# Richtlijnen voor Web/Saas applicaties gemeente Zaanstad

*Richtlijnen voor technische en organisatorische beheersmaatregelen bij Web/SaaS-oplossingen*

# Versiebeheer

## Versies

| Versie | Datum | Auteur | Samenvatting van de wijzigingen |
|---|---|---|---|
| 1.0 | | M. Kortzorg | |
| 1.1 | 26-2-2020 | M. Kortzorg | Aanpassingen i.v.m. BIO. |
| 1.2 | 07-01-2021 | M. Kortzorg | Toevoegen privacy en IB eisen |
| 1.3 | 28-10-2021 | M. Kortzorg | Nieuwe OWASP top 10 2021 toegevoegd. |
| 1.4 | 23-06-2022 | M. Kortzorg | Aanpassing SSO protocollen (T11) |

Gemeente Zaanstad

Maatregelen voor SaaS-leveranciers

**Wijzigingsprocedure**

Het document wordt door de afdeling IBT/IBPO beheerd. Het wordt minimaal eens per jaar geactualiseerd en wanneer nodig herzien. Na een herziening wordt de nieuwe versie opnieuw vastgesteld.

**Gerelateerde documenten**

| | |
|---|---|
| ■ ICT-Beveiligingsrichtlijnen voor webapplicaties | NCSC |
| ■ Baseline Informatiebeveiliging Overheden (BIO) | IBD |
| ■ Aansluitvoorwaarden ICT | Gemeente Zaanstad |

**Doel**

Dit document dient ter ondersteuning van de informatiebeveiliging van de gemeente Zaanstad. Het geeft richtlijnen die voor de informatiebeveiliging bij SaaS-oplossingen nodig zijn en stuurt hiermee de selectie van nieuwe SaaS-leveranciers.

**Doelgroep**

De richtlijnen kennen twee doelgroepen. Het is enerzijds geschreven voor de proceseigenaar bij de gemeente, in hoedanigheid van bijvoorbeeld de opdrachtgever, projectleider of product-owner. Anderzijds geeft de SaaS-leverancier, aan de hand van de richtlijnen in paragraaf 3.1 t/m 3.24, inzage in het beveiligingsniveau van de SaaS-oplossing. Deze tabellen dienen door de SaaS-leverancier ingevuld te worden.

# Inhoud

# 1 Informatiebeveiligingseisen SaaS-systemen

## 1.1 Wat is SaaS

SaaS, oftewel Software As A Service, heeft betrekking op software die als online dienst wordt aangeboden. Er wordt ook van webservices of web-based api's gesproken. De SaaS-leverancier is eigenaar van de software en biedt dit in licentievorm aan met een daarbij behorend dienstniveau en beheer.

Het Informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten, vanaf 01-01-2020 de Baseline Informatiebeveiliging Overheid, en wordt gebruikt als basis voor de beoordeling van processen en informatiesystemen op aanwezige risico's. Dit document geeft invulling aan zowel de technische als organisatorische beheersmaatregelen die voor alle SaaS-systemen geldt.

### 1.1.1 Waarom een specifieke set maatregelen voor SaaS-systemen?

SaaS-systemen worden in regel afgenomen van leveranciers die van buiten het gecontroleerde netwerk van de gemeente opereren en van daaruit hun diensten aanbieden. Een dergelijke oplossing biedt zowel kansen als risico's.

De uitbesteding via SaaS-oplossingen ontslaat de gemeente zich niet van haar verantwoordelijkheid om zorgvuldig met (gevoelige) gegevens om te gaan die zij in bezit heeft. Wanneer de gemeente besluit een dienstverlening via een SaaS-oplossing uit te besteden, is het van belang om inzicht te krijgen in het beveiligingsniveau dat van toepassing is bij de leverancier. Dat leidt tot een bewustere omgang met risico's, kennis van genomen maatregelen en in sommige gevallen de nog te treffen maatregelen.

Deze richtlijnen zijn opgesteld om de risico's van SaaS-systemen voor de gemeente zodanig te verminderen dat eventuele rest-risico's acceptabel blijven.

# 2 Maatregelen

Om de eerder genoemde risico's van SaaS-systemen te kunnen verminderen volgt de gemeente de volgende bestaande kaders voor SaaS-systemen:

- De maatregelen uit ICT Beveiligingsrichtlijnen voor webapplicaties (NCSC)
- De maatregelen die de ICT-Infra organisatie stelt en voor SaaS-oplossingen van belang zijn. Het gaat hier vooral om de technische implementatie.

Bovendien staat bewustwording op het gebied van informatiebeveiliging ook bij een SaaS-oplossing centraal. Verschillende normeringen die voor de gemeente van toepassing zijn, verplichten een organisatie om beveiliging doorlopend aandacht te geven. Bewustwording wordt daarom ook in dit document opgenomen.

## 2.1 Informatiebeveiligingskader voor SaaS-systemen

Net als alle andere gemeenten hanteert de gemeente Zaanstad de Baseline Informatiebeveiliging Overheid als kader voor diens Informatiebeveiliging.
De genoemde maatregelen zijn overeenkomstig aan het Basis Beveiligings Niveau (BBN) 2. Dit niveau wordt als standaard baseline gehanteerd voor overheidssystemen.

Om de set aan beveiligingsmaatregelen begrijpelijk en toepasbaar te maken, is de keuze gemaakt om een selectie te maken uit de richtlijn "ICT-beveiligingsrichtlijnen voor webapplicaties " van het Nationaal Cyber Security Centrum (NCSC). Deze norm is vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Rijks auditdienst en NCSC. De beveiligingsrichtlijnen van NCSC zijn breed toepasbaar voor ICT- oplossingen die gebruikmaken van webapplicaties zoals ook SaaS-oplossingen.

Het Informatiebeveiligingskader voor SaaS-systemen geeft aandacht aan de eerder genoemde risico's die zich bij SaaS-oplossingen kunnen voordoen.
Dit Informatiebeveiligingskader is van toepassing voor SaaS-systemen die in de Baselinetoets BIO tot en met BIV rating 1-2-2 (BIO BBN 2) scoren. Wanneer er een hogere BIV rating gescoord wordt, dienen aanvullende maatregelen genomen te worden of er moet een uitgebreide analyse worden uitgevoerd.

## 2.2 Maatregelen bij ICT

Bij interne systemen van de gemeente behoort een deel van de technische beveiligingsmaatregelen tot het uitvoeringsgebied van ICT. Het moet helder zijn welke

maatregelen bij ICT van toepassing zijn, zowel in generieke zin als eventueel per beveiligingsniveau.

Voor SaaS-systemen geldt dat de SaaS-leverancier zelf verantwoordelijk is voor de te nemen beveiligings- en continuïteitsmaatregelen. Bij SaaS-diensten is er vaak minder ruimte om specifieke maatregelen op procesniveau te treffen omdat de dienst niet bij de gemeente in beheer is. Dit betekent dat er op voorhand gekeken moet worden of de SaaS-dienstverlening een voldoende beveiligingsniveau biedt.

In specifieke gevallen zal er Service Level Agreement (SLA / DAP) opgesteld kunnen worden. Hierin komen ook afspraken in terug die van invloed zijn op de informatiebeveiliging, zoals de beschikbaarheid, rapportages, backup & restorepolicy en uitwijkmogelijkheden. Vaker zal de SaaS-leverancier echter een Service Level Commitment aanbieden en zullen er geen specifieke SLA afspraken gemaakt kunnen worden. De gemeente weegt dan bij de voorselectie van de SaaS-leverancier af of deze maatregelen bij de SaaS-leverancier voldoende geborgd worden.

## 2.3 Bewustwording en kwetsbaarhedentest

De gemeente verwacht van SaaS-leveranciers een actuele kennis op het gebied van risico's, kwetsbaarheden en security. Voor SaaS-applicaties kan de OWASP Top Ten (2017) als startpunt voor bewustwording dienen. Voorts zijn er verschillende alternatieven op het gebied van bewustwording, waaronder het NCSC of het NIST.

Elke SaaS oplossing, die door de gemeente wordt afgenomen, dient minimaal (maar niet uitsluitend) te worden getest op de meest voorkomende kwetsbaarheden uit de OWASP Top Ten 2021waarmee aangetoond kan worden dat deze kwetsbaarheden bij de productie versie niet meer aanwezig zijn;

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server Side Request Forgery (SSRF)

# 3 Informatiebeveiligingskader SaaS

De onderstaande tabellen  worden door de leverancier ingevuld en waar nodig van uitleg voorzien.

## 3.1 Beleidsdomein

| Code NCSC | Maatregel | Aanwezig Ja/Nee/NVT | Uitleg indien niet aanwezig of NVT |
|---|---|---|---|
| B.05[1] | In een contract met een derde partij voor de uitbestede levering of beheer van een (web)applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juist (organisatorische) niveau vastgesteld. | | |
| U/TV.01 | De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. | | |
| U/TV.01 | Wachtwoorden worden gebruikt op basis van de geldende beveiligingseisen  uit de BIO[2] en worden eenrichting-versleuteld (hash en salt) opgeslagen. | | |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. | | |
| U/WA.03 | De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. | | |
| U/WA.04 | De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren. | | |
| U/WA.05 | De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en crypto grafische technieken. | | |
| U/WA.05 | Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en communicatie. | | |
| U/PW.02 | De webserver garandeert specifieke kenmerken van de inhoud van de protocollen. | | |
| U/PW.03 | De webserver is ingericht volgens een configuratie-baseline (zie 3.2 uitvoerend domein) | | |
| U/PW.05 | Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen. | | |
| U/NW.04 | De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen. | | |

[1] B.05 wordt door de gemeente Zaanstad ingevuld. De overige items worden door SaaS-leverancier ingevuld.
2 Zie BIO maatregel 9.4.3.1

| | | | |
|---|---|---|---|
| U/NW.05 | Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd. | | |
| U/NW.06 | Voor het configureren van netwerken hanteert de leverancier een vastgestelde hardenings richtlijn. | | |
| C.02 | Leverancier is ISO27001 gecertificeerd.. De werking van de certificering en het gevolgde beveiligingsniveau wordt aangetoond d.m.v. een Assurance verklaring van een onafhankelijke Norea auditor in de vorm van een SOC 1 of SOC 2 Assurance rapportage (ISAE 3402 of 3000) (afhankelijk van de invloed op de financiële jaarrekening van de gemeente).<br>Tevens levert de leverancier een conformiteitsverklaring aan waarin de gecertificeerde normen staan vernoemd (ANNEX A ISO27001) | | |
| C.03 | Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op alle ICT componenten van de webapplicatie (scope) conform de web richtlijnen van het NCSC en de OWASP top tien normering | | |
| C.04 | Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). Specifiek: een penetratietest is uitgevoerd bij ingebruikname, door onafhankelijke auditor die is aangesloten bij Norea j. Alternatief is het kunnen overhandigen van een TPM van maximaal 1 jaar. | | |
| C.06 | In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht. | | |
| C.07 | De logging- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd. De logs worden in exporteerbaar formaat aan de gemeente ter beschikking gesteld op verzoek. | | |
| C.08 | Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. | | |
| C.09 | Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen. | | |
| C.10 | Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest | | |

## 3.2 Privacy eisen (AVG)

| | | | |
|---|---|---|---|
| P1 | Persoonsgegevens worden uitsluitende verwerkt binnen de grenzen van de EER | | |
| P2 | Leverancier treft alle noodzakelijke maatregelen conform de AVG om de persoonsgegevens van de gemeente vertrouwelijk te houden | | |
| P3 | De leverancier heeft de mogelijkheid om productiedata (of een subset) te anonimiseren of pseudonimiseren. Het is mogelijk de geanonimiseerde data te kopiëren naar een andere omgeving. De geanonimiseerde data mag niet herleidbaar zijn tot een natuurlijk persoon. | | |
| P4 | De leverancier heeft een beschreven procedure voor de gegarandeerde vernietiging van productiegegevens uit de oplossing. | | |
| P5 | Productiedata mag niet gedeeld/gebruikt worden buiten de productie omgeving om. Dus in Acceptatie, Test en Ontwikkelomgeving mag alleen gepseudonimiseerde of geanonimiseerde data voorkomen waarvan geen enkel gegeven herleidbaar mag zijn naar een natuurlijk persoon. | | |
| P6 | Leverancier heeft een proces voor het melden van datalekken aan verwerkingsverantwoordelijke ingericht. | | |
| P7 | Toegang tot persoonsgegevens van de gemeente is door de leverancier afgeschermd door hetzij versleuteling of autorisaties. | | |

## 3.3 Informatiebeveiligingseisen

| | | | |
|---|---|---|---|
| IB 1 | Iedere gebruiker beschikt over een uniek login account | | |
| IB2 | Het gebruik van sterke wachtwoorden wordt door de oplossing afgedwongen | | |
| IB3 | De oplossing biedt een lock-out mogelijkheid van een, door de gemeente te bepalen tijdsframe, na minimaal 5 foutieve inlogpogingen. | | |
| IB4 | Alle inlogpogingen (inclusief mislukte) van gebruikers worden gelogd. Minimaal wordt in de log vastgelegd de accountnaam, de locatie, het tijdstip, en het resultaat van de inlogpoging | | |
| IB5 | Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. | | |
| IB6 | Wachtwoorden worden versleuteld opgeslagen op het device en niet in de oplossing. | | |
| IB7 | De geleverde oplossing biedt standaard two-factor authenticatie (2FA). | | |
| IB8 | De aangeboden 2FA oplossing moet minimaal Microsoft Azure AD of vergelijkbaar ondersteunen. | | |
| IB9 | De oplossing past encryptie toe op alle communicatie via netwerken | | |
| IB10 | De oplossing controleert tijdens het opzetten van een versleutelde verbinding of het servercertificaat vertrouwd is en neemt de nodige maatregelen bij afwijkingen. | | |
| IB11 | De applicatie is ontwikkeld conform de richtlijn Secure Software Development (https://www.cip-overheid.nl/media/1500/20200720-ssd-normen-v30.pdf) | | |

| | | | |
|---|---|---|---|
| IB12 | Leverancier toont periodiek aan, d.m.v. een SOC 2 ISAE 3000 type 2 verklaring, opgesteld door een onafhankelijke Norea auditor, dat de geleverde dienst(en) voldoen aan de ISO 27001 beveiligingseisen en de richtlijnen van het NCSC. | | |

## 3.4 Uitvoerend IT domein (technisch)

| **Maatregel nr.** | | Aanwezig Ja/Nee/NVT | Uitleg indien niet aanwezig of NVT |
|---|---|---|---|
| T.01 | Algemeen<br>Leverancier maakt gebruik van webservices of web-api's die hoofdzakelijk via het http applicatie-protocol versleuteld worden aangeboden. Non-http applicatie-protocollen niet toegestaan | | |
| T.02 | Versleuteling<br>Dataverkeer wordt versleuteld met PKI-certificaten, conform de richtlijnen van het NCSC (TLS 1.2 of hoger). Voor domeinnamen eindigend op zaanstad.nl worden PKI-Overheidscertificaten gebruikt. HTTPS verkeer verloopt over poort 443. | | |
| T.03 | Architectuur<br>De oplossing van de SaaS-leverancier is horizontaal en/of verticaal schaalbaar. Het systeem is in staat om schommelingen in gebruik, binnen de marges van de gebruiksvoorwaarden, adequaat op te vangen. | | |
| T.04 | Communicatie met gemeentelijke infrastructuur vindt alleen plaats via de daarvoor bestemde gateways en api-services. | | |
| T.05 | Output, exports, of gecreëerde bestanden worden via de front-end van de leverancier benaderbaar gemaakt. | | |
| T.06 | Data van de gemeente mag niet voor andere gebruikers beschikbaar komen. In geval van multi-tenancy oplossingen mogen api-services en netwerkservices shared zijn, maar data niet. De data blijft alleen per tenant toegankelijk.. | | |
| T.07 | Kantooromgeving;<br>Er is zowel bij leverancier als afnemer geen mogelijkheid voor het gebruik van files shares (o.a. WebDAV), ftp, remote access (RDP o.i.d.) | | |
| T.08 | Geleverde diensten zijn compatible met browsers waaronder Edge/Chrome en Firefox[3]. Specifieke cliënt-applicaties of plugins zijn niet noodzakelijk om de SaaS-diensten te kunnen afnemen (zero footprint) | | |
| T.09 | Indien SaaS-dienst output voor kantoortoepassingen levert, zijn deze compatible met Office 365 | | |
| T.10 | Toegangsbeveiliging<br>Burger authenticatie verloopt via DigiD, ketenauthenticatie via e-Herkenning EH-2 of EH-3 | | |
| T.11 | OpenID Connect-/OAUTH 2.0 wordt als SSO authenticatie- en delegatieprotocol gebruikt waarbij Azure AD ondersteuning onderdeel van de standaard is. Indien geen OpenID connect mogelijk is dan mag SAML 2.0 gehanteerd worden | | |
| T.12 | Netwerken<br>Leverancier heeft netwerksegmentatie geïmplementeerd waarbij omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden. Zoals bijvoorbeeld de kantoor-, acceptatie-, en productie omgevingen. | | |

[3] Huidige versie en vorige versie (n-1).