulde self assessment van de Baseline Informatiebeveiliging Overheid, waarbij hij aantoont dat de informatiebeveiliging voldoet aan het gestelde normenkader. In het kader van het Pas toe of Leg uit principe dient de Opdrachtnemer afwijking van het genoemde normenkader toe te lichten.
- * Eigen controles of eigen mededelingen over de BIO/ ISO27001 beveiligingsmaatregelen vastgelegd in een formeel vastgesteld document.

De eventuele kosten voor het aantonen van de toereikendheid en/of het opvolgen van eventuele adviezen zijn voor Opdrachtnemer. 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 Opdrachtnemer 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.

32. Het Kadaster blijft te allen tijde eigenaar van haar data.
33. Kadaster kan een externe audit, waaronder een penetratietest, laten uitvoeren om te controleren of aan beveiligingseisen die van toepassing zijn wordt voldaan. De kosten voor het eerste externe onderzoek zijn voor Opdrachtnemer. Een audit is niet nodig als Opdrachtnemer 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 het Kadaster. Indien Opdrachtnemer niet kan of niet wenst te voldoen aan de beveiligingseisen die van toepassing zijn, heeft het Kadaster de mogelijkheid tot opzeggen van de te sluiten overeenkomst.
34. Opdrachtnemer draagt, na beëindiging van de te sluiten Overeenkomst, de data van het Kadaster in een algemeen geaccepteerd bestandsformaat over en vernietigt de data van haar eigen systemen.
35. De oplossing biedt beveiligde API's om het systeem te integreren met Kadaster systemen (ondersteunende protocollen zijn SOAP, sFTP en REST, met voorkeur voor REST met OAuth).
36. De oplossing voldoet aan de verplichte standaarden van het Forum Standaardisatie (<https://www.forumstandaardisatie.nl/open-standaarden/verplicht>).
37. De locatie van de verwerking van data (daaronder begrepen maar niet beperkt tot: data in rust, productie, back-ups, etc.) vindt plaats binnen de Europese Economische Ruimte waar minimaal Europees recht van toepassing is. Voor zover (sub)verwerking plaatsvindt buiten de EER is dat alleen toegestaan op grond van door een bevoegde toezichthoudende autoriteit goedgekeurde bindende bedrijfsvoorschriften zoals is bedoeld en voor zover die voldoen aan alle eisen zoals genoemd in artikel 47 Algemene Verordening Gegevensbescherming.