

Bijlage 22 - Informatiebeveiligingskader SAAS

De beheersmaatregelen SaaS 1.0. document is de meetlaet voor het goed kunnen borgen van de webapplicatie. Dit document is onlosmakelijk verbonden aan het in productie nemen van de gekozen oplossing, de in het blauw gearceerde beheersmaatregelen van dit document onderstrepen daarbij een extra belang voor dit product om te borgen.

Maatregel nr.		Aanwezig Ja/Nee Uitleg indien niet aanwezig
IB.01	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.	
IB.02	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.	
IB.03	Het (webapplicatie)beheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	
IB.04	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	
IB.05	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	
IB.06	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	
IB.07	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.	
IB.08	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	
IB.10	Voor het configureren van netwerken is een hardenings richtlijn beschikbaar.	
IB.11	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT componenten van de webapplicatie (scope).	
IB.12	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	
IB.13	Leverancier is ISO 27001 en/of ISAE 3402 type2 / 3000 gecertificeerd met betrekking op de te leveren dienstverlening en toont dit aan. Vooraf aan de definitieve oplevering wordt een technische beveiligingsaudit (pen en hacktest) uitgevoerd op de op te leveren oplossing. De gemeente Amsterdam kan hiervoor een onafhankelijke derde partij aanwijzen die deze test gaat uitvoeren. De leverancier implementeert, op eigen kosten, de aanbevelingen	

	die naar aanleiding van de pen- of configuratietesten worden gedaan. Indien de leverancier een recent uitgevoerde pen en hacktest heeft uitgevoerd, dan ontvangt de gemeente Amsterdam een kopie ter validatie.	
IB.14	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	
IB.15	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	
IB 16 Privacy	De leverancier werkt volgens de geldende wet - en regelgeving zoals de Wet Bescherming Persoonsgegevens/Algemene verordening Gegevensbescherming en past voor zover mogelijk zaken als privacy by design en by default toe.	
IB 17 Privacy	Bij een SaaS oplossing waarbij persoonsgegevens verwerkt worden, ondertekend de Leverancier de verwerkersovereenkomst van de gemeente Amsterdam en werkt conform de daarin gemaakte afspraken. In de verwerkersovereenkomst is een clause opgenomen over het melden van datalekken.	
IB 18	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en crypto grafische technieken.	
IB 19	Leverancier tekent een geheimhoudingsverklaring met de gemeente Amsterdam. Leverancier zorgt dat zijn personeel zich houdt aan deze geheimhoudingsverklaring.	
IB.20	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICTvoorzieningen.	

INFORMATIEBEVEILIGING versie 1.0

1.1 Technische maatregelen SAAS

Maatregel nr.		Aanwezig Ja/Nee/NVT
		Uitleg indien niet aanwezig of NVT
T.01	Verkeer encryptie via minimaal TLS 1.2 of hoger over http (https) poort 443	
T.02	Compatible met Internet Explorer 11 en MS Office 2013 / 2016	
T.03	Geen applicatie specifieke plugins (Zero footprint)	
T.04	Non-http verkeer, bijvoorbeeld bestanduitwisselingen t.b.v. secure e-mail, dient over protocollen als https, sftp (ftp-over-ssh) of ftps (ftp-over-https) met als minimum TLS 1.2 of hoger plaats te vinden.	
T.05	Authenticatie vindt plaats op basis van SAML2.0/OAUTH2.0 of hoger.	
T.06	Burger authenticatie via DigiD Ketenauthenticatie via e-Herkenning EH-2 of EH-3	
T.07	Alle output, exports, of gecreëerde bestanden via de frontend benaderbaar. Geen shares of ftp services die rechtstreeks moeten worden benaderd.	
T.08	Geen communicatie over en weer met overige applicaties binnen de gemeentelijke infrastructuur behalve wanneer deze API's hanteren die hiervoor geschikt zijn. (geen backchannel communicatie)	
T.09	Verbindingen tussen cliënt (webbrowser/app) en de (SAAS/webapplicatie) server dienen versleuteld (minimaal SSL/TLS) plaats te vinden op basis van een PKI Overheids Extended Validation SSL certificaat van de gemeente Amsterdam. Bij verwerking van bijzondere persoonsgegevens dienen deze gegevens aanvullend versleuteld via de bestaande SSL	
T.10	Het netwerk (van de leverancier) is onderverdeeld in aparte en gescheiden beveiligingssegmenten zoals gescheiden productie, acceptatie en kantoor applicatie omgevingen.	
T.11	Verkeer tussen de verschillende segmenten wordt gefilterd en verkeer wordt alleen toegestaan in overeenstemming met applicatie behoeftes	
T.12	De leverancier inspecteert al het inkomende en uitgaande netwerkverkeer via IDS/IPS en meldt verdachte zaken aan de afnemer indien dit relevant is voor de afgenomen dienst.	
T.13	De leverancier staat geen remote acces tot de oplossing via SBC oplossingen (Citrix of RDP.	

1.2 Beheersmaatregelen SAAS

Maatregel nr.		Aanwezig Ja/Nee
		Uitleg indien niet aanwezig of NVT
B.01	Bij de verwerking van gevoelige en bijzondere persoonsgegevens dient er een aanvullende authenticatie methode plaats te vinden, minimaal two factor, beter bekend als MFA	
B.02	De op te leveren oplossing biedt een gelaagde autorisatiemogelijkheden met de mogelijkheid van beheer aan de gebruikers organisatie. Rollen en rechten zijn gescheiden voor beheer, gebruik en rapportages.	

B.03	Wachtwoorden moeten zijn samengesteld op basis van de geldende beveiligingseisen (bijv. NIST 800-63) en worden opgeslagen middels salted hash	
B.04	Het dagelijks gebruik van admin of superuser accounts dient vermeden te worden. De oplossing moet zodanig ingericht zijn dat dagelijks gebruik van dergelijke accounts niet nodig is. Het gebruik van dergelijke dient te worden gelogd.	
B.05	Inlogpogingen moeten beperkt zijn tot maximaal 10 foutieve pogingen per keer met een lockperiode minimaal 5 minuten voordat weer kan worden ingelogd. Dit om bruteforcing te voorkomen.	
B.06	Handelingen van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden gelogd en minimaal voor 3 maanden te worden bewaard. Op aanvraag van de gemeente Amsterdam worden deze ter beschikking gesteld	
B.08	Er wordt minimaal gebruik gemaakt van een (O)TAP omgeving om gestructureerd wijzigingen door te (kunnen) voeren	
B.09	In het geval van multi-tenancy; mag de data van de gemeente Amsterdam op geen enkele wijze beschikbaar komen van de andere tenants. Virtuele services of netwerk devices mogen shared zijn behalve de data.	
B.10	De toegang tot vertrouwelijke (persoons) <u>gegevens</u> in de database dient te worden gereguleerd of door encryptie onmogelijk te zijn gemaakt. Bijvoorbeeld Azure Key Vault van Microsoft Azure (1)	
B.11	Webapplicaties worden ieder jaar op de laatste bekende versie van de OWASP (top 10) richtlijnen getoetst d.m.v. een hack en pentest die door een onafhankelijke derde wordt uitgevoerd.	
B.12	Webapplicaties worden reeds in acceptatie fase, door een onafhankelijk derde, aan een hack en pentest onderworpen waarbij de gevonden beveiligingsproblemen aantoonbaar, d.m.v. een hertest verholpen voordat de webapplicatie in productie gaat	
B.13	De leverancier neemt alle technische maatregelen om inbraak in de oplossing te voorkomen en te detecteren. Iedere inbraak, of pogingen er toe, dient dit binnen 24 uur bij de gemeente Amsterdam gemeld te worden.	
B.14	Er is een backup policy overeengekomen die gebaseerd is op de eisen en wensen van de gemeente Amsterdam, welke is opgenomen in de SLA/DAP. Backup media wordt conform deze policy opgeslagen en regelmatig gecontroleerd op herstelbaarheid. De leverancier draagt zorg voor het testen van backups t.b.v. een snelle recovery.	