

Programma van Eisen

Veilig mailen en uitwisselen bestanden

25.O.152

Shared Service Centrum

Functionele eisen	
1.	Het systeem moet volledig integreren met Microsoft 365/Outlook, (Outlook classic, het nieuwe Outlook en Outlook op het web), waarbij het opstellen, verzenden en lezen van beveiligde berichten binnen de vertrouwde Outlook-interface plaatsvindt.
2.	Het systeem moet beveiligd verzonden berichten terugvindbaar en doorzoekbaar maken vanuit de reguliere mailclient, waaronder in de map Verzonden items van Outlook.
3.	Gebruikers moeten zonder extra handelingen veilig kunnen mailen. Met extra
4.	Het systeem legt bij berichten en bijlagen minimaal de volgende metadata vast: - Identificatienummer - Bestandsnaam - Ontvanger - Verzender - Datum van verzending/ontvangst - Datum van creatie - Status (concept of verzonden) -Beveiligingsclassificatie
5.	Het systeem stuurt bovenstaande metadata mee bij verplaatsing/kopiëren berichten en bijlagen naar andere locaties zoals Teams/SP en Zaaksysteem en legt in de metadata vast dat het bericht en bijlage zijn verplaatst/gekopieerd naar Teams/SP en Zaaksysteem (indien technisch ondersteund).
6.	De oplossing maakt veilige bestanduitwisseling mogelijk van bestanden tot maximaal 50GB via de oplossing te versturen, zowel binnen de organisatie als daarbuiten. De oplossing biedt de mogelijkheid om deze maximale grootte per use-case te verhogen.
7.	De oplossing ondersteunt het verifiëren van ontvangers door middel van een door de verzender vast te stellen authenticatiemethode.
8.	De oplossing beschikt over een beveiligde conversatiestarter die via een publiceerbare URL beschikbaar kan worden gesteld, waarmee externe partijen veilig berichten en bestanden kunnen uitwisselen met de organisatie zonder dat vooraf een account hoeft te worden aangemaakt.
9.	De oplossing ondersteunt archivering van e-mailberichten naar het archiveringssysteem van de organisatie (bijvoorbeeld via een beveiligde API), waarbij de scope van de te archiveren berichten vooraf configureerbaar is.
10.	Het systeem moet de organisatie in staat stellen centraal beleid te configureren waarin per doelgroep, ontvangerdomein of gegevensclassificatie is vastgelegd wanneer beveiligde verzending verplicht, geadviseerd of optioneel is.
11.	Wanneer een externe ontvanger een beveiligd bericht ontvangt, moet deze het bericht en de bijlagen kunnen openen zonder accountregistratie of software-installatie, op zowel desktop als mobiel.
12.	Indien een bericht niet kan worden verzonden (bijvoorbeeld door een ontbrekende sessie of verbinding), moet het systeem de gebruiker direct en ondubbelzinnig informeren en het bericht als concept bewaren; een bericht mag nooit ongemerkt verloren gaan.
13.	De oplossing faciliteert aantoonbaar verzend-, aflever- en ontvangstbewijzen voor beveiligde berichten.
14.	De aangeboden oplossing voor veilig mailen moet volledig bruikbaar zijn vanuit zowel persoonlijke en gedeelde mailboxen. Gebruikers moeten namens een gedeelde mailbox beveiligde berichten kunnen verzenden, ontvangen, openen en beheren, waarbij alle functionaliteiten voor veilig mailen beschikbaar blijven.

15.	De oplossing biedt de verzender de mogelijkheid om na verzending de toegang tot een e-mail en de bijbehorende bestanden met gevoelige gegevens op afstand in te trekken. Na intrekking kan de ontvanger de betreffende e-mail en bestanden niet langer openen of raadplegen via de oplossing.

Eisen Architectuur en standaarden	
16.	Op basis van het afgesloten contract garandeert de Inschrijver dat het systeem, gedurende de contractperiode, doorontwikkeld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief, ook verstaan dat op het systeem adaptief onderhoud wordt uitgevoerd om als Opdrachtgever te blijven voldoen aan in de contractperiode geldende wet- en regelgeving en inspeelt op ontwikkelingen in de markt. Nieuwe ontwikkelingen op grond van specifieke wensen van de Opdrachtgever vallen hierbuiten.
17.	Inschrijver waarborgt dat het aangeboden systeem te allen tijde voldoet aan de actuele open standaarden met een 'pas toe of leg uit'-verplichting van het Forum Standaardisatie die voor het systeem van toepassing zijn. • Indien een standaard op deze lijst wordt gewijzigd of vervangen, verwerkt de Inschrijver deze wijziging binnen 12 maanden nadat de gewijzigde/nieuwe standaard door het Forum Standaardisatie als verplicht is aangewezen. • Om continuïteit te waarborgen, blijft de voorgaande (vervallen) standaard/versie door de Leverancier nog minimaal 12 maanden na de wijzigingsdatum ondersteund binnen het systeem. • Leverancier toont bij inschrijving en gedurende de looptijd op verzoek aan welke specifieke (versies van) open standaarden worden gehanteerd.
18.	Er worden twee omgevingen opgeleverd. De productieomgeving en een testomgeving die is bedoeld voor het testen van, (1) configuratie(s) en (2) koppelingen met andere systemen.
19.	~~De testomgeving moet gevuld kunnen worden met gegevens van vergelijkbare productieomvang, waarbij data geanonimiseerd/gepseudonimiseerd moet kunnen worden.~~ De oplossing beschikt over minimaal één testomgeving die logisch is gescheiden van de productieomgeving. SSC Ons moet hierin configuraties en koppelingen met andere systemen kunnen testen voordat deze in productie worden genomen. De testomgeving dient het gebruik van meerdere testgebruikers en shared mailboxen te ondersteunen en moet voldoende representatief zijn voor het uitvoeren van tests voor configuratiewijzigingen en nieuwe koppelingen met andere systemen.
20.	Aanpassingen in de test omgeving kunnen zonder tussenkomst van de leverancier flexibel naar de productie omgeving worden gebracht.
21.	Het systeem ondersteunt het gebruik van tablets, smartphones en andere mobiele devices zonder in te leveren op kwaliteit en leesbaarheid van de tekst en met behoud van functionaliteiten. De werking hierop wordt gegarandeerd op recente versies van gangbare platforms/webbrowsers zonder extra plugins: • Windows, MacOS • Edge, Safari, Chrome, Firefox • Android, iOS Het gebruik van browser plugins (zoals bv. Flash, ActiveX, Java Runtime) aan de client/gebruikerskant is niet toegestaan.

22.	Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10
23.	De Oplossing ondersteunt minimaal RBAC en zo mogelijk ABAC en realiseert een volledig geautomatiseerde autorisatie toekenning, waarbij de Identity Provider als bron fungeert voor de functies en rollen binnen de applicatie.
24.	Het systeem hanteert voor berichten en bijlagen duurzame bestandsformaten zoals vastgelegd in de Norm voorkeursformaten. Norm Voorkeursformaten | Nationaal Archief
25.	De oplossing dient als private cloudoplossing te worden geleverd.
26.	De oplossing wordt als SaaS afgenomen.

Eisen Cloud	
27.	Leverancier is, binnen de grenzen van de door hem geleverde ICT-prestatie en invloedssfeer, verantwoordelijk voor het in stand houden van de beschikbaarheid, integriteit en vertrouwelijkheid van de geboden oplossing en de informatie die daarin wordt verwerkt en opgeslagen, conform de normen uit de BIO2 en de van toepassing verklaarde GIBIT 2025.
28.	De hosting en opslag van data vindt plaats vanaf een locatie binnen de Europees Economische Ruimte (EER).
29.	Inschrijver laat minimaal 1 x per jaar een penetratietest uitvoeren op de geleverde dienst en communiceert het resultaat. Kwetsbaarheden worden geclassificeerd en krijgen opvolging.
30.	Authenticatie verloopt via de Identity Provider van de Opdrachtgever. Het systeem ondersteunt authenticatie op basis van Entra ID, SAML 2.0 en OpenID Connect (OIDC). Na authenticatie hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van het aangeboden systeem, uiteraard voor zover ze daartoe zijn geautoriseerd. Hierbij is 2-factor authenticatie vereist.
31.	De Opdrachtgever blijft eigenaar van de gegevens binnen applicatie en deze gegevens mogen niet voor andere doeleinden gebruikt worden door de Leverancier van de applicatie. Dit geldt zowel voor gegevens in de Test- als Productieomgevingen.
32.	Er wordt voorkomen dat gevoelige gegevens worden gecached.
33.	De Content-Security-Policy wordt aangepast op basis van wat exact gebruikt wordt in de website.
34.	De website voldoet aan de Europese cookie richtlijn2.
35.	Er wordt geen gebruik gemaakt van derde partij analytics, trackers en hulpmiddelen in gedeelten en pagina's die alleen met authenticatie beschikbaar zijn.
36.	Er worden geen advertenties ingevoegd in pagina's en diensten die gekoppeld zijn aan de kerntaken van de gemeentelijke dienstverlening.
37.	De website waarop de SAAS applicatie (het systeem) wordt aangeboden dient te voldoen aan minimaal een A rating bij Qualys SSL Labs (https://www.ssllabs.com/) en minimaal een A rating bij Securityheaders (https://www.Securityheaders.com).
38.	De leverancier heeft maatregelen genomen om de toegang tot de broncode van informatiesystemen te beperken tot de medewerkers, die deze code onderhouden of installeren.

Privacy	
39.	De oplossing waarborgt dat uitsluitend verzenders en ontvangers toegang hebben tot de inhoud van berichten. Inschrijver licht toe welke technische en organisatorische maatregelen dit waarborgen.
40.	Inschrijver verleent alle redelijkerwijs benodigde medewerking aan het uitvoeren en actualiseren van een DPIA en verstrekt daarvoor tijdig alle relevante informatie.

Eisen Security	
Generiek	
41.	Leverancier verstrekt gegevens van Opdrachtgever niet aan een overheidsinstantie van een derde land, tenzij en voor zover deze verstrekking verenigbaar is met het toepasselijke Unierecht.
42.	Leverancier toetst ieder verzoek van een overheidsinstantie van een derde land tot toegang tot gegevens van Opdrachtgever vooraf op rechtmatigheid en betwist het verzoek indien daarvoor naar toepasselijk recht redelijke juridische gronden bestaan.
43.	Leverancier informeert Opdrachtgever onverwijld over een dergelijk verzoek, tenzij dit op grond van een wettelijk voorschrift verboden is. Indien onmiddellijke kennisgeving wettelijk verboden is, informeert Leverancier Opdrachtgever zodra dat verbod niet langer van toepassing is.
44.	Het product voldoet aan de norm NTA 7516 (of logische opvolger). De leverancier stuurt de link door naar de publicatie waarin zij aangeven aan welke eisen van de NTA 7516 zij al voldoet en/of gaat voldoen. De Leverancier verklaart zich te certificeren voor de NTA 7516 wanneer mogelijk.
45.	De aangeboden oplossing mag niet voortgebracht worden door landen met een actief cyberprogramma tegen de EER en/of genoemd worden op de lijst met statelijke actoren gepubliceerd door AIVD/MIVD en NCTV.
46.	Het systeem moet beveiligde berichten verzenden vanaf het afzenderdomein van de organisatie, in de huisstijl van de organisatie en met correcte SPF-, DKIM- en DMARC-afhandeling, zodat berichten herkenbaar en betrouwbaar zijn en spam-classificatie wordt geminimaliseerd.
47.	De Leverancier beschikt over een aantoonbaar en geldige ISAE3000 Type II-verklaring, SOC 2 (of gelijkwaardig assurance-rapport). De Leverancier verstrekt deze rapportages en eventuele onderliggende certificeringsdocumentatie op verzoek kosteloos aan de Opdrachtgever.
48.	Er wordt altijd gebruik gemaakt van best-practice encryptiestandaarden en sleutellengtes. Voor standaarden vanuit de beveiligingsrichtlijn vanuit de NCSC gebruikt worden geldt dat deze zijn toegestaan wanneer deze in de richtlijn de status “Goed” hebben gekregen. Voor bestaande toepassingen geldt dat het gebruik van een in de NCSC richtlijn beschreven standaard met de status “Voldoende“ ook acceptabel is.
49.	Voor symmetrische versleuteling wordt gebruik gemaakt van algoritmes en cipher modes, die de status “acceptabel” hebben in NIST SP800-131A.
50.	AES wordt toegepast in een veilige “mode of operation”, zoals beschreven in NIST SP800-131A.
51.	Er wordt gebruik gemaakt van de in de FIPS 197 standaard gepubliceerde minimale sleutellengte.
52.	De websites worden altijd versleuteld dan wel voorzien van PKIoverheid Extended Validation SSL certificaat (EV SSL) (of vergelijkbaar).
53.	De oplossing ondersteunt versleutelde opslag van e-mailberichten en bijlagen die gevoelige gegevens bevatten, waarbij gebruik wordt gemaakt van cryptografische maatregelen conform de laatste stand der techniek.
54.	Alle e-mail die via de oplossing wordt verzonden, wordt tijdens transport versleuteld volgens de laatste stand der techniek.
55.	De Leverancier kan niet zonder medewerking van de Opdrachtgever beschikken over de cryptografische sleutels waarmee gegevens van de Opdrachtgever worden beschermd.
56.	Er is sprake van logging in het systeem. Relevante zaken om te loggen zijn: • Type gebeurtenis (zoals back-up/restore, reset wachtwoord, betreden ruimte);

	• (poging tot) Ongeautoriseerde toegang; • Handelingen van gebruikers met speciale bevoegdheden, waarbij alle handelingen van hen worden gelogd; • Systeemwaarschuwingen; • (poging tot) Wijziging van de beveiligingsinstellingen.
57.	Bij de verwerking van persoonsgegevens worden in de log aanvullend de volgende zaken opgenomen: • Ontvangen gegevens; • Gestelde vraag; • Datum/tijdstip van aanroep; • Naam van leverende of afnemende bron of systeem; • Een gebruikersnaam of ID; • Eventuele transformaties of verrijkingen; • Eventueel opgetreden fouten.
58.	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; • De gebeurtenis; • Waar mogelijk de identiteit van het werkstation of de locatie; • Het object waarop de handeling werd uitgevoerd; • Het resultaat van de handeling; • De datum en het tijdstip van de gebeurtenis.
59.	De logbestanden van het systeem zijn alleen toegankelijk voor daartoe geautoriseerde medewerkers.
60.	Logging kan op basis van één van de formats CEF, JSON of Syslog naar het SIEM van de Opdrachtgever worden gestuurd worden.
61.	Het product moet volledige logboekregistratie bieden van alle relevante gebeurtenissen rond het verzenden en ontvangen van beveiligde e-mails, inclusief minimaal hoe en wanneer de werknemer werd geverifieerd toen het bericht werd verzonden, werd het bericht afgeleverd op de ontvangende server, met welke beveiliging werd het bericht afgeleverd, wat was het antwoord van de ontvangende server, had de ontvanger toegang tot het bericht en met welke authenticatie.
62.	Met betrekking tot de beveiliging van de data is minimaal geborgd: • Invoervalidatie, • Controle op mutatie tijdens transport, ~~Gegevens worden niet buiten de bron opgeslagen en niet buiten de bron gewijzigd.~~
63.	De Opdrachtgever is gerechtigd zelf of door een onafhankelijke auditor onderzoek te (laten) doen naar de naleving van plichten uit de overeenkomst.
64.	Er worden binnen de oplossing geen wachtwoorden opgeslagen. Authenticatie vindt buiten de oplossing plaats met behulp van de Identity Provider van de Opdrachtgever.
Eisen Security	
Beschikbaarheid	
65.	De Leverancier heeft een wijzigings- en acceptatieproces. Hierin borgt de Leverancier ten minste dat: • De Opdrachtgever wordt geïnformeerd over wijzigingen die betrekking hebben op de dienst of organisatie van de dienst of organisatie zelf die invloed heeft op de geleverde dienst • De acceptatie wordt hierbij uitgevoerd door de Opdrachtgever.
66.	De oplossing ondersteunt het maken en herstellen van back-ups van alle relevante gegevens binnen de veilige mailoplossing. De Leverancier verzorgt deze functionaliteit of

	stelt de Opdrachtgever in staat deze uit te voeren met de door de Opdrachtgever gebruikte back-upoplossing: • De Leverancier maakt dagelijks een online back-up van de data. • De gegarandeerde RTO is 16 werkuren (2 werkdagen) • De gegarandeerde RPO is maximaal 28 uur. • De Leverancier bewaart backups minimaal 180 dagen • De Leverancier test disaster recovery minimaal eenmaal per jaar. • De Leverancier doet de Opdrachtgever verslag van disaster recoverytest.

Eisen Security	
Integriteit & Vertrouwelijkheid	
67.	Onderliggende software componenten, zoals operating systemen, database software, browser versie, programmeer framework, waarop de software is gebouwd en draait, dienen altijd een door de oorspronkelijke Leverancier van de betreffende software of framework ondersteunde versie te zijn. Bijvoorbeeld: als Microsoft Windows gebruikt wordt is dit op basis van een nog door Microsoft ondersteunde versie.
68.	De Leverancier beschikt over een formeel patch- en kwetsbaarhedenbeheerproces. Beveiligingsupdates en patches voor de onderliggende software worden tijdig geïmplementeerd op basis van de ernst van de kwetsbaarheid en het bijbehorende risico.
69.	Het is de Leverancier niet toegestaan, zonder voorafgaande uitdrukkelijke schriftelijke toestemming van de Opdrachtgever, de uitvoering van een overeenkomst geheel of gedeeltelijk aan derden over te dragen of uit te besteden.
70.	De Leverancier is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De Leverancier waarborgt hierbij tevens ook met scheiding van taken onbedoelde of ongeautoriseerde toegang. De Opdrachtgever heeft het recht hierop te controleren.
71.	De Leverancier is verantwoordelijk voor de kwalificaties en screening van het eigen personeel. Op verzoek van Opdrachtgever dient een VOG te worden overlegd, van personen die worden ingezet op de opdracht.
72.	Alle voorwaarden en eisen die gelden voor personeel van de Leverancier zijn ook van toepassing op derden, die in opdracht van de Leverancier diensten verrichten voor de Opdrachtgever
73.	Er zijn geen "algemene" accounts/ gebruikers binnen de software. Als deze noodzakelijk zijn, betreft het een beperkt aantal en met specifieke doelen. De Leverancier dient hierin inzicht te geven.
74.	Bij interne of externe applicatiekoppelingen biedt de applicatie voldoende waarborgen tussen componenten zodat er geen verlies van berichten optreedt (bijvoorbeeld buffering van berichten) en dat de validiteit van berichten beschermd is (uitsluiting van oa spoofing, MITM).

Eisen levering	
75.	Het systeem moet zonder voorafgaande training te bedienen zijn voor zowel verzenders als (externe) ontvangers.

Eisen Beheer	
76.	Het product dient multi-tenancy te ondersteunen waarbij centraal beheer van alle tenants mogelijk is met een enkel beheeraccount.
77.	De Opdrachtgever moet zelfstandig beleidsinstellingen, authenticatie-instellingen, bewaartermijnen, classificatieregels en rapportages kunnen beheren zonder tussenkomst van de Leverancier.
78.	Het onderhoud van de oplossing moet niet de standaard-bedrijfsvoering hinderen of het gebruik van de oplossing limiteren. Dit geldt zowel voor onderhoud aan de oplossing als aan eventuele hardware, backups, accountmanagement etc.
79.	Per partnerorganisatie moeten afzonderlijke instellingen kunnen worden ingericht voor: • Verificatiemethoden; • Beveiligingsniveaus; • Bewaartermijnen; • Huisstijl; • Domeinregels; • Gebruikersgroepen.
80.	Delegatie van beheer: Het moet mogelijk zijn beheerrechten per partnerorganisatie te delegeren zonder toegang te geven tot gegevens of instellingen van andere partners.
81.	Systeem moet automatisch nieuwe gebruikers beschikbaar worden gesteld en vertrokken medewerkers moeten automatisch toegang verliezen.