

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier
	I.g.v. uit-huis-oplossing d.w.z. buiten het gemeentelijk ICT netwerk, dient de oplossing / systeemleverancier te voldoen aan de volgende SaaS-voorwaarden.	
a	De applicatie is een webapplicatie of webservice die werkt onder de in deze TA ondersteunde browsers en hoger met standaard beveiligingsinstellingen. De interface is zonder beperking van functionaliteit, benaderbaar zonder gebruik te maken van browser plug-ins of andere methodieken/software.	
b	Interfaces voor inwoners en bedrijven van de ICT-oplossing voldoen aan de eisen vermeld op www.digitoegankelijk.nl .	
c	De applicatie voldoet aan de beveiligingsrichtlijnen voor webapplicaties van het NCSC, is versleuteld met protocollen en algoritmen volgens de laatste stand van de techniek en moet voldoen aan de pas-toe-of-leg-uit lijst (PTOLU) van het Forum Standaardisatie (o.a. https:// , DNSSEC, IPv6 etc.)	
d	Het gebruik van TLS en HTTP headers voldoet aan de laatste stand van de techniek. De vereiste maatregelen op dit punt zijn uitgewerkt in het document: "Gebruik van TLS en HTTP response headers" (zie bijlage) Daarin de eis om bij onderstaande test-tools de SaaS applicatie een A+ te scoren: https://www.ssllabs.com/ssltest/index.html https://securityheaders.io/ En de eis om 100% te scoren op de testtool: https://internet.nl Wat is de URL van de Saas applicatie? Wat zijn de scores op de drie test-tools? Indien niet volledig goed, wanneer worden de bevindingen aangepakt om wel tot volledig juiste score te komen?	
e	Webapplicaties maken bij voorkeur gebruik van een koppeling met Single Sign On (SSO) met AzureAD/Entra ID als de Identity Provider . De SaaS-leverancier mag hierbij gebruik maken van SAML 2.0 of Open-id connect (OAuth 2.0). We gaan uit van minimale set aan gegevens en attributen: voor-	

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier
	en achternaam en email. De SSO-koppeling is bedoeld voor authenticatie, autorisatie dient plaats te vinden binnen de gekoppelde applicatie. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access. Als SSO via Azure AD/Entra ID niet mogelijk is, is het mogelijk om de toegang tot de applicatie te beperken tot het IP-adres van het vaste netwerk van de gemeente (dit is niet mogelijk voor mobiele apps), <i>of</i> gebruik te maken van 2-factor authenticatie. Onder bepaalde voorwaarden kan System for Cross-Domain Identity Management (SCIM) worden gebruikt voor het synchroniseren van gebruikers met de applicatie. De gegevens die via SCIM vanuit Entra ID worden gesynchroniseerd, hebben betrekking op medewerkers en niet op groepen. Dit voorkomt dat Entra ID als autorisatiebron binnen de applicatie fungeert, wat niet is toegestaan. De gekoppelde applicatie kan gebruikmaken van de reeds beschikbare gegevens in AD/Entra ID zonder extra toevoegingen van velden of verplichte veldwaarden die momenteel niet zijn ingevuld. Bovendien vereist de gekoppelde applicatie geen beheerrechten binnen AD/Entra ID voor medewerkers buiten de ICT-afdeling	

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier	
f	Indien er sprake is van de verwerking van persoonsgegevens dient applicatie een verwerkersovereenkomst te worden afgesloten.		
g	Bij verwerking van bijzondere en/of gevoelige persoonsgegevens levert de SaaS-Leverancier jaarlijks een SOC II Type II verklaring en/of een Third Party Memorandum (TPM) op basis van een andere erkende norm op het gebied van informatieveiligheid. De betreffende verklaring dient expliciet assurance te geven over de effectieve werking van de beheersmaatregelen (operating effectiveness) gedurende de beoordeelde periode.		
h	Wanneer de SAAS applicatie een financieel proces verwerkt dat bijv. voor de jaarrekening van materieel belang kan zijn levert de SAAS leverancier jaarlijks een ISAE 3402 Type II verklaring.		
i	De SaaS-Leverancier en de hostende partij beschikken over een ISO27001-certificering. Waarbij de verklaring van toepasbaarheid dient te worden aangeleverd.		

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier	
j	De data moet zijn opgeslagen binnen de Europese Economische Ruimte. Tevens is de vestigingsplaats van de inschrijver binnen de Europese Economische Ruimte.		
k	De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA: • een autorisatieproces voor toegang en rechten van gebruikers en beheerders van de applicatie; • de verplichting tot het bijhouden van een lijst van geautoriseerde personen tot het gebruik van een dienst en hun rechten en privileges ten aanzien van een dergelijk gebruik; • beperkingen ten aanzien van het kopiëren en openbaar maken van informatie; • verantwoordelijkheden ten aanzien van installatie en onderhoud van hardware en software; • het beoogde niveau van de service (responsetijden, beschikbaarheid), evenals onaanvaardbare serviceniveaus; • het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren; • het vaststellen van een escalatieproces voor het oplossen van problemen;		
l	Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde "audit logs", die tenminste het volgende bevatten: • gebruikers-ID's; • data en tijdstippen van aanloggen en afmelden; • overzichten van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem; • overzichten van geslaagde en geweigerde en andere pogingen om toegang te krijgen tot individuele onderdelen van het systeem en bestanden; • overzichten van raadplegingen en mutaties inclusief gebruikers-ID's, data en tijdstippen in geval van verwerking van persoonsgegevens en of vertrouwelijke gegevens; • De audit logs zijn beschermd zodat ze niet aangepast of gemanipuleerd kunnen worden; • De audit logs zijn 24/7 raadpleegbaar en exporteerbaar (en een gangbaar bestandsformat) voor geautoriseerde medewerkers van de gemeente 's-Hertogenbosch.		

A	Algemene voorwaarden SAAS applicaties en websites	Toelichting leverancier	
m	SaaS-applicaties en -websites welke gebruikmaken van domeinen die eigendom zijn van de gemeente dienen te voldoen aan de volgende uitgangspunten: ☐ Productie SaaS-applicaties en -websites tebedenkennaam.gemeentelijkdomein.tld ☐ Acceptatie SaaS-applicaties en -websites tebedenkennaam.accp.gemeentelijkdomein.tld ☐ De domeinnamen dienen vervolgens gekoppeld te worden op basis van het IP-adres aan een A- en AAAA-record. ☐ Het gebruik van CNAME-records voor het verwijzen naar diensten is niet toegestaan.		
Extra	Het eigenaarschap van de data in het systeem ligt bij de gemeente 's-Hertogenbosch en wordt (kosteloos) bij beëindiging SaaS looptijd in een door de Gemeente 's-Hertogenbosch voorgeschreven formaat beschikbaar gesteld.		

B	Eis t.a.v. koppelingen	Toelichting leverancier	
	Indien het noodzakelijk is dat de SAAS oplossing wordt gekoppeld aan ander systeem, gelden hierbij de volgende uitgangspunten:		
a	Koppelingen met een externe applicatie met een intern systeem van Gemeente 's-Hertogenbosch kunnen zowel synchroon als asynchroon plaatsvinden. Gezien de complexiteit geldt dat nieuwe ontwerpen van koppelingen altijd van een intakeprocedure lopen. Voor transportbeveiliging en vaststelling van identiteit over onvertrouwde netwerken wordt altijd, ongeacht het vertrouwelijkheidsniveau van de informatie, gebruik gemaakt van PKI. Bij informatieverwerkingen van persoonsgegevens en of gegevens met een vertrouwelijkheidsniveau van 'vertrouwelijk' of hoger, moeten mogelijk aanvullende maatregelen worden genomen. Deze afweging wordt gemaakt op de basis van de resultaten van dataclassificatie en risicoanalyse.		
b	Asynchrone koppelingen tussen een intern systeem en een externe applicatie worden ondersteund op onderstaande wijzen: - Vanuit de applicatie kunnen gegevens worden gepusht naar onze omgeving. Hierbij wordt gebruik gemaakt van ebMS XML of		

B	Eis t.a.v. koppelingen	Toelichting leverancier	
	webservice berichtenverkeer wat in een interne queue wordt gezet voor onze broker. - Vanuit een applicatie in het interne netwerk van Gemeente 's-Hertogenbosch wordt periodiek gecontroleerd op de gegevens in de applicatie. Dit gaat altijd via een veilige verbinding. Voor https koppelingen gebruiken we de Service Gateway. Voor sftp, ftps etc. gebruiken we GoAnywhere. - Gegevens worden aangeboden aan een interne applicatie door middel van een webformulier en de broker. Systeemtechnische koppelingen, zoals bijvoorbeeld automatische updates, kunnen via de webproxy of de loadbalancer lopen.		
c	Bij synchrone koppelingen wordt gebruik gemaakt van webservices om informatie tussen systemen uit te wisselen. Via een webservice aanroep wordt de benodigde informatie opgevraagd en direct teruggeleverd. De koppelingen met applicaties via webservices lopen via een Service Gateway.		
d	Voor applicaties kan indien nodig een DigiD koppeling worden aangevraagd. De applicatie dient hiervoor te voldoen aan de eisen uit de DigiD checklist testen van Logius en het Beveiligingsassessment DigiD. Voor het Beveiligingsassessment DigiD dient jaarlijks een TPM worden afgegeven door de SAAS-leverancier.		

C	Eis t.a.v. mailen vanuit externe applicaties	Toelichting leverancier	
	Het beleid van de gemeente staat niet toe dat e-mail voor domeinen die gebruikt worden door de organisatie zelf wordt verstuurd via e-mail-servers van derden. Mail kan worden verzonden via de volgende mogelijkheden:		
1	E-mail versturen via externe, niet in beheer van de gemeente zijnde mailservers, met zelf aan te vragen domeinen (al bij de gemeente horende domeinen zoals @s-hertogenbosch.nl kunnen dus niet worden gebruikt). De oplossing moet voldoen aan het gemeentelijke beveiligingsbeleid en moet gebruik maken van de relevante technieken zoals op de pas-toe-of-leg-uit lijst (PTOLU) 4 staan vermeld (SPF, DKIM, DMARC, STARTTLS+DANE).		

C	Eis t.a.v. mailen vanuit externe applicaties	Toelichting leverancier	
2	E-mail versturen via de gemeentelijke mailservers met al door de gemeente in gebruik zijnde domeinen: De gemeente biedt toegang tot een service-/API-gateway door een service, of services, te publiceren waar de leverancier gebruik van kan maken. Deze services zijn beveiligd met Mutual TLS (MTLS) en IP-restricties. De service om de mail te versturen ondersteunt een aantal Microsoft Graph-operaties. Daarbinnen zijn er de volgende mogelijkheden: A. In de afhandeling van het bericht zal de service-/API-gateway een token ophalen bij Microsoft 365. Dit token wordt aan het bericht van de aanroepende partij toegevoegd en verstuurd naar Microsoft Graph. Hierbij wordt dus gebruik gemaakt van één service, één endpoint. B. Óf er zijn twee endpoints beschikbaar: - o een service/endpoint voor de tokenaanvraag bij microsoftonline - o een service/endpoint voor de Microsoft Graph-operaties In het laatste geval zal de service-/API-gateway geen token toevoegen, maar verwacht het dat de aanroepende partij dit gedaan heeft; het is dus niet toegestaan om rechtstreeks met de Microsoft Graph API te verbinden namens de gemeente.		

Toetsing van een volledige en correcte implementatie van deze voorwaarden vindt vóór in gebruik name in overleg met de gemeentelijke security-officer plaats. Deze toets zal jaarlijks worden herhaald. In geval van SAAS applicaties blijft de leverancier te allen tijden verantwoordelijk voor de goede en veilige werking inclusief compliancy van de complete oplossing.