GGD BRANDWEER
Veiligheidsregio Kennemerland

Beleid t.a.v. SaaS en webapplicaties Veiligheidsregio Kennemerland

Kerngegevens

Documenteigenaar:	I&A
Documentbeheerder:	I&A
Tegen-gelezen door:	CISO
Datum:	Januari 2024
Versie:	1.0
Status:	Goedgekeurd door Directie VRK jan. 2024
Excerpt:	Dit document bevat de VRK-beleid vanuit informatiebeveiliging en privacy voor SaaS en webapplicaties. Dit document kan gebruikt worden bij de verwerving van dit type applicatie. Tevens is dit beleid van toepassing bij vervanging of verlenging van bestaande SaaS toepassingen en webapplicaties bij de VRK

Wijzigingsprocedure

Het document wordt door de afdeling I&A beheerd en vastgesteld door de directie. 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

Doel

Dit document dient ter ondersteuning van de informatiebeveiliging van de Veiligheidsregio Kennemerland (hierna VRK). Het beschrijft het beleid dat voor de informatiebeveiliging bij SaaS-oplossingen en webapplicaties nodig is en stuurt hiermee de selectie van nieuwe SaaS-leveranciers.

Doelgroep

Dit beleid is enerzijds geschreven voor de proceseigenaren bij de VRK, in hoedanigheid van bijvoorbeeld de opdrachtgever, projectleider of product-owner. Anderzijds geeft dit beleid de SaaS-leverancier, inzage in het vereiste beveiligingsniveau van een SaaS-oplossing. De informatiebeveiligingskaders in hoofdstuk 3 bieden die mogelijkheid. Bij de selectie van een nieuwe SaaS leverancier zijn deze tabellen onderdeel van de eisen die aan een nieuwe SaaS leverancier gesteld worden. Deze tabellen dienen door de SaaS-leverancier te worden ingevuld voordat een overeenkomst tot stand komt.

Versieblad

Datum	Versie	Gemaakt door	Aanpassingen
01-10-2023	0.1	B. Hermus / E. Beukenkamp	1e concept
15-10-2023	0.2	B. Hermus	1e aanpassingsronde ICT-IM Board verwerkt
01-11-2023	0.3	B. Hermus / E. Beukenkamp	2e aanpassingsronde ICT-IM board verwerkt
05-12-2023	0.4	B. Hermus / E. Beukenkamp	Laatste aanpassingen verwerkt, document klaar gemaakt voor besluit DT
25-01-2024	0.9	E. Beukenkamp / B. Hermus	Toevoeging toepasselijkheid, hoofdstuk 1.3, aanpassing versieblad en voettekst, aanpassing titel
29-01-2024	1.0	---	Definitief, goedgekeurd door DT
07-05-2023	1.0	B. Hermus	In overleg met ICT-IM classificatie aangepast naar openbaar om dit document toe te kunnen voegen aan bv een aanbesteding.

.

Inhoud

1. Inleiding

1.1 Wat is SaaS

SaaS, oftewel Software as a Service, heeft betrekking op software die als onlinedienst wordt aangeboden. Er wordt ook van web services of webbased 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 VRK is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), 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 en webapplicaties geldt.

1.2 Waarom een specifieke set maatregelen voor SaaS-systemen?

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

De uitbesteding via SaaS-oplossingen ontslaat de VRK niet van haar verantwoordelijkheid om zorgvuldig met (gevoelige) gegevens om te gaan die zij in bezit heeft. Wanneer de VRK 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.

Dit beleid is opgesteld om de risico's van SaaS-systemen voor de VRK zodanig te verminderen dat eventuele rest-risico's acceptabel blijven en geaccepteerd kunnen worden.

1.3 Toepassing SaaS beleid VRK

Dit beleid is van toepassing op alle nieuw te verwerven SaaS toepassingen bij de VRK. Tevens is dit beleid van toepassing bij vervanging of verlenging van bestaande SaaS toepassingen bij de VRK.

2. Maatregelen

Om de eerdergenoemde risico's van SaaS-systemen te kunnen verminderen volgt de VRK 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 VRK van toepassing zijn, verplichten een organisatie om beveiliging doorlopend aandacht te geven. Bewustwording wordt daarom ook in dit document opgenomen.

Daarnaast worden ook maatregelen meegenomen in het kader van de AVG wetgeving.

2.1 Informatiebeveiligingskader voor SaaS-systemen

De VRK hanteert de Baseline Informatiebeveiliging Overheid (BIO) als kader voor diens Informatiebeveiliging en is gecertificeerd voor ISO27001 en NEN7510.

De genoemde maatregelen zijn compliant 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, Auditdienst Rijk (ARD) 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 eerdergenoemde 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 moet er een uitgebreide analyse worden uitgevoerd.

2.2 Maatregelen bij ICT

Bij interne systemen van de VRK 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 VRK in beheer is. Dit betekent dat er op voorhand gekeken moet worden of de SaaS-dienstverlening een voldoende beveiligingsniveau biedt.

In specifieke gevallen zal een Service Level Agreement (SLA/DAP) opgesteld moeten worden. Hierin komen ook afspraken in terug die van invloed zijn op de informatiebeveiliging, zoals de beschikbaarheid, rapportages, back-up & 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 VRK 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 VRK verwacht van SaaS-leveranciers actuele kennis op het gebied van risico's, kwetsbaarheden en security. Voor SaaS-applicaties kan de OWASP Top Ten (2021) als startpunt voor bewustwording dienen. Voorts zijn er verschillende alternatieven/white papers/hulpmiddelen en andere informatie op het gebied van bewustwording te vinden, waaronder bij het NCSC of het NIST.

Bovendien dient elke SaaS-applicatie minimaal (maar niet uitsluitend) te worden getest op de meest voorkomende kwetsbaarheden uit het OWASP Top Ten (2021) document waarmee aangetoond kan worden dat deze kwetsbaarheden bij de productieversie niet meer aanwezig zijn;

A01:2021-Broken Access Control;

A02:2021-Cryptographic Failures;

A03:2021-Injection;

A04:2021-Insecure Design;

A05:2021-Security Misconfiguration;

A06:2021-Vulnerable and Outdated Components;

A07:2021-Identification and Authentication Failures;

A08:2021-Software and Data Integrity Failures;

A09:2021-Security Logging and Monitoring Failures;

A10:2021-Server-Side Request Forgery.

3. Informatiebeveiligingskader SaaS

De onderstaande tabellen geven het informatiebeveiligingskader weer van de VRK, Deze moeten door de SaaS leverancier worden 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 juiste (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/WA.02	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 crypto grafische 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 3.4 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 VRK ingevuld. De overige items worden door de 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 hardenings richtlijn.		
C.02	Leverancier is ISO27001 gecertificeerd met betrekking op de te leveren dienstverlening. De werking van de certificering en het gevolgde beveiligingsniveau kan worden aangetoond d.m.v. een Assurance-verklaring van een onafhankelijke auditor of d.m.v. een SOC 1 of SOC 2 Assurance-rapportage (ISAE 3402 of 3000) (afhankelijk van de invloed op de financiële jaarrekening van de VRK).		
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope) conform de webrichtlijnen van het NCSC en de OWASP top 10 2021.		
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 derde partij. 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 een exporteerbaar formaat aan de VRK 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 de laatste (beveiliging) 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 uitsluitend verwerkt binnen de grenzen van de EER.		
P2	Leverancier treft alle noodzakelijke maatregelen conform de AVG om de persoonsgegevens van de VRK 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 productieomgeving 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 VRK is door de leverancier afgeschermd door versleuteling of autorisaties.		
P8	De leverancier heeft in de applicatie een proces ingebouwd zodat aan de vereisten van bewaartermijnen kan worden voldaan.		
P9	De leverancier heeft in de applicatie een proces ingericht om eenvoudig uitvoering te kunnen geven aan rechten van betrokkenen		

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 VRK te bepalen tijdsframe na minimaal 5 foutieve inlogpogingen.		
IB4	Alle inlogpogingen (inclusief mislukte) van gebruikers worden gelogd. Minimaal wordt het volgende 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 apparaat en niet in de oplossing.		
IB7	De geleverde oplossing biedt standaard two-factor authenticatie (2FA). In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal iedere 90 dagen het wachtwoord vernieuwd.		
IB8	De aangeboden MFA/2FA 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 TPM (ISAE 3402 of ISAE 3000 type 2) of anderzijds een audit verslag, dat de geleverde dienst(en) voldoen aan de ISO 27001 beveiligingseisen of de richtlijnen van het NCSC.		
	Indien de applicatie archiefwaardige informatie bevat dan wel opslaat is de ISO 16175-1 van toepassing		

3.4 Uitvoerend IT domein (technisch)

Maatregel nr.		Aanwezig Ja/Nee/NVT	Uitleg indien niet aanwezig of NVT
T.01	Algemeen Leverancier maakt gebruik van webservices of web-api's die hoofdzakelijk via het http-applicatie-protocol versleuteld worden aangeboden. Non-http-applicatie-protocollen worden alleen in overleg toegestaan.		
T.02	Versleuteling Dataverkeer wordt versleuteld met PKI-certificaten, conform de richtlijnen van het NCSC (TLS 1.2 of hoger). Voor domeinnamen eindigend op vrk.nl worden PKI-Overheidscertificaten gebruikt. Https-verkeer verloopt over poort 443.		
T.03	Architectuur De oplossing van de SaaS-leverancier is horizontaal en/of verticaal schaalbaar. Het systeem is in staat om schommelingen in gebruik adequaat op te vangen zolang deze binnen de marges van de gebruiksvoorwaarden vallen.		

T.04	Communicatie met de VRK-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 VRK 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; 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 minimaal de Microsoft Edge Chromium browser. Specifieke client-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 MS Office 2019 of hoger		
T.10	Toegangsbeveiliging Burger authenticatie verloopt via DigiD, ketenauthenticatie via e-Herkenning EH-2 of EH-3		
T.11	De VRK hanteert Azure OpenID Connect (OIDC) als primair SSO authenticatie- en delegatieprotocol, secundair wordt ook SAML2.0 via Azure ondersteund als SSO-authenticatie- en delegatieprotocol.		
T.12	Netwerken Leverancier heeft netwerksegmentatie geïmplementeerd waarbij omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden. Zoals bijvoorbeeld de kantoor-, acceptatie-, en productieomgevingen.		
	De oplossing maakt gebruikt van de verplichte standaarden (pas toe of leg uit) die het Forum Standaardisatie heeft goedgekeurd voor alle overheidsinstanties, indien zulke technologieën nodig zijn binnen de oplossing. Afwijkingen t.o.v. de lijst van standaarden worden schriftelijk onderbouwd en uitgelegd.		