

Bijlage 16 – Security vereisten

Betreft Aanbesteding

Zaak- en VTH-applicatie

Door in te schrijven bevestigt u als Inschrijver dat uw oplossing voldoet aan onderstaande security vereisten. Na definitieve gunning zal de winnende inschrijving een toelichting worden gevraagd op het ondersteunen van deze vereisten.

Volgnr.	Beschrijving
0. Algemeen	
0.1	De Leverancier conformeert zich aan GIBIT 2023.
0.2	De Leverancier is ISO27001:2022 (of gelijkwaardig) gecertificeerd of is bereid zich binnen een jaar te certificeren. Het certificaat en de VvT (Verklaring van toepasselijkheid) behorend bij de certificering is voor de Opdrachtgever inzichtelijk en wordt na voorlopige gunning aan de Opdrachtgever toegestuurd. De jaarlijkse TPM waaruit blijkt dat de leverancier voldoet aan de norm wordt bij inschrijving kosteloos verstrekt en vervolgens jaarlijks kosteloos aan de Opdrachtgever toegestuurd.
0.3	In het geval dat de Leverancier (nog) geen ISO27001-certificaat of gelijkwaardig kan overleggen levert de directie van de Leverancier jaarlijks een In Control Verklaring (ICV) op over de status van haar informatiebeveiliging en de beveiligingsmaatregelen waar de ICV betrekking op heeft. Deze verklaring moet bij de inschrijving worden aangeleverd.
0.4	De RTO (Recovery Time Objective – herstel van de beschikbaarheid van de Toepassing) bedraagt 24 uur in het geval van een calamiteit bij de leverancier. De RPO (Recovery Point Objective – maximaal dataverlies) voor de Opdrachtgever in het geval van een calamiteit bij de leverancier bedraagt 24 uur.
6. Beveiligingsorganisatie	
6.1	De Leverancier heeft een beveiligingsfunctie benoemd en een beveiligingsorganisatie ingericht waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
6.2	De Leverancier heeft een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
7. Personeel	
7.1	De Leverancier instrueert haar medewerkers door middel van een doorlopend programma over het belang van een goede informatiebeveiliging en naleving van de privacywetgeving.
7.2	Op verzoek van Opdrachtgever toont Leverancier aan dat haar medewerkers trainingen succesvol hebben gevolgd.
8. Beheer bedrijfsmiddelen	
8.1	De Leverancier behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.
9. Toegangsbeveiliging	
9.1	Het softwarepakket behoort een autorisatiemechanisme te bieden.
9.2	De Toepassing ondersteunt Single Sign On (SSO) c.q. biedt een federatief koppelvlak aan voor uitwisseling van rollen en rechten (Azure AD van Microsoft).
9.3	Als extra beveiligingslaag is de toegang tot de Toepassing beveiligd met meer-factor authenticatie (MFA).
9.4	Als MFA niet geboden wordt gelden de volgende eisen (sub .1 en .2) voor de Toepassing:

Volgnr.	Beschrijving
9.4.1	De wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.
9.4.2	Het wachtwoord wordt minimaal halfjaarlijks het wachtwoord vernieuwd.
9.5	De Toepassing dwingt eisen aan wachtwoorden geautomatiseerd af.
9.6	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
9.7	De Toepassing en data zijn (logisch) geïsoleerd van andere klanten van de Leverancier. De gegevens en gegevensverwerkingen mogen niet toegankelijk of zichtbaar zijn voor onbevoegde derden, waaronder andere klanten van de Leverancier.
9.8	De rechten die gebruikers hebben binnen de Toepassing (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.
10. Cryptografie	
10.1	Leverancier heeft beleid ontwikkeld en geïmplementeerd ten aanzien van het beheer van cryptografie en cryptografische sleutels.
10.2	Certificaat- en sleutelbeheer is ingericht.
10.3	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.
10.4	De Opdrachtgever dient gebruik te kunnen maken van certificaten op naam van een door de Opdrachtgever vertrouwde Certificaatautoriteit.
10.5	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.
10.6	De beveiliging van de netwerkverbinding(en) met de applicatie voldoet aan de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security.
10.7	Bij multi-tenancy wordt de klantdata binnen clouddiensten, die door meerdere klanten worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.
11. Beveiliging omgeving en werkplek	
11.1	Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.
12. Bedrijfsvoering	
12.1	Al het dataverkeer, alle data, en de besturingssystemen worden gescand op aanwezigheid of dreiging van tenminste virussen, malware, spyware en ransomware. De daarvoor gebruikte middelen en software voldoen te allen tijde aan de meest actuele stand van de techniek. Alle gevaren die de prestatie (kunnen) raken worden onverwijld geëlimineerd of geneutraliseerd.
12.2	De gebruikte anti-malware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
12.3	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: a. Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. b. Bijlagen en downloads vóór gebruik.
12.4	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.
12.5	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

Volgnr.	Beschrijving
12.6	De (audit-)logbestanden moeten te allen tijde door de Opdrachtgever kunnen worden geraadpleegd voor nadere analyse.
12.7	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.
12.8	In audit-logbestanden wordt tenminste vastgelegd: de gebeurtenis; de benodigde informatie die nodig is om een beveiligingsincident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
12.9	De hardware en software die de Leverancier gebruikt moet afkomstig zijn van betrouwbare leveranciers.
12.10	Alle hardware is gehardened en de configuraties worden tenminste jaarlijks herzien.
12.11	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen (DMZ, firewalls, IDS, IPS) en de rule sets worden actueel gehouden.
12.12	Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de laatste (beveiligings-)patches kunnen worden geïnstalleerd.
12.13	Vulnerability management is procesmatig ingericht. Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort procesmatig en tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.
12.14	De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.
12.15	<p>Inschrijver beschikt over een sluitend en betrouwbaar back-up en restoreproces. Hierbij zijn minimaal de volgende eisen van toepassing:</p> <ul style="list-style-type: none"> • De back-up en restore procedures zijn ingericht en worden tenminste jaarlijks getest; • Er wordt dagelijks een incrementele back-up gemaakt; • Wekelijks en maandelijks wordt een full back-up gemaakt. • De week- en maandback-ups worden op een externe offline locatie bewaard. • De maandback-up wordt zes maanden bewaard; • De weekback-ups worden 1 maand bewaard. • De procedures voor back-up en recovery worden tenminste jaarlijks getest door middel van een restore. Over het resultaat wordt aan Leverancier gerapporteerd. • Na de bewaartermijn moet de back-up vernietigd worden.
12.16	De Opdrachtgever kan beschikken over een acceptatietestomgeving.
13. Communicatiebeveiliging	
13.1	Als vanuit de Toepassing e-mails worden verstuurd: E-mailverkeer dat namens OD NHN (@odnhn.nl) plaatsvindt (intern dan wel extern) voldoet blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en DANE.
13.2	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.
13.3	De Leverancier heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.

Volgnr.	Beschrijving
13.4	De Toepassing biedt volledig werkende ondersteuning voor de Open Standaarden IPv4 én IPv6 ('dual stack') -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent in ieder geval dat: <ol style="list-style-type: none"> 1. Gebruikers en andere ICT-systemen het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen. 2. Configuratiefunctionaliteit voor IP-adressen (bijv. een IP-whitelist) in het ICT-systeem zowel voor IPv4 als IPv6 beschikbaar is.
13.5	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.
13.6	Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.
13.7	De Toepassing gebruikt veilige API's voor import en export van gegevens.
13.8	De Toepassing moet mechanismen bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.
14. Ontwikkeling en onderhoud	
14.1	De Leverancier hanteert gangbare principes rondom Security by design als uitgangspunt voor de ontwikkeling van software en systemen.
14.2	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheer framework zoals BiSL en ITIL.
14.3	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: <ul style="list-style-type: none"> - het administreren van wijzigingen; - risicoafweging van mogelijke gevolgen van de wijzigingen; - goedkeuringsprocedure voor wijzigingen.
14.4	Er zijn maatregelen genomen dat alleen bevoegd personeel van de Leverancier toegang heeft tot het netwerk, de applicaties en data. Functiescheiding is doorgevoerd in de autorisatiestructuur. Hieronder wordt ook toegang tot de source code verstaan.
14.5	De drie componenten hardware, software, appliances die betrokken zijn bij de applicatie zijn aantoonbaar getest op kwetsbaarheden met gangbare testmethodieken voordat deze in productie worden genomen.
14.6	De componenten betrokken bij de applicatie mogen niet in productie worden genomen voordat alle bevindingen uit de acceptatietest zijn verholpen, tenzij nadrukkelijk anders overeengekomen.
14.7	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.
14.8	Van de testresultaten wordt verslag gemaakt.
14.9	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.
14.10	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.
15. Leveranciersrelaties	
15.1	Met de Leverancier wordt een verwerkersovereenkomst gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
15.2	De Leverancier moet haar keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde beveiligingseisen ook door te vertalen naar hun toeleveranciers.
15.3	Met de Leverancier behoren de informatiebeveiligingseisen en een periodieke actualisering daarvan contractueel te worden overeengekomen en periodiek te worden geëvalueerd.

Volgnr.	Beschrijving
15.4	In de overeenkomst met de Leverancier moet een exit-strategie te zijn opgenomen waarbij zowel een aantal bepalingen over exit zijn opgenomen, als condities die aanleiding kunnen geven tot een exit.
16. Beveiligingsincidenten	
16.1	De Leverancier heeft een meldloket waar beveiligingsincidenten kunnen worden gemeld.
16.2	De Leverancier heeft een meldprocedure geïmplementeerd waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
16.3	De Leverancier documenteert de opvolging van bevindingen en behandelt deze als beveiligingsincident.
16.4	Incidenten die de Opdrachtgever raken worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld. Tijdens de inrichting van de overeenkomst wordt in het DAP een incidentmanagementprocedure uitgewerkt, waarin in ieder geval, maar niet uitsluitend, aandacht is voor het rapporteren over beveiligingsincidenten die de Opdrachtgever raken.
16.5	De Leverancier werkt bij ernstige beveiligingsincidenten die de Opdrachtgever raken volledig mee aan forensisch onderzoek, zorgt ervoor dat alle noodzakelijke onderzoeksgegevens gereed zijn voor het snel en succesvol kunnen starten met een forensisch onderzoek en stelt bewijzen veilig.
16.6	De Leverancier informeert de CISO van de Opdrachtgever tijdig over kritische CVE's en rapporteert in de Service Level Rapportage over gepatchte CVE's.
17. Continuïteit	
17.1	De beschikbaarheid van de Toepassing is 24/7 gegarandeerd op 99,5% gemeten op jaarbasis, exclusief geplande downtijd voor bijvoorbeeld onderhoud.
17.2	De Leverancier herstelt bij uitval van de Toepassing de dienstverlening van uiterlijk binnen twee werkdagen.
17.3	De Leverancier heeft haar BCM-proces adequaat georganiseerd waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
17.4	De Leverancier test jaarlijks de continuïteitsplannen op geldigheid en bruikbaarheid.
18. Naleving	
18.1	De Leverancier laat penetratietesten uitvoeren op de web-facing componenten van haar infrastructuur en volgt de testbevindingen tijdig op. Er wordt ten minste getest op de OWASP top-10 kwetsbaarheden.
18.2	De Leverancier heeft een Information Security Management System (ISMS-proces) ingericht waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.
18.3	De Leverancier beschikt over een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.
18.4	De Toepassing wordt jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.
18.5	De Opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren. Deze audit wordt in overleg met de Leverancier ingepland.
J. Privacy	
P.1	In de Toepassing is "Privacy by design" toegepast. Dat houdt in dat je al tijdens de ontwikkeling van de applicatie rekening is gehouden met privacyaspecten. Bijvoorbeeld door gedurende het proces extra (technische) maatregelen te nemen en in te bouwen om de persoonsgegevens te beschermen

Volgnr.	Beschrijving
P.2	In de Toepassing is "Privacy by default" toegepast. Dat wil zeggen dat de applicatie met de hoogst mogelijke privacy-instellingen wordt aangeboden aan gebruikers. Een gebruiker kan dan zelf besluiten om dit aan te passen en zo eventueel meer gegevens aan te bieden.
P.3	De Leverancier heeft een DPIA op de Toepassing uitgevoerd en is bereid de resultaten te delen of mee te werken aan een eigen uit te voeren DPIA.
P.4	Leverancier conformeert zich aan de standaard verwerkersovereenkomst van de OD NHN.
P.5	De Leverancier heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
P.6	Opslag van data in de EU.