Bijlage A tabblad 2: informatiebeveiliging - programma van eisen e t.b.v. de offerteaanvraag Network As A Service (NAAS)

Eis/Wens	Nr.	Categorie	Beschrijving	Antwoord/opmerking
E	1	Audit en Pentest	Leverancier werkt mee aan audits en pentesten op verzoek van de gemeente (right to audit). Leverancier laat, bij hosting, periodiek (minimaal 1x per jaar) een Grey box pentest uitvoeren, waarbij een kwetsbaarheids-scan onderdeel vormt van de pentest, op zijn systemen binnen de scope van de dienstverlening. De resultaten van deze pentest, de opvolging van de testresultaten en de oplossingsmogelijkheden worden gerapporteerd aan de gemeente. Daarbij is vereist dat alle high-risk bevindingen opgelost worden binnen de vastgestelde tijd conform de SLA.	
E	2	Audit en Pentest	Vóór oplevering wordt een pentest uitgevoerd en de kritieke bevindingen worden binnen twee weken verholpen, de overige bevindingen binnen twee maanden. De PENTEST wordt door een onafhankelijke partij uitgevoerd.	
E	3	Authenticatie	Iedere gebruiker, dus ook beheerder, dus ook van de aanbieder, heeft een eigen account op naam.	
E	4	Autorisatie	De software heeft een mogelijkheid om vastgelegde autorisaties op alle niveaus inzichtelijk te maken per persoon, per gebruikersgroep en rol. Hiervoor is het toegepaste autorisatieschema te exporteren naar een bestand, dat leesbaar en interpreteerbaar is voor derden (zoals toezichthouders zoals bijvoorbeeld de accountant, auditors, etc.).	
E	5	Backup en herstel	Indien er sprake is van (gedeeltelijke) SAAS- of PAAS oplossingen, is de leverancier onder enig voorbehoud verantwoordelijk voor backup, restore, recovery en uitwijk met betrekking tot de gehele oplossing. Hierbij geldt een Recovery Point Objective van maximaal 24 uur en een Recovery Time Objective van maximaal 4 uur.	
E	6	Beheer	De beheerportalen mogen niet zonder beperkingen worden blootgesteld.	
E	7	Beveiligingsstandaarden	De leverancier past de hardening richtlijnen van zowel NIST SP 800-53 als CIS Benchmarks toe, om een robuuste en veilige IT-infrastructuur te waarborgen	
E	8	Beveiligingsstandaarden	Alle verplichte beveiligingsstandaarden van het forum standaardisatie zijn toegepast. De leverancier garandeert dat dit zo blijft bij wijzigingen van deze standaarden gedurende de looptijd van het contract, zie voor de huidige lijst, zie kolom opmerking.	https://www.forumstandaardisatie.nl/open-standaarden/verplicht?trefwoord=172
E	9	Beveiligingsstandaarden	Indien er sprake is van (gedeeltelijke) SAAS- of PAASoplossingen, is de basisbeveiliging van de software en mailcomponement op orde volgens test van internet.nl.	
E	10	Beveiligingsstandaarden	De webinterface van de software is beveiligd tegen de OWASP-top 10 en de leverancier garandeert dat dit gedurende de looptijd van het contract zo blijft.	
E	11	Beveiligingsstandaarden	Mail is beveiligd met STARTTLS over ten minste het TLS1.3 protocol, DANE, DNSSEC of gekoppeld met Exchange Online via MS Graph	
	12	Beveiligingsstandaarden	De leverancier past de ICT-beveiligingsrichtlijnen voor webapplicaties toe (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties)	
w	13	Bewustwording	de leverancier moet in staat zijn om training en bewustwordingssessies te geven aan gebruikers om hen te helpen veilige praktijken te begrijpen en te implementeren.	.
E	14	Change management	De leverancier moet beschikken over een solide changemanagement- en gebruikersbeheerproces.	
E	15	Compatibiliteit	Indien er sprake is van (gedeeltelijke) SAAS- of PAAS-oplossingen, zijn deze oplossingen benaderbaar via een browser userinterface en is compatible met Microsoft, Android en Apple op basis van de laatste én voorlaatste versies van het operating systeem.	.
E	16	Cookie beheer	Er worden geen vertrouwelijke gegevens in cookies opgeslagen.	
E	17	Cookie beheer	Cookies ten behoeve van authenticatie worden niet persistent opgeslagen.	
E	18	Cookie beheer	Leverancier gebruikt unieke namen, paden en domeinen voor cookies ten behoeve van authenticatie (cookie parameters 'name', 'path' en 'domain').	
E	19	DDoS bescherming	Er zijn maatregelen genomen om de applicatie te beschermen tegen DDOS aanvallen.	
w	20	Export functionaliteit	Het is belangrijk dat de softwareoplossing de mogelijkheid biedt om gegevens te exporteren in een gestandaardiseerd formaat, voor het geval de gemeente besluit om over te stappen naar een andere oplossing.	
E	21	Gegevensbeheer	De leverancier biedt een procedure voor het verwijderen van data/informatie (Niet zijnde Exit strategie).	
E	22	Gegevensbeheer	De SAAS-/Cloud-oplossing dient ervoor te zorgen dat de gegevens/documenten worden opgeslagen in een datacenter/cloudserver binnen de Europese Unie en het is vereist dat de leverancier/eigenaar van de SAAS-/Cloud-oplossing een Europees bedrijf is.	
w	23	Gegevensbeheer	De leverancier moet duidelijke beleidslijnen en procedures hebben voor het beheren van de levenscyclus van gegevens, inclusief creatie, opslag, gebruik, delen, archiveren en vernietigen.	
w	24	Incident management	de leverancier moet een incidentresponsplan hebben en in staat zijn om snel en adequaat te reageren op beveiligingsincidenten. Ze moeten ook in staat zijn om regelmatig te rapporteren over incidenten en hun status.	
E	25	Integratie	De software werkt binnen de Citrix/Ivanti omgeving van de gemeente en werkt clientonafhankelijk. Alle in dit document als aanwezig genoemde functionaliteiten moeten beschikbaar zijn in Microsoft O365, via een browser. Indien niet alle functionaliteiten beschikbaar, bij de betreffende functionaliteit bij de toelichting aangeven in welke client deze functionaliteit niet beschikbaar is	
E	26	Logging	De software biedt zodanige functionaliteit m.b.t. auditing/logging dat van alle relevante handelingen en pogingen daartoe voor wat betreft processen, processtappen en statuswijzigingen - zowel door gebruikers als de oplossing zelf - door middel van logging een historie wordt vastgelegd (van welke handelingen en pogingen daartoe, wanneer en door wie zijn uitgevoerd). Deze auditing/logging dient zonder tussenkomst van de leverancier door functioneel en daartoe geautoriseerde gebruikers bekeken te kunnen worden.	
w	27	Logging	Applicatie logging is te koppelen aan een SIEM ten behoeven vanmonitoren van beveiligingsgebeurtenissen en het detecteren van mogelijke inbreuken	
w	28	Patchmanagement	Er moet een duidelijk beleid zijn voor hoe en wanneer beveiligingsupdates en patches worden uitgevoerd om ervoor te zorgen dat de software altijd up-to-date is.	
E	29	Plug-in beheer	Wanneer de (gedeeltelijke) SAAS- of PAAS-oplossingen via een browser worden benaderd, worden er voor de werking van de software géén plugins lokaal geïnstalleerd.	
w	30	Rapportage	De leverancier moet minmaal 4x per jaar beveiligingscontroles uitvoeren en de resultaten hiervan aan de gemeente rapporteren.	
E	31	Regelgeving	De software functioneert voor wat betreft aspecten van beveiliging en privacy volledig conform alle betreffende wet- en regelgeving (ten minste AVG en BIO) en andere van toepassing zijnde wetgeving, tenzij door de inschrijver nadrukkelijk anderzijds in de inschrijving aangegeven. De BIO voldoet uiteraard enkel voor de reikwijdte die redelijkerwijs aan een SaaS-leverancier kan en behoort te worden gesteld. Wij verwijzen in dit kader expliciet naar die BIO-eisen waarbij in de kolom "Verantwoordelijke" (ondermeer) de "Dienstenleverancier" wordt benoemd.	
E	32	Sessiebeheer	Voor een applicatie met een hoog beveiligingsniveau moeten sessies automatisch worden beëindigd na 5 minuten van inactiviteit, om ongeoorloofde toegang tot gevoelige gegevens te minimaliseren, of aansluiten op conditional access van MS Entra (AzureAD)	
E	33	Sessiebeheer	Voor een applicatie met een laag beveiligingsniveau moeten sessies automatisch worden beëindigd na 15 minuten van inactiviteit, om ongeoorloofde toegang te minimaliseren	Azure AD
E	34	Sessiebeheer	Kritieke en vertrouwelijke sessiewaardes worden niet doorgegeven via een query string.	
E	35	Testomgeving	Het is mogelijk de test omgeving op te zetten door de productie omgeving te kopiëren zonder daarbij de persoonsgegevens uit de productie omgeving mee te kopieren.	
E	36	Toegangscontrole	Toekenning van autorisaties wordt gedaan middels groepslidmaatschappen in de Azure active directory.	
E	37	Toegangscontrole	SAAS- of PAAS-oplossingen ondersteunen het gebruik van Multi-Factor Authenticatie (MFA) en Single Sign-On (SSO) indien van toepassing. De software ondersteunt veilig inloggen door SSO door middel van OAuth en SAML en federatie met Azure AD.	
E	38	Toegangscontrole	Gebruikers behoren alleen toegang te krijgen tot de informatie die behoort bij hun functie en rol.	autorisatiematrix
E	39	Versleuting	De software ondersteunt TLS 1.3 met betrekking tot de API-koppelingen voor gegevensuitwisselingen.	
E	40	Versleuting	De gegevens die opgeslagen zijn (zowel in de back-up als in rust) en de gegevens die worden overgedragen, worden gedurende de gehele duur van het contract versleuteld volgens de geldende standaarden. Op dit moment is de standaard voor gegevensoverdracht TLS 1.3 en voor gegevens in rust wordt Advanced Encryption Standard (AES)-256 gebruikt. Het is belangrijk dat de prestaties acceptabel zijn.	
E	41	wachtwoordbeheer	Er wordt geen gebruik gemaakt van een standaard wachtwoord. Ieder toegekend wachtwoord is willekeurig gegenereerd.	
E	42	wachtwoordbeheer	Voor het beheren van wachtwoorden van speciale accounts (bijv. admin- of serviceaccounts) wordt een passwordmanager gebruikt. Geen account heeft hetzelfde wachtwoord. Voor toegang tot de wachtwoordkluis is twee factor-authenticatie nodig	
E	43	wachtwoordbeheer	Wachtwoorden van accounts van diensten (service accounts) dienen complex te zijn en tenminste 20 karakters lang.	

E	44	Privacy	Leverancier moet bereid zijn om een DPIA of pre-PIA uit te voeren indien nodig.	
E	45	Privacy	De applicatie moet passende technische en organisatorische maatregelen ondersteunen om de privacy van persoonlijke gegevens te waarborgen vanaf het ontwerp en de standaardinstellingen.	
E	46	Privacy	De applicatie moet functionaliteit bieden om individuen in staat te stellen hun rechten uit te oefenen, zoals toegang, rectificatie, verwijdering en dataportabiliteit van hun persoonlijke gegevens.	
E	47	Privacy	De applicatie moet een geautomatiseerd proces hebben voor het detecteren, rapporteren en reageren op inbreuken op de beveiliging van persoonsgegevens.	Meldingsplicht datalekken
E	48	Privacy	Indien persoonsgegevens worden verwerkt, dient er een verwerkersovereenkomst te worden opgesteld tussen de leverancier en gemeente	
E	49	Privacy	De applicatie moet de mogelijkheid bieden om persoonsgegevens alleen te verwerken voor specifieke, welomschreven en rechtmatige doeleinden	
E	50	Privacy	De applicatie moet functionaliteit bieden om gegevensbewaartermijnen in te stellen en te handhaven, zodat persoonsgegevens niet langer worden bewaard dan noodzakelijk, in overeenstemming met de geldende wettelijke en reglementaire vereisten.	
E	51	AI en Machine learning	AI-functionaliteiten mogen alleen worden ingeschakeld na expliciete toestemming van de opdrachtgever en er dient een Data Protection Impact Assessment (DPIA) te zijn uitgevoerd. De opdrachtgever blijft te allen tijde eigenaar van de data. Afwijkingen hiervan, zoals de integratie van AI-functionaliteiten zonder voorafgaande toestemming of zonder een DPIA, worden formeel ter besluitvorming aan de opdrachtgever voorgelegd. De leverancier moet aantonen hoe AI binnen de systemen wordt geïntegreerd met inachtneming van privacy, ethiek en naleving van relevante wetgeving zoals de AVG en BIO.	
E	52	Beveiliging	Leverancier past Zero Trust toe en verplicht NAC voor alle netwerktoegang.	
E	53	Incidentmanagement	Beveiligingsincidenten worden binnen 4 uur gemeld en geregistreerd.	
E	54	Compliance	Leverancier levert aantoonbaar bewijs van naleving BIO en NIS2.	
E	55	Logging & Monitoring	Alle beheerhandelingen worden volledig gelogd en minimaal 1 jaar bewaard.	
E	56	Exit-strategie	Bij einde contract vindt volledige overdracht plaats van data, logs en configuraties.	