

1. “Concept” technische eisen ICT en AVG normen (versie 0.7)

Nr	Omschrijving
Hosting	
Eis.1	Het zaaksysteem moet binnen Nederland, respectievelijk Europese Economische Ruimte (EER) gehost worden op basis van een Software-as-a-Service (SaaS) oplossing. Dit geldt niet alleen voor de hosting, maar ook voor de opslag, support, verwerking van persoonsgegevens en uitwijkmogelijkheden.
Eis.2	Als de leverancier van het zaaksysteem zelf de hosting faciliteert dan dienen de beveiligde gebieden te worden beschermd, met passende maatregelen voor toegangsbeveiliging. Als de leverancier van het zaaksysteem dit niet zelf faciliteert, dient de leverancier te garanderen dat hier bij de uitbesteedde hostingspartij in is voorzien.
Beveiliging en toegang	
Eis.3	De leverancier van het zaaksysteem heeft een toegangsbeveiligingsbeleid vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.
Eis.4	De leverancier van het zaaksysteem heeft het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen vastgelegd.
Eis.5	<p>De leverancier van het zaaksysteem heeft ter bescherming van communicatie en opslag van informatie een beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd.</p> <p>Dit beleid dient minimaal de volgende onderwerpen te beschrijven:</p> <ul style="list-style-type: none"> • Wie verantwoordelijkheid is voor de implementatie en het sleutelbeheer. • Het bewaren van geheime authenticatie-informatie tijdens verwerking, transport en opslag. • De wijze waarop de normen van het Forum Standaardisatie worden toegepast.
Eis.6	De leverancier van het zaaksysteem zal de klant op de hoogte houden over nieuwe ontwikkelingen binnen de aangeboden dienst.
Eis.7	De leverancier van het zaaksysteem behoort processen, procedures tot redundantie, disaster recovery en beheersmaatregelen te documenteren, te implementeren en te handhaven.
Eis.8	<p>Het zaaksysteem is voorzien van mechanismen voor normalisatie en validatie van invoer en voor schoning van de uitvoer.</p> <p><i>Toelichting: Er komt geen code in de applicatie die er niet in hoort, b.v. tekstvelden kunnen alleen tekst bevatten, bescherming tegen onder andere SQL injections etc</i></p>
Eis.9	<p>Het zaaksysteem voorziet standaard in sessiebeheer:</p> <p><i>Toelichting: sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden:</i></p> <ul style="list-style-type: none"> • Indien ze niet langer nodig zijn; • Gebruikers hun sessie expliciet hebben laten verlopen; • De limiet voor het verlopen voor de harde sessie is bereikt.
Eis.10	De leverancier van het zaaksysteem zorgt ervoor dat de gegevens van de veiligheidsregio op een passende wijze versleuteld opgeslagen worden.
Eis.11	<p>Het zaaksysteem is voorzien van een robuust inlogstelsel.</p> <p><i>Toelichting: onder een robuust inlogstelsel wordt onderstaande minimaal geëist:</i></p> <ul style="list-style-type: none"> • Gebruikersnaam en wachtwoord zijn gehashed in zaaksysteem; • Wachtwoordlengte is minimaal 8 posities en complex van samenstelling;

Nr	Omschrijving
	<ul style="list-style-type: none"> • De geldigheidsduur van de wachtwoorden is instelbaar; • Het zaaksysteem dwingt af dat standaard wachtwoorden bij het eerste gebruik gewijzigd moeten worden; • Het wachtwoord is bij invoer niet zichtbaar; • Een herhaalde foutieve aanmelding zorgt voor een time-out van de gebruiker. Nadat voor een gebruikersnaam drie keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker een verzoek indient deze lock-out op te heffen of het wachtwoord te resetten volgens de gestelde procedure. <p>In het geval van een SAML-koppeling vervalt deze eis voor standaard gebruikers. De eis blijft staan voor bijzondere autorisaties (bijvoorbeeld de beheerders van de leverancier die niet gebruik kunnen maken van de SAML-koppeling).</p>
Eis.12	<p>Het zaaksysteem voorziet standaard in een niet-muteerbare audit-trail (logging), waarin automatische registratie en opslag van de navolgende gegevens plaats vindt:</p> <ul style="list-style-type: none"> • Gebruik van technische beheerfuncties; • Gebruik van functionele beheerfuncties; • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren van gebruikers, toekennen en intrekken van rechten, wachtwoord resetten, uitgifte en intrekken van cryptosleutels (certificaten); • Beveiligingsincidenten, zoals de aanwezigheid van malware, testen op kwetsbaarheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van Security Services; • Verstoringen in het productieproces, zoals het vollopen van queues, systeemfouten, afbreken tijdens het uitvoeren van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of -systemen; • Handelingen van gebruikers. <p>De audit-trail wordt regelmatig beoordeeld door de leverancier en is door functioneel beheer te raadplegen.</p>
Eis.13	<p>De audit-trail dient minimaal 6 maanden bewaard te worden. In het geval van een beveiligingsincident moet de minimale bewaartermijn verlengd kunnen worden tot 3 jaar, of geëxporteerd kunnen worden.</p>
Eis.14	<p>Het zaaksysteem heeft standaard een mechanisme om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.</p>
Eis.15	<p>De leverancier van het zaaksysteem heeft versiebeheer adequaat geregeld en stelt de Veiligheidsregio Noord-Holland Noord tijdig op de hoogte van de actueel te gebruiken versies.</p>
Eis.16	<p>De leverancier van het zaaksysteem heeft een patchmanagementproces welke volgens vastgestelde procedures uitgevoerd wordt. Naast het proces en de procedure dient de leverancier te borgen dat vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code.</p> <p><i>Toelichting:</i> als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.</p>

Nr	Omschrijving
Eis.17	De leverancier van het zaakstelsel heeft het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen vastgelegd.
Eis.18	De leverancier van het zaakstelsel moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
Eis.19	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. Voor bijzondere (beheer)authorisaties dient er een vier ogen procedure te zijn.
Eis.20	Multi-factor authenticatie is mogelijk. Het zaakstelsel voorziet er standaard in dat conditie gebonden (o.a. bijzondere (beheer)authorisaties) multi-factor authenticatie kan worden ingezet.
Eis.21	<p>Voor zover er binnen het zaakstelsel sprake is van uitwisseling van autorisatie- en authenticatiegegevens, wordt dit gedaan op basis van de SAML-standaard (versie 2.0).</p> <p><i>Toelichting: VRNHN gebruikt Okta voor de single sign on en online identity provider.</i> https://www.okta.com/</p> <p><i>Toelichting SAML standaard: https://www.forumstandaardisatie.nl/open-standaarden/saml</i></p>
Eis.22	<p>Met betrekking tot de web-omgeving van het zaakstelsel, de verbinding daar naartoe en de adressering hierbij, voldoet het zaakstelsel aan de volgende standaarden:</p> <ul style="list-style-type: none"> • DNSSEC (RFC 4033, 4034 en 4035); • HTTPS en HSTS (versie 1.2); • TLS (minimaal versie 1.2 en versie 1.3); • IPv6 en IPv4. <p><i>Toelichting: https://www.forumstandaardisatie.nl/open-standaarden. De van toepassing zijnde standaarden zijn conform de richtlijnen van het NCSC en het forum van standaardisatie. Het zaakstelsel beweegt mee met wijzigingen van de richtlijnen van het NCSC en het forum van standaardisatie.</i></p>
Eis.23	<p>Voor zover er binnen het zaakstelsel sprake is van emailfunctionaliteit (het versturen dan wel ontvangen van mails), voldoet het zaakstelsel aan de navolgende standaarden:</p> <ul style="list-style-type: none"> • DKIM (RFC 6376); • DMARC (RFC 7489); • SPF (versie 1). <p><i>Toelichting: https://www.forumstandaardisatie.nl/open-standaarden. De van toepassing zijnde standaarden zijn conform de richtlijnen van het NCSC en het forum van standaardisatie. Het zaakstelsel beweegt mee met wijzigingen van de richtlijnen van het NCSC en het forum van standaardisatie.</i></p>
Eis.24	<p>Voor zover er binnen het zaakstelsel sprake is van een verbinding tussen twee of meerdere emailservers, voldoet het zaakstelsel eveneens aan de navolgende standaarden:</p> <ul style="list-style-type: none"> • STARTTLS (RFC 3207); • DANE (RFC 7672). <p><i>Toelichting: https://www.forumstandaardisatie.nl/open-standaarden. De van toepassing zijnde standaarden zijn conform de richtlijnen van het NCSC en het forum van standaardisatie. Het zaakstelsel beweegt mee met wijzigingen van de richtlijnen van het NCSC en het forum van standaardisatie.</i></p>

Nr	Omschrijving
Eis.25	In het zaaksysteem is het mogelijk dat gebruikers meerdere autorisaties (rollen) hebben. Rollen met betrekking tot beheer taken, moeten gescheiden uitgevoerd kunnen worden van gebruikers taken. Het toewijzen en gebruik van speciale toegangsrechten behoort te worden beperkt en beheerst.
Eis.26	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. Waarbij minimaal de identiteit en het feit dat de gebruiker recht heeft, vastgesteld is. <i>Toelichting:</i> Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit en het feit dat de gebruiker recht heeft op het authenticatiemiddel vastgesteld.
Eis.27	De leverancier van het zaaksysteem dient een verwerkersovereenkomst volgens model VR-NHN aan te gaan waarin o.a. relevante wettelijke, statutaire, regelgevende, contractuele en passende technische en organisatorische beheersmaatregelen zijn opgenomen.
Eis.28	De onderlinge netwerkconnecties (koppelvlakken) van het zaaksysteem met systemen van VRNHN behoren te worden bewaakt, geanalyseerd op kwaadaardige elementen middels detectie voorziening.
Eis.29	Als het zaaksysteem voorziet in module voor archivering dan dient dit gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.
Eis.30	De leverancier van het zaaksysteem realiseert de volgende scheiding van clouddienstverlening: <ul style="list-style-type: none"> • Onderlinge scheiding van CSC's in een multi-tenant omgeving; • Scheiding tussen de afgenomen cloud-service en de interne informatievoorziening van de CSP; • De CSP maakt het mogelijk om de beoogde scheiding van clouddiensten te verifiëren.
Eis.31	Bij Multi-tenancy wordt het zaaksysteem zodanig ingericht, dat data van VRNHN op versleutelde datadragers is opgeslagen en gescheiden wordt verwerkt op gehardende (virtuele) machines.
Eis.32	Ter bescherming tegen malware dienen beheersmaatregelen te zijn geïmplementeerd voor detectie, preventie en herstel.
Eis.33	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld
Eis.34	De leverancier van het zaaksysteem heeft een escalatieprocedure en een meldingssysteem voor het melden van inbreuken op informatiebeveiliging, datalekken en technische kwetsbaarheden. Leverancier voegt deze bij de inschrijving toe en dit document zal, na gunning, onderdeel uitmaken van het verificatiegesprek om gezamenlijk vast te stellen dan wel aan te passen.
Eis.35	De leverancier van het zaaksysteem behoort minimaal één keer per jaar de naleving van de cloud beveiligingsovereenkomsten met de Cloud Service Provider op compliance te beoordelen en jaarlijks een assurance verklaring aan de VRNHN uit te brengen. Dit kan d.m.v. Interne controle, accountants verklaring of leveranciersbeoordeling.
Eis.36	Er wordt een dagelijkse back-up gemaakt van het zaaksysteem. De leverancier van het zaaksysteem maakt dagelijks een back-up van alle data met een retentietijd van minimaal 60 dagen. De back-ups moeten worden gecontroleerd op compleetheid en teruggezet kunnen worden naar de productieomgeving. De leverancier rapporteert aan geautoriseerde personen indien de back-up niet gerealiseerd is.

Nr	Omschrijving
Eis.37	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.
Eis.38	De leverancier van het zaakstelsel dient een globale systeem beschrijving op te leveren inclusief de benodigde koppelingen.
Schaalbaarheid versus apps	
Eis.39	De interface van het zaakstelsel werkt op basis van HTML5 of hoger (alles binnen de browser). De backoffice maakt dus geen gebruik van ingebouwde plug-ins die apart geïnstalleerd moeten worden.
Eis.40	Dataportabiliteit dient gegarandeerd te zijn door het toepassen van standaarden voor datauitwisseling.
Beheer en Releasemanagement	
Eis.41	De leverancier van het zaakstelsel garandeert dat alle instellingen en wijzigingen binnen het zaakstelsel die door de eindgebruiker zelf kunnen worden gedaan, niet overschreven (kunnen) worden bij de implementatie van nieuwe releases (patches, bug fixes, etc.). Bij wijzigingen in de structuur van het systeem waardoor bovenstaande niet mogelijk is, levert de leverancier hiervoor aparte tooling om deze instellingen afzonderlijk te exporteren en na de update weer te importeren.
Eis.42	De leverancier van het zaakstelsel heeft een acceptatie en productie omgeving die logisch (d.w.z. softwarematig en op databaseniveau) gescheiden zijn. En heeft een acceptatie omgeving die qua functionaliteit en beveiliging gelijkwaardig is aan de productie omgeving.
Eis.43	De leverancier van het zaakstelsel werkt volgens een OTAP-proces (Ontwikkelen, Testen, Acceptatie en Productie). <i>Toelichting: Patches, releases en changes worden altijd eerst in de acceptatie omgeving aan de functioneel beheerder van VRNHN aangeboden zodat deze kan testen en de impact van de patches, releases of changes voor de productie omgeving kan bepalen.</i>
Beschikbaarheid en beveiliging van het zaakstelsel	
Eis.44	De leverancier van het zaakstelsel garandeert responsetijden van < 3 seconde in de gebruikersinterface voor elke gebruiker (ongeacht het aantal gebruikers) van het zaakstelsel, bij het invoeren van informatie en het schakelen tussen velden en schermen. Dit geldt niet voor het genereren van overzichten en rapportages, en uploaden van bestanden.
Eis.45	Beveiliging van kopieën (o.a. back-up) van gegevens bevinden zich minimaal op dezelfde norm als de primaire gegevens.
Eis.46	Gegevens uit productieomgeving worden niet gebruikt in ontwikkel- en testomgevingen tenzij deze zijn geanonimiseerd of de verwerkingsverantwoordelijke hier toestemming voor heeft gegeven.
Koppelingen	
Eis.47	Het zaakstelsel beschikt standaard over de mogelijkheid om medewerkersgegevens minimaal eenmaal per dag te kunnen importeren vanuit het E-HRM systeem (Afas) van de opdrachtgever. <i>Toelichting: VRNHN werkt met het E-HRM systeem van AFAS. Medewerkersgegevens worden door AFAS aangeboden via een zogenaamde GET-connector. De GET-Connector biedt alleen gegevens aan. Het zaakstelsel moet de GET-connector actief bevragen om gegevens te kunnen ontvangen. De medewerkersgegevens uit AFAS fungeren als stamgegevens voor de gebruikers in het zaakstelsel. Te denken valt minimaal aan: voornaam, achternaam, mailadres, functienaam, leidinggevende, organisatorische eenheid,</i>

Nr	Omschrijving
	<i>locatie. Technische documentatie is hier te vinden:</i> https://help.afas.nl/?query=get%20connector
Eis.48	<p>Het zaaksysteem kan automatisch door middel van gangbare open standaarden data uitwisselen met een Business intelligence (BI) tooling zoals Power BI, zoals de geformuleerd in het Forum Standaardisatie:</p> <ul style="list-style-type: none"> • OpenAPI specification (3.0); • JSON (RFC8259, december 2017); • OAuth (2.0); • OData (4.0); • REST API Design Rules (1.0); • SOAP (1.2); • WSDL (2.0); • XML (1.0, fifth edition). <p><i>Toelichting:</i> https://www.forumstandaardisatie.nl/open-standaarden.</p>
Eis.49	<p>Bij een update of upgrade van het zaaksysteem zorgt de Leverancier ervoor dat bestaande koppelingen blijven functioneren. Dit onder de voorwaarde dat leverancier voldoet aan N-1 (Nieuwste standaard minus 1 versies) voor de vereiste Programmatuur.</p>
Eis.50	<p>De services en koppelingen van toepassing voor het zaaksysteem zijn functioneel en technisch beschreven en worden door de leverancier opgeleverd bij acceptatie van het zaaksysteem.</p>

2. “Concept” Eisen AVG

Nr	Omschrijving
Eis.51	Leverancier verklaart invulling te kunnen geven aan de inhoud van de Verwerkersovereenkomst van de VRNHN (deze is als bijlage bij de aanbestedingsdocumenten gevoegd). De Verwerkersovereenkomst van VRNHN is opgesteld op basis van het landelijke standaard model van de IBD. Voor contractondertekening worden de beheersmaatregelen voortvloeiend uit de Verwerkersovereenkomst afgestemd tussen Leverancier en VRNHN.
Eis.52	Leverancier verklaart dat de diensten worden uitgevoerd volgens de vereisten uit de Algemene Verordening Gegevensbescherming en aanverwante regelgeving.
Eis.53	Leverancier verklaart de beginselen van Privacy by Design en Privacy by Default toe te passen bij het ontwikkelen van nieuwe diensten, producten of functionaliteiten binnen bestaande producten of diensten en is in staat dit aan te tonen.
Eis.54	Leverancier verklaart de beginselen van Privacy by Design en Privacy by Default te hebben toegepast ten aanzien van de verwerking van persoonsgegevens binnen de dienstverlening en de ICT-prestatie (zie artikel 1.15 GIBIT) en is in staat dit aan te tonen.