Gemeente Utrecht

Deze aansluitvoorwaarden zijn van toepassing op alle typen SaaS applicaties.

Algemene eisen en wensen

Nr.	Eis / Wens	Omschrijving	Waarom?	Invulling
1	Eis	De verbinding met de SaaS webapplicatie is beveiligd.	Borgen van vertrouwelijkheid en integriteit.	Gebruik https over TLS. http is niet toegestaan. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC, waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden. Minimaal TLS1.3 en IPv 6 on default configureerbaar.
2	Eis	De URL SaaS applicatie dient te kunnen benaderd middels de Fully Qualified Domain Name.	Borgen van integriteit.	Voorbeeld: wel https://applicatie.domeinnaam.nl of niet https://applicatie.nl
3	Eis	Het gebruik van remote display en/of digitale workspace software om een externe applicatie te benaderen is niet toegestaan.	Borgen vertrouwelijkheid, integriteit en beheer (zero footprint).	Remote desktop uitschakelen, applicatie niet aanbieden via digitale workspace software zoals bijv. Citrix/horizon view etc. (PCOIP), ICA en RGS.
4	Eis	De SaaS applicatie is vanuit elke mogelijke locatie via het internet benaderbaar.	In het kader van flexibiliteit van levering via welk medium dan ook, zonder gebonden te zijn aan type medium (bijv. niet gebonden aan werkplek).	De applicatie kan ook buiten Utrechtse werkplek gebruikt worden.
5	Eis	De SAAS applicatie maakt geen gebruik van plug-in componenten.	Borgen van interoperabiliteit en beheer van de beheerde werkplek	Geen gebruik maken van o.a. Microsoft Active X, Microsoft Silverlight, Microsoft ClickOnce, Adobe Flash en Java plug-in.

Nr.	Eis / Wens	Omschrijving	Waarom?	Invulling
			infrastructuur van de gemeente Utrecht.	
6	Eis	Voor het functioneren van de SAAS applicatie op het client device en/of in de webbrowser zijn geen verdere instellingen en/of installaties op het client device en/of in de browser benodigd.	Borgen van interoperabiliteit en beheer van de beheerde werkplek infrastructuur van de gemeente Utrecht.	Voor het gebruik van de applicatie hoeft geen software geïnstalleerd te worden, geen aanpassingen aan de browser instellingen, de applicatie maakt geen gebruik van extensies op de browser.
7	Eis	Het gebruik van voorzieningen voor opslag en bestandsuitwisseling in ‘de cloud’ kan geconfigureerd worden.	Waarborgen integriteit en vertrouwelijkheid	Met opslag en bestandsuitwisseling worden diensten als Dropbox, OneDrive, Google Drive, iCloud, WeTransfer, SendAnywhere etc. bedoeld. Met ‘geconfigureerd’ wordt bedoelt: 1. Het gebruik van deze diensten kan in- of uitgeschakeld worden en 2. De dienst ingesteld kan worden. Voorbeeld: in de applicatie kan ingesteld worden dat applicatie OneDrive voor bestandsuitwisseling gebruikt.
8	Wens	De beschikbaarheid van SaaS applicaties kan door de gemeente Utrecht gemonitord worden.	Borgen van continuïteit	De constructie van de SaaS applicatie dient toe te laten dat de applicatie door de gemeente Utrecht gemonitord wordt.
9	Wens	De database van de SaaS applicatie beschikt over de optie om gegevens versleuteld op te slaan.	Waarborgen van vertrouwelijkheid.	Versleuteling is onderdeel van het database management systeem dat door de SaaS applicatie gebruikt wordt.

Gemeente Utrecht

Eisen en wensen m.b.t. Koppelingen

De eisen en wensen zijn van toepassing op SaaS applicatie die koppelingen hebben met andere applicaties.

Nr.	Eis / Wens	Omschrijving	Waarom?	Invulling
10	Eis	De verbinding voor koppelingen tussen de SaaS applicatie en andere applicaties of systemen (zowel voor applicaties in het datacenter van de gemeente Utrecht als koppelingen met andere SaaS applicaties) moet ‘end to end’ beveiligd te worden d.m.v. encryptie.	Borgen vertrouwelijkheid en integriteit.	Https moet voldoen aan HTTP over een met TLS beveiligde verbinding. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC, waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden. Minimaal TLS1.3 en IPv 6 on default configureerbaar.
11	Eis	Bij het opzetten van de verbinding wordt de identiteit van de client en server vastgesteld en gecontroleerd.	Borgen vertrouwelijkheid en integriteit.	Hierbij wordt gebruik gemaakt van tweezijdige TLS, waarbij zowel client als server zich identificeren met een certificaat. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC, waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden.
12	Eis	Bestandsoverdracht is beveiligd.	Waarborgen integriteit en vertrouwelijkheid	Er dient minimaal gebruik te worden gemaakt van SFTP met een SSH Key.
13	Eis	Koppelingen van de SaaS applicatie met bij de gemeente Utrecht gehoste applicaties, die gebruik maken van XML en transformatie, verlopen via de ESB van de gemeente Utrecht.	Omwille van Interoperabiliteit	Aansluiten via de Utrechtse Enterprise Service Bus (ESB).
14	Eis	Koppelingen van de SaaS applicatie met applicaties buiten de infrastructuur van de gemeente Utrecht (zoals andere SaaS applicaties of landelijke voorzieningen) verlopen	Verminderen complexiteit beheer alsmede efficiëntie.	Koppelingen verlopen direct van de SaaS applicatie met de voorziening of SaaS applicatie en dus niet via de infrastructuur van de gemeente Utrecht.

		direct van de SaaS applicatie met de voorziening of SaaS applicatie.		De leverancier en de gemeente maken gezamenlijk afspraken met de beheerder van de voorziening of SaaS applicatie.
15	Eis	Als de SaaS applicatie koppelingen heeft met landelijke voorzieningen (bijv. een basisregistratie) en/of SaaS applicaties die door de gemeente Utrecht gebruikt worden, dan identificeren de SaaS applicaties zich namens de gemeente Utrecht.	Borgen traceerbaarheid	De leverancier en de gemeente maken gezamenlijk afspraken met de beheerder van de voorziening of SaaS applicatie.
16	Eis	Koppelingen van SaaS applicaties naar applicaties die gehost worden in het datacenter van de gemeente Utrecht verlopen altijd via DMZ van de gemeente Utrecht.	Borgen vertrouwelijkheid en integratie, alsmede borgen stabiliteit platformen	De constructie van de applicatie dient hiertoe niet belemmerend te zijn.

Eisen en wensen aan data, toegang, back-up en recovery, algoritmes, hosting

Nr.	Eis / Wens	Omschrijving	Waarom?	Invulling
17	Eis	Gemeente Utrecht data die in de SaaS applicatie wordt ingevoerd cq gegenereerd blijft altijd eigendom van de gemeente Utrecht en verstrekking aan derden kan alleen plaatsvinden met schriftelijke toestemming van de gemeente Utrecht	Gemeente Utrecht is eigenaar van de gegenereerde data. De SaaS applicatie wordt als een service afgenomen en is van de leverancier.	Opnemen in een verwerkersovereenkomst
18	Eis	Een verwerkersovereenkomst is van toepassing op SaaS applicaties vanwege het gebruik van	Namen van medewerkers van de gemeente Utrecht valt ook onder	Opnemen in een verwerkersovereenkomst en register van verwerkingen.

		persoonsgegevens in de zin van de AVG en UAVG en in het kader van dataclassificatie gebaseerd op de BIV(Betrouwbaarheid, Integriteit, Vertrouwelijkheid)	persoonsgegevens. Verwerkingen van persoonsgegevens worden opgenomen in het register van verwerkingen van de gemeente Utrecht en in een verwerkersovereen komst.	
19	Eis	De SaaS applicatie beschikt over Multi Factor Authenticatie	Extra beveiligingslaag via authenticator token/app	Op welke manier kan MFA worden ingezet voor de SaaS applicatie
20	Eis	De SaaS applicatie beschikt over Federation Services/koppelen aan Active Directory gemeente Utrecht	Identity Acces Management kan worden toegepast en maakt het voor de medewerker van de gemeente Utrecht makkelijker om in te loggen met de juiste beveiliging.	Met de voorziening IAM van de gemeente Utrecht afstemmen
21	Eis	De SaaS applicatie beschikt over minimaal het volgende wachtwoord policy	Extra beveiliging op wachtwoord d.m.v. onleesbaar maken van opslag van wachtwoorden in de database.	

		Database encryptie op persoonlijke gegevens Wachtwoord Alleen instelbaar door gebruiker Wachtwoord – hashing Wachtwoord - sterkte afdwingen \Wachtwoord – verloop Two Factor Authentication	Sterkte afdwingen van het wachtwoord en periodiek nieuw wachtwoord afdwingen.	
22	Eis	De leverancier beschikt over een back-up en recovery policy van de SaaS applicatie waarin de back-up gescheiden is van de productieomgeving	Vanwege ransomware aanvallen is een fysiek gescheiden backup nodig voor de data weerbaarheid van het bedrijfsproces.	Aanleveren van een back-up en recovery policy document
23	Eis	De leverancier is verplicht om beveiliginsincidenten/lekken en data lekken direct te melden aan de gemeente Utrecht	Procedure van de gemeente Utrecht wordt gevolgd	○ Product - Beveiligingslek of datalek melden - Online loket (utrecht.nl)
24	Eis	Een verwerkersovereenkomst is van toepassing op SaaS	Verwerking van data d.m.v. algoritmes wordt opgenomen in een	○ Benoemen algoritme voor geautomatiseerde beslissingen, toelichting waarvoor/doeleinden, openbare of gesloten algoritmes. ○ Wat is de rol van het algoritme of voorspellend model binnen het proces?

		applicaties die gebruik maken van algoritmes.	verwerkingsovereenkomst en in het register van verwerkingen van de gemeente Utrecht	○ Geeft het algoritme of voorspellend model informatie of neemt het zelfstandig een besluit? ○ Welke data wordt gebruikt voor het algoritme is hier sprake van labeled of unlabeled data toepassing.
25	Eis	De SaaS applicatie is zo geconfigureerd bij het opstarten dat alleen noodzakelijke/functionele cookies default worden aangezet voor de performance van de applicatie	Geen profilering van gebruikers van de SaaS applicatie d.m.v. analyse en overige cookies	Een testlink van de SaaS applicatie wordt verstrekt ter verificatie bij voorlopige gunning
26	Eis	De SaaS applicatie wordt gehost op servers in een datacenter in Nederland of binnen de europese unie waar de AVG/GDPR van toepassing is.	Bij voorkeur in Nederland gehost	In een document van de leverancier waar de producten en diensten zijn benoemd is de locatie(Nederland of…) van het datacenter van de hosting van de SaaS applicatie opgenomen en wordt aangegeven dat op de locatie AVG/GDPR wetgeving van toepassing is.