Bijlage 06

Security & AVG

IWR2024|PSM

ICT Werkomgeving Rijk

Status: Versie 1.0
Referentie: IUC2024123004

Inhoud

1. Beveiliging

Voor de Rijksoverheid is een adequate beveiliging van wezenlijk belang. De PSM-Oplossing moet ingezet kunnen worden om documenten tot en met Departementaal Vertrouwelijk (Dep.V) gebruik met een maximaal beschermingsniveau BBN2 te kunnen verwerken.

Voor de PSM-Oplossing worden hiervoor de volgende vereisten gesteld.

2. Algemeen

1	De PSM-Oplossing dient te voldoen aan de eisen gesteld in deze Bijlage.

3. Privacy

2.	De PSM-Oplossing voldoet aan de AVG-wetgeving.
3	De verwerking van persoonsgegevens is conform de AVG ingevuld, waarbij de Opdrachtgever verwerkingsverantwoordelijke is en de Opdrachtnemer verwerker is. De Opdrachtnemer geeft dus invulling aan alle eisen die aan een verwerker worden gesteld. Tevens sluiten Opdrachtgever en Opdrachtnemer een verwerkersovereenkomst conform het model opgenomen in Bijlage 28. Opdrachtnemer werkt mee aan de totstandkoming van de DPIA en draagt zorg voor de implementatie van de mitigerende maatregelen.
4	De PSM-Oplossing heeft de mogelijkheid om geautomatiseerd de aan een specifiek natuurlijk persoon gerelateerde gebruikersgegevens te verwijderen of inactief te zetten op basis van een vooraf in te stellen interval.
5	In aanvulling op eis 1 geldt tevens dat de Opdrachtnemer op aanvraag van de IDV Belastingdienst binnen één week na de datum van aanvraag bewijs aanlevert dat in de gehele ontwerp en realisatie van de PSM-Oplossing rekening is gehouden met de gangbare principes van de AVG (conform Privacy en Security bij Design en Default) en dat er enkel word gewerkt met strikt noodzakelijke (persoons)gegevens. De standaardinstelling is dat persoonsgegevens zo veel mogelijk worden beschermd.
6	De Opdrachtnemer voldoet bij het leveren van een webapp aan de NCSC ICT-beveiligingsrichtlijnen voor webapplicaties: ICT-beveiligingsrichtlijnen voor webapplicaties | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl) https://www.ncsc.nl/documenten/publicaties/2023/december/01/infosheet_webapplicaties
7	Indien Opdrachtnemer naast een webapplicatie een native app aanbiedt gelden dezelfde eisen als voor de webapp, daarnaast dienen periodiek correctieve en functionele verbeteringen te worden doorgevoerd in de native apps.
8	De Opdrachtnemer zorgt voor een actief updatebeleid waarbij updates en patches van het onderliggende OS (het maakt niet uit of dit een VDI/Desktop/Laptop of mobiel device is) geen impact hebben op de werking van de PSM-Oplossing.
9	Indien Opdrachtnemer naast een webapplicatie ook een native app aanbiedt heeft deze een methodiek beschikbaar waarmee er een veilige koppeling conform de security-eisen gelegd kan worden tussen het mobiele device van de Rijksmedewerker en de PSM, minimaal versleuteld conform gangbare standaarden en adequate authenticatie.
10	De Opdrachtnemer voldoet voor een native iOS/iPadOS/Android app aan de NCSC ICT-beveiligingsrichtlijnen voor mobiele apps: ICT-beveiligingsrichtlijnen voor mobiele apps

	| Publicatie | Nationaal Cyber Security Centrum (ncsc.nl) (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps)
11	Opdrachtnemer voldoet aan de vigerende en toekomstige wet- en regelgeving (waaronder de AVG) met betrekking tot onder meer: - bewaartermijnen per gegevenssoort, - archiveren, - anonimiseren en - vernietigen van Persoonsgegevens en andere Klantgegevens. - regionale verwerking binnen de EER of een land met een adequaatheidsbesluit.
12	Voor het versturen en ontvangen van e-mail wordt als afzender een e-mailadres gebruikt op basis van een eigen e-mail suffix (bijv. @rijksprint.nl).
13	De mailvoorziening voldoet aan de relevante standaarden op de pas-toe-of-leguit-lijst van het forum standaardisatie (denk aan o.a. DNSSEC, DKIM, DMARC, DANE, SPF en IPV6).
14	De initiatie van de datastromen tussen MFP en de PSM gebeurt altijd vanuit de MFP's (Pull), met uitzondering van de enrollment van de MFP's.
15	Opdrachtnemer deelt en/of gebruikt geen Gegevens voor eigen doeleinden, anders dan strikt noodzakelijk voor de uitvoering van de Overeenkomst én dan alleen ná expliciete toestemming van de Opdrachtgever. In geval toont Opdrachtnemer aan welke Gegevens om welke reden(en) strikt noodzakelijk zijn.
16	Opdrachtnemer zal, in navolging van voorgaande, aangeven welke Gegevens in een dergelijk geval als noodzakelijk worden geacht voor de uitvoering van de Overeenkomst.

Gegevens die te relateren zijn aan de Opdrachtgever of haar medewerkers mogen zonder expliciete toestemming van de Opdrachtgever niet buiten de PSM-Oplossing verwerkt worden. Dat geldt uiteraard ook voor Persoonsgegevens. Productiegegevens worden alleen in de Productieomgeving verwerkt.

Buiten de Productieomgeving zijn de Gegevens, conform marktstandaarden, bijvoorbeeld die van de NCSC, gepseudonimiseerd of geanonimiseerd. Opdrachtnemer geeft de Opdrachtgever vooraf inzicht in hoe dit plaats vindt.

17	Opdrachtnemer conformeert zich, conform bovenstaande alinea, aan dat bij testen van de PSM-Oplossing geen gebruik wordt gemaakt van: • Productiegegevens; • Naar natuurlijke personen herleidbare Gegevens. Persoonsgegevens is slechts in uitzonderlijke situaties mogelijk, bijvoorbeeld bij analyse van opgetreden foutsituaties. Per geval dient door Opdrachtnemer expliciete toestemming aan Opdrachtgever te worden gevraagd conform een waiver-procedure. Deze waiver geldt slechts voor de benoemde test en tijdvak. Deze waiverprocedure wordt vastgelegd in een DAP met de IDV Belastingdienst

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Opdrachtgever mogen op geen enkele manier gecompromitteerd raken. Van medewerkers van Opdrachtnemer met toegang tot Gegevens en PSM-Oplossing wordt vooraf de achtergrond gecontroleerd. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG (algemeen screeningsprofiel, functie-aspecten: 11, 12, 13 en 41).

Voor niet ingezeten kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan.

Niet Nederlandse ingezetenen kunnen voor informatie terecht bij Justis. Zie voor meer informatie:

https://www.justis.nl/service-contact/veelgestelde-vragen/vog/hoe-kan-ik-een-vog-aanvragen-als-ik-niet-ben-ingeschreven-in-de-brp#:~:text=Sluiten-,Hoe%20kan%20ik%20een%20VOG%20aanvragen%20als%20ik%20niet%20ben,VOG%20rechtstreeks%20bij%20Justis%20aanvragen

en

https://www.rijksoverheid.nl/wetten-en-regelingen/productbeschrijvingen/aanvragen-verklaring-omtrent-het-gedrag-vog-bij-justis

18	Opdrachtnemer beschikt voor al zijn medewerker(s) die werkzaamheden m.b.t. de PSM-Oplossing uitvoeren, tijdens uitvoering van de betreffende werkzaamheden over een geldige Verklaring Omtrent Gedrag (hierna VOG.) algemeen screeningsprofiel, functie-aspecten: 11, 12, 13 en 41.

4. Gegevens

De Gegevens van de Opdrachtgever moeten gescheiden worden verwerkt (waaronder opgeslagen) van andere klanten van Opdrachtnemer; de Opdrachtgever wil geen zicht hebben in Gegevens van andere klanten van de Opdrachtnemer en andere klanten mogen geen zicht in de Gegevens van de Opdrachtgever hebben.

Medewerkers van Opdrachtnemer mogen alleen toegang hebben tot de Gegevens van de Opdrachtgever voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

Vereisten:

19	Gegevens van de Opdrachtgever worden gescheiden opgeslagen van de Gegevens van andere klanten van de Inschrijver.

20	Met betrekking tot bovenstaande geldt dat de private key zowel bij de Opdrachtgever dienst als de Opdrachtnemer in beheer moet kunnen worden gegeven.

21	De gegevens van Opdrachtgever zijn ten minste logisch gescheiden van de gegevens van overige afnemers van de diensten van Opdrachtnemer. Hierbij geldt het gehele verzorgingsgebied, zoals beheerd door de IDV Belastingdienst, als één afnemer.
22	De aangeboden oplossing dient in een voor Rijksoverheid beschikbaar gestelde eigen tenant te draaien.
23	Indien de dienstverlening van de PSM-Oplossing gedeeld wordt met andere klanten, laat de opdrachtnemer zien dat de voorzieningen en gegevens van klanten van elkaar gescheiden zijn.
24	Opdrachtnemer garandeert dat buitenlandse mogendheden niet op grond van een MLAT (mutual legal assistance treaty) of andere vorm van wetgeving of via zeggenschap in de onderneming van de Opdrachtnemer toegang hebben tot de gegevens of de continuïteit van de dienstverlening kunnen beïnvloeden. Bij twijfel of er zal kunnen worden voldaan aan het gestelde kan de Opdrachtgever een veiligheidsonderzoek starten, conform de Wet Veiligheidsonderzoeken.
25	De Opdrachtnemer erkent dat alle door de PSM-Oplossing verwerkte gegevens eigendom zijn van de Opdrachtgever. Dit betreft onder meer, maar is niet gelimiteerd tot, gebruikersadministratie, printopdrachten, scanopdrachten. Diagnostische gegevens mogen uitsluitend gebruikt worden ter verbetering van de PSM-Oplossing. Deze gegevens heten gezamenlijk: Klantgegevens.

26	De Opdrachtnemer maakt inzichtelijk welke gegevens op welk endpoint verwerkt worden en toont aan dat dit ook feitelijk het geval is.
27	De dataopslag van printjobs is minimaal logisch gescheiden van de dataopslag van de PSM.
28	Binnen de PSM-Oplossing zijn de bestandsnamen van de printopdrachten standaard verborgen. De gebruiker ziet in zijn of haar lijst van klaarstaande printopdrachten wel de volledige naam van het af te drukken document.
29	De Opdrachtnemer beoordeelt zijn toeleveranciers op opzet, bestaan en werking van de (uitwijk)maatregelen. Hierbij is specifiek aandacht voor de wijze waarop geborgd is dat er geen overdracht van persoonsgegevens plaatsvindt buiten de Europese Economische Ruimte (EER) noch naar landen waarvoor geen adequaatheidsbesluit van de Europese Commissie is afgegeven. Beschrijf hoe u dat doet.
30	Toegang tot Gegevens van de Opdrachtgever is beperkt voor medewerkers van de Opdrachtgever en medewerkers van de Inschrijver voor zover dit noodzakelijk is voor de uitvoering van de Overeenkomst.

De Aanbestedende dienst maakt gebruik van versleutelde Gegevens bij opslag. Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten de PSM-Oplossing terechtkomen, andere partijen geen gebruik kunnen maken van deze Gegevens. De vereisten hiervoor zijn:

31	Data in de PSM-Oplossing is versleuteld. Encryption-at-rest en encryption-in-transit is hierbij toegepast
32	De gegevens in transit zijn End-to-end versleuteld. Gegevens ‘at rest’ zijn versleuteld als het gaat om printjobs. De scanbestanden worden na het verwerken versleuteld verstuurd/verplaatst naar de eindlocatie.
33	De toegang tot onversleutelde gegevens is strikt op basis van noodzakelijkheid. De inschrijver maakt inzichtelijk tot welke onversleutelde gegevens hijzelf en zijn Toeleveranciers toegang hebben, op welke momenten, en voor welk doel.
34	Alle data en daarvan af te leiden inzichten binnen de PSM zijn en blijven te allen tijde eigendom van de Rijksoverheid. Daarnaast zijn ze te allen tijde voor de Rijksoverheid toegankelijk.

5. Beveiligingsincidenten

Dit zijn Incidenten die een vermoedelijk of mogelijk opzettelijke inbreuk veroorzaken op de beschikbaarheid, vertrouwelijkheid of integriteit van de Gegevens in informatie verwerkende systemen of inbreuk maken op deze systemen zelf.

Voor beveiligingsincidenten geldt dat bij ontdekking/melding zowel de Impact als Urgentie als Hoog worden gekwalificeerd wat resulteert in een prioriteit 1 Incident. Een beveiligingsincident wordt altijd per direct opgevolgd met een actie van de Opdrachtnemer.

Na een eerste evaluatie kan onderbouwd besloten worden de prioriteit te verlagen. De Opdrachtgever heeft hierbij het laatste woord.

Er worden vier typen beveiligingsincident onderkend:

1. (Cyber)hack, of een poging daartoe;
2. Coordinated Vulnerability Disclosure (CVD, voorheen Responsible disclosure);
3. Kwetsbaarheid via CVE-database of Security Note van leverancier van ICT-component of beveiligingsberichten van CERTs (NCSC, bedrijfstak- of sectorgerichte CERT) en
4. Kwetsbaarheid vanuit beveiligingstest (A&P-test of Vulnerability scan, die Ongeacht de opdrachtgever van deze test (opdrachtgever en/of opdrachtnemer PSM-dienst) geïnitieerd kan worden.

Als waarderingsmethodiek voor Kwetsbaarheden wordt gebruik gemaakt van de meest recente versie van marktstandaard Common Vulnerability Score System (CVSS, momenteel

versie 4.0). Oplostermijnen die hieraan gekoppeld zijn, zijn vermeld in Bijlage 17 - SLA parameters.

Voordat de PSM-Oplossing in productie kan gaan, wordt de beveiliging van de PSM-Oplossing getest ter Acceptatie (zie Bijlage 2, par. 2.5 Fasering punt 2 testen). Daarna gebeurt dat periodiek (minimaal jaarlijks).

Gemiddeld- en Laagrisico bevindingen worden afgehandeld conform het Pas-toe-of-Leg-uitprincipe. Dit laatste, een Leg uit (Explain), betekent dat er besloten is dat de Kwetsbaarheid niet weggenomen wordt of dat adresseren ervan meer tijd gaat kosten dan de standaard Oplostijd. Opdrachtnemer onderbouwt in een dergelijk geval haar besluit (bijvoorbeeld: er zijn afdoende mitigerende maatregelen getroffen waardoor de Kwetsbaarheid niet uitgevoerd hoeft te worden of dat de impact nihil is). Het is aan de Opdrachtgever om akkoord te gaan met een Leg-uit.

Opdrachtgever heeft geen oplossingen in productie staan waarin zich Kwetsbaarheden bevinden die als Kritisch of Hoog risico zijn gekwalificeerd. Bij Kritische- en Hoge risico's kan een Leg-uit alleen gebruikt worden om de oplostermijn (beperkt) op te rekken. Dit kan alleen met nadrukkelijke instemming van de Opdrachtgever.

Het Stekkermandaat (zie ook paragraaf 1.1.7 **Stekkermandaat**) wordt in gang gezet als een ICT-oplossing reeds in productie staat. Staat een ICT-oplossing nog niet in productie, dan zal dat ook niet mogen totdat de Kritische-en Hoge risicobevindingen zijn weggenomen.

De vereisten hiervoor zijn:

35	Uit bovenstaande volgt daarom de Eis dat Opdrachtnemer zich conformeert, gedurende de looptijd van de Overeenkomst, aan de door de Opdrachtgever gebruikte methode (CVSS) om beveiligingsincidenten te kwalificeren en heeft haar organisatie zodanig ingericht dat de door de Opdrachtgever onderkende typen Beveiligingsincidenten voor (onderdelen) van de PSM-Oplossing binnen gestelde termijnen, als onderdeel van het Onderhoud & Support, opgepakt en opgelost worden.
36	Bij het constateren van Kwetsbaarheden met een niveau van kritisch (critical) of hoog (high), conform CVSS (de huidige bij de Opdrachtgever toegepaste versie CVSS 4.0), wordt de Opdrachtgever daarover binnen één (1) uur door Opdrachtnemer geïnformeerd. Afspraken over het toepassen van een volgende versie van CVSS hier omtrent worden vastgelegd in een DAP met de IDV Belastingdienst.
37	Kwetsbaarheden die leiden tot een Incident worden gekwalificeerd door middel van CVSS 4.0. Op basis van de CVSS 4.0 kwalificaties gelden voor de Opdrachtnemer de oplostijden genoemd in Bijlage 17 – SLA parameters.
38	In de PSM-Oplossing gebruikte Open Source-code en/of libraries van andere toeleveranciers bevatten geen bekende Kwetsbaarheden. Er wordt gebruik gemaakt van de meest recente veilige versies uit betrouwbare bron.

Opdrachtgever gaat er van uit dat Opdrachtnemer de PSM-Oplossing ook levert of gaat leveren aan derden. Indien in dergelijke instances zich inbreuken op beveiliging en/of privacy voordoen, die zich ook kunnen voordoen in de aan de Opdrachtgever geleverde PSM-Oplossing, dan wordt de Opdrachtgever daarvan onverwijld van op de hoogte gebracht om zo nodig mitigerende maatregelen te kunnen treffen. Opdrachtgever monitort dit actief.

Het gaat niet alleen om opgetreden Incidenten, maar ook om mogelijke toekomstige Incidenten waar Opdrachtnemer van kan uitgaan dat deze in de (nabije) toekomst kunnen optreden, ook als het Opdrachtgever mogelijk niet direct raakt. Denk aan een zero-day exploit.

Het gaat de Opdrachtgever om het (technisch) inhoudelijke Incident om deze te kunnen analyseren en, zo nodig, mitigerende maatregelen te treffen. Opdrachtgever wenst zich te kunnen voorbereiden op mogelijke incidenten of nieuwsberichten rondom diensten die de

Opdrachtgever gebruikt. Er worden nadrukkelijk geen bedrijfsgegevens van getroffen partijen gedeeld.

Opdrachtnemer zal in dat geval tevens de omvang van het Incident aangeven, de verwachte consequenties voor de Opdrachtgever, alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken.

Vereiste

39	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de PSM-Oplossing bij derden. Het proces hiervoor moet worden beschreven in een DAP met de IDV Belastingdienst.

Indien Opdrachtgever (op basis van een risico-inschatting) het noodzakelijk acht een A&P-test uit te laten voeren dan staat Opdrachtnemer dat toe en werkt daar conform afspraken aan mee. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de PSM-Oplossing onderdeel van is of op de PSM-Oplossing zelf.

Het organiseren van deze A&P-test gebeurt door Opdrachtgever; het uitvoeren van de A&P-test zelf is voor rekening van Opdrachtgever.

Eventuele Kwetsbaarheden worden opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer werkt hier als onderdeel van Onderhoud & Support aan mee.

Vereiste

40	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. inbreuken op beveiliging en/of privacy in de PSM-Oplossing bij derden.

6. Datalek

De IDV Belastingdienst handelt als verwerkingsverantwoordelijke conform de wettelijke kaders als primaire partij Data incidenten af. De verwerkingsverantwoordelijke moet de Autoriteit Persoonsgegevens (AP) binnen 72 klokuren op de hoogte stellen van een Datalek en eist van Opdrachtnemer onverwijld, doch uiterlijk binnen 24 klokuren op de hoogte te worden gesteld van een door Opdrachtnemer geconstateerd Datalek. Een (potentieel) Datalek is het gevolg van een beveiligingsincident en moet ook als zodanig worden geregistreerd en afgehandeld. Melding aan AP en afhandeling van het corresponderende beveiligingsincident kan parallel plaatsvinden.

Bij het informeren over een Datalek moet de omvang worden aangegeven alsmede de getroffen en/of te nemen maatregelen om de gevolgen te adresseren. In afstemming wordt bepaald welke partij primair analyse en afhandeling uitvoert. Verwerkingsverantwoordelijke en Opdrachtnemer houden elkaar op de hoogte. Procedures hier omtrent worden vastgelegd in een DAP met de IDV Belastingdienst.

Vereiste

41	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van een Datalek in de PSM-Oplossing.

7. Coordinated Vulnerability Disclosure

IDV Belastingdienst heeft een Coordinated Vulnerability Disclosure-procedure (CVD-procedure). Goedwillende beveiligingsonderzoekers kunnen via een vastgesteld proces kwetsbaarheden, mits er geen wetten worden overtreden, melden. Het CVD-proces is op deze pagina beschreven: https://www.belastingdienst.nl/security#coordinated-vulnerability-disclosure. En op pagina van het NCSC https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad.

Vereiste

42	Opdrachtnemer conformeert zich aan bovengenoemde CVD-procedure m.b.t. het afhandelen van CVD-meldingen. Procedures hier omtrent worden vastgelegd in een DAP met de IDV Belastingdienst.

8. Stekkermandaat

Opdrachtgever kent het principe van het Stekkermandaat. Opdrachtgever kan opdracht geven dat de PSM-Oplossing (inclusief de Gegevens) van de IDV Belastingdienst onbeschikbaar gemaakt wordt voor (minimaal) toegang vanaf het internet. Effectief zal dit betekenen dat:

- Gegevens van de Opdrachtgever ontoegankelijk worden gemaakt en/of
- (Relevante delen van) de PSM-Oplossing onbeschikbaar worden gemaakt.

Het Stekkermandaat wordt uitgevoerd op het moment dat de beveiliging van de PSM-Oplossing (inclusief Gegevens) in gevaar is. Dat is het geval als er zich een beveiligingsincident met een score van Kritisch of Hoog risico voordoet waarbij de onderliggende Kwetsbaarheid niet tijdig kan worden weggenomen.

De PSM-Oplossing wordt weer in productie (online) gebracht na toestemming van de Security Officer van de IDV Belastingdienst. Opdrachtnemer werkt, daar waar relevant, kosteloos mee bij:

- Het onbeschikbaar en ontoegankelijk maken van de PSM-Oplossing of de Gegevens (dit is inclusief andere portalen en koppelingen);
- Exportacties van Gegevens indien het proces via een andere oplossing/procedure voortgezet dient te worden bij Opdrachtgever.

Het proces en de afspraken hiervoor worden beschreven in een DAP met de IDV Belastingdienst.

Vereiste

43	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. het omgaan met van het Stekkermandaat in relatie tot de PSM-Oplossing. Hierbij geldt dat tussen het inroepen van het Stekkermandaat en het afronden van de uitvoering maximaal 4 uur zit. Het startmoment begint als het verzoek om Gegevens veilig te stellen door Opdrachtnemer is ontvangen.

Bij (langdurige) uitval van de PSM-Oplossing krijgt de Opdrachtgever de beschikking over de meest recente Gegevens. Aanlevering gebeurt via een afgestemd veilig kanaal en conform afspraken conform (machine leesbaar) formaat.

Vereiste

44	Opdrachtnemer levert op aanvraag en conform afspraken een voor de IDV Belastingdienst bruikbare digitale kopie van de meest actuele Gegevens en haar structuur. Vertrouwelijkheid en integriteit blijven geborgd. De afspraken hierover worden in een DAP met de IDV Belastingdienst vastgelegd.

Reinstate

Het weer beschikbaar maken van de PSM-Oplossing (Reinstate) houdt in dat de PSM-Oplossing weer in productie wordt gebracht met gebruikmaking van de meest actuele Gegevens. Dit is inclusief importacties van de Gegevens indien het proces via een andere oplossing/procedure voortgezet is geweest.
Hierbij geldt de speciale aandacht voor de situatie dat Gegevens van vóór het stopzetten van de PSM-Oplossing samengevoegd moeten worden met de Gegevens die in de tussentijd, zijn gegenereerd. Integriteit en Vertrouwelijkheid van de Gegevens blijven te allen tijde geborgd.
Opdrachtnemer werkt met betrekking tot bovenstaande alinea's als onderdeel van het Onderhoud & Support mee met het opnieuw in gebruik nemen van de PSM-Oplossing.
De afspraken hierover worden in een DAP met de IDV Belastingdienst vastgelegd.

Vereiste

45	Opdrachtnemer conformeert zich aan bovenstaande alinea's m.b.t. de Reinstate van de PSM-Oplossing.

9. Beveiligingstesten

Inleiding

Beveiligingstesten zijn een belangrijk onderdeel in het stelsel van beveiligingseisen-en maatregelen. De Opdrachtgever stelt Eisen aan deze beveiligingstesten.

Deze Eisen betreffen de testmethode, waardering van de bevindingen, de testende partij, de rapportage en de afhandeling van de Kwetsbaarheden.

Er worden periodiek of rond een omvangrijke release beveiligingstesten uitgevoerd op onder andere, maar niet beperkt tot, de internet, user- en beheerder-facing kanten van de ICT-oplossing. Het betreffen zowel Attack & Penetration testen als Vulnerabilty scans. De partij waar primair de hosting plaatsvindt, is de eerstverantwoordelijke om deze beveiligingstesten uit te voeren. Meestal is dat de Opdrachtnemer. Beveiligingstesten zijn slechts momentopnamen. Herhaling is dus van belang. Net als het hertesten van geadresseerde bevindingen. De kosten van uitvoering van dergelijke beveiligingstesten worden gedragen door de Opdrachtnemer die de beveiligingstest behoort uit te voeren. Opdrachtgevver werkt op verzoek kosteloos mee aan dergelijke testen. Onder het kosteloos meewerken, valt onder andere:

- Het beantwoorden van vragen in de verschillende fasen van voorbereiding en uitvoering van een beveiligingstest;
- Het oplossen van bevindingen die uit de beveiligingstesten volgen. Dit is inclusief eventueel benodigd overleg hierover.

A&P test vanuit Opdrachtnemer

Opdrachtnemer doet op verzoek van Opdrachtgever, een voorstel aan Opdrachtnemer voor de (gecertificeerde) partij voor uitvoering van de A&P-test en de inhoud van de A&P-tests. De Opdrachtgever kan in zijn verzoek eisen stellen aan de kwaliteit van zowel de A&P-test, als de rapportage daarover.

Bevindingen volgend uit de beveiligingstesten zullen tussen de Opdrachtgever en Opdrachtnemer worden gedeeld en zo nodig besproken. Hetzelfde geldt voor plannen van aanpak en Verbeterplannen op het gebied van security. Ook voor deze specifieke Verbeterplannen geldt het proces zoals opgenomen in Bijlage 2, eis 124. Om de A&P-test te kunnen beoordelen wordt het volgende tussen de partijen gedeeld:

- De scope van de test (infrastructuur, middleware, tooling en (API-)koppelingen) is beschreven. Het is duidelijk welke delen van de PSM-Oplossing binnen en buiten scope zijn geweest. Het is bekend welke beveiligingsmaatregelen (tijdelijk) uitgeschakeld waren;

- Welke testmethodieken (black-, grey- of crystal boxtesting, wel of niet inclusief broncodereview) zijn gebruikt, en welke normenkaders zijn gebruikt (bijvoorbeeld STRIDE, OWASP Top 10, SANS Top 25, OWASP Mobile Top 10, etc.);
- Hoe getest is; geautomatiseerd, handmatig (worden geautomatiseerd gevonden handmatig geverifieerd?);
- Managementsamenvatting met een definitie van de opdracht, relevante kenmerken van de A&P-test, een conclusie en aanbevelingen;
- Alle gevonden Kwetsbaarheden zijn opgenomen in de rapportage met CVSS-waardering. Aangegeven welke versie van CVSS (vanaf 3.0) is gebruikt. Bij voorkeur met de statusaanduiding, bijvoorbeeld "In behandeling" (met plandatum) of "Opgelost (en hertest)".

In een Verbeterplan wordt het volgende opgenomen:

- Onderwerp/naam van het Verbeterpunt;
- Startdatum;
- Geplande einddatum oplossing;
- Beoogde aanpak (kort);
- Status;
- Lessons learned;
- De Security Roadmap.

Vereisten

46	Opdrachtnemer conformeert zich aan bovenstaande, onder het kopje **Inleiding** genoemde, alinea's m.b.t. Beveiligingstesten in relatie tot de PSM-Oplossing.
47	De Opdrachtnemer voldoet gedurende de duur van de Overeenkomst aan de eis van ISO 27001 certificering. De PSM-Oplossing voldoet aan de normen die genoemd zijn in de actuele versie van de BIO op BBN2 niveau. Opdrachtnemer toont jaarlijks en bij inschrijving aan dat hij aan de normen voldoet (in opzet, bestaan en werking) die genoemd zijn in de BIO, middels de volgende documenten: 1. SOC2 Type2 en/of ISAE3402 Type II verklaring; 2. Rapport dat aantoont dat er jaarlijks een onafhankelijke pentest op de PSM-Oplossing correct, volledig en succesvol naar oordeel van de IDV Belastingdienst, is uitgevoerd; Of andere verklaringen en rapporten die een vergelijkbaar niveau van informatiebeveiliging aantonen. IDV Belastingdienst heeft het recht vast te stellen of een betreffende verklaring of rapport het vergelijkbare niveau van informatiebeveiliging aantoont.
48	De oplossing en de Opdrachtnemer voldoen en blijven voldoen aan de normen die genoemd zijn in de actuele versie van de BIO (en NIS2 na inwerkingtreding) op BBN2-niveau in opzet, bestaan en de werking. Informatiebeveiliging is een dynamisch onderwerp: de Opdrachtnemer evalueert ten minste jaarlijks de beveiligingsmaatregelen en stel deze bij. Het verbeterplan wordt gedeeld met de Opdrachtgever. Een SOC2 verklaring kan onderdeel uitmaken van het verbeterplan.
49	De implementatie van de beveiligingsmaatregelen voldoet aan best practices waaronder common criteria, bescherming tegen OWASP-kwetsbaarheden, de handreiking TLS van NCSC (https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1).
50	De Opdrachtgever heeft naast een SOC2 verklaring het recht om een security gerelateerde test (bijvoorbeeld, maar niet gelimiteerd tot, een audit, een kwetsbaarhedenscan, een pentest of red team testing) uit te laten voeren om de beveiliging te testen tot een maximum van twee per jaar.

	De Opdrachtgever voert dit zelf uit of contracteert hierbij een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. Opdrachtnemer werkt kosteloos mee aan tests die door of namens de Opdrachtgever worden uitgevoerd. Opdrachtnemer en de Opdrachtgever besluiten gezamenlijk de scope van de test. Mochten partijen er niet gezamenlijk uit komen, dan neemt de Opdrachtgever de uiteindelijke beslissing hierover. Security tests zijn enkel toetsend en vervangen niet de beveiligingsmaatregelen van de Opdrachtnemer. De resultaten van de testen worden gedeeld met de Opdrachtnemer. Voor het oplossen van de bevindingen maakt de Opdrachtnemer een plan met een planning die passend is gezien de ernst van de bevindingen. Dit plan wordt besproken met en geaccordeerd door de Opdrachtgever. Na implementatie vindt een aansluitende hertest plaats.
51	De opdrachtnemer gekwalificeerd kwetsbaarheden doormiddel van het Common Vulnerability Scoring System 4.0 (CVSS 4.0) en de logische opvolgers. En dienen conform de in de SLA opgegeven oplostijden te worden verholpen.
52	Indien kwetsbaarheden in productiesystemen een CVSS-score van 7 of hoger hebben, wordt dat direct gemeld bij de Opdrachtgever en binnen 16 werkuren opgelost. In de tussenliggende periode wordt het risico beheerst met mitigerende maatregelen.

A&P test vanuit Opdrachtgever

Als de Opdrachtgever het noodzakelijk vindt om de sterkte van de beveiligingsmaatregelen van de PSM-Oplossing te (laten) toetsen wenst Opdrachtgever hiervoor een onafhankelijk (gecertificeerd) A&P-testbedrijf in te zetten. Het organiseren en de (kosten) voor het uitvoeren van deze A&P-test gebeurt door de Opdrachtgever. Opdrachtnemer werkt (kosteloos) mee aan deze testen onder dezelfde voorwaarden als van toepassing zijn voor Opdrachtgever zoals vermeld onder punt 9 bij ***Inleiding.***

Voor de aanvullende uitgangspunten bij A&P-testen die door of namens de Opdrachtgever worden uitgevoerd, geldt:

- Er getest wordt in de Acceptatieomgeving welke technisch gelijk is aan en voorzien is van dezelfde beveiligingsmaatregelen als de Productie-omgeving; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er wordt géén gebruik gemaakt van Productiegegevens; voor noodzakelijke afwijkingen is toestemming van de Opdrachtgever vereist;
- Er is sprake van een freeze-periode in de omgeving wordt getest; alleen in samenspraak met het A&P-testbedrijf, bijvoorbeeld om een patch uit te voeren om een Kwetsbaarheid weg te nemen, kan hiervan worden afgeweken;
- Kwetsbaarheden gekwalificeerd als Kritisch of Hoog risico worden zo mogelijk tijdens de A&P-test opgelost en hertest.

Opdrachtgever voert jaarlijks of na een significante release een A&P-test uit conform de hierboven beschreven richtlijnen van de IDV Belastingdienst. De precieze invulling van de A&P-test is afhankelijk van de situatie. Het kan een A&P-test zijn binnen de keten waar de PSM-Oplossing onderdeel van is.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

Opdrachtnemer accepteert en werkt hieraan mee; hiervoor is het nodig dat de Opdrachtnemer een Vrijwaringsverklaring af geeft.

Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.

Vereiste

53	Opdrachtnemer conformeert zich aan het meewerken aan een toets en hierboven, onder het kopje punt 9, **Inleiding** genoemde, beschreven werkwijze.

Vulnerability scans

Deze zijn bedoeld om geautomatiseerd te scannen op bekende Kwetsbaarheden. Een Vulnerability scan kan dus met een grote regelmaat worden uitgevoerd. De reden is dat aan de ene kant de PSM-Oplossing ge-update wordt en aan de andere kant hackers en beveiligingsonderzoekers constant op zoek zijn naar nieuwe Kwetsbaarheden.
Aanvullend kan de PSM-Oplossing tijdens het ontwikkelproces on-the-fly worden getest met daarvoor geschikte hulpmiddelen.

Vereisten:

54	Opdrachtnemer voert minimaal maandelijks een Vulnerability scan uit op de PSM-Oplossing conform bovenstaande. Hierbij geldt dat de gebruikte tooling, waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarhedendefinitiebestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de IDV Belastingdienst. Eventuele Kwetsbaarheden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan.
55	In aanvulling op **Fout! Verwijzingsbron niet gevonden.**1 geldt dat de gebruikte tooling t.b.v. het uitvoeren van een Jaarlijkse A&P test., waar Opdrachtnemer zelf in dient te voorzien, gebruik maakt van up-to-date kwetsbaarhedendefinitiebestanden. Op verzoek worden testresultaten, zeker als ze gekwalificeerd zijn als Kritisch of Hoog, gedeeld met de IDV Belastingdienst. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer conformeert zich hier aan.

56	Als Opdrachtgever het noodzakelijk acht, op basis van een risico inschatting, een Vulnerability scan uit te laten voeren op de PSM-Oplossing, dan staat Opdrachtnemer dat toe. De kosten van het uitvoeren van de Vulnerability scan worden gedragen door de Opdrachtgever. Eventuele Kwetsbaarheden worden als onderdeel van Onderhoud & Support opgelost. In overleg worden relevante acties opgenomen in het Verbeterplan. Opdrachtnemer conformeert zich hier aan.

Beveiligingstestbeleid

De Opdrachtgever wenst inzage in het beveiligingstestbeleid van Inschrijver. Het betreft opzet, bestaan en werking van de A&P-testen en Vulnerability scans. Hiertoe worden documenten aangeleverd waarin het beveiligingstestbeleid wordt beschreven en hoe eventuele tekortkomingen worden afgehandeld. Ook moet blijken onder welke omstandigheden dergelijke beveiligingstesten worden uitgevoerd en dat deze worden uitgevoerd**.** Hier maken ook voorbeelden van een A&P-testrapport en een Vulnerability testrapport deel van uit.

Vereiste

57	Inschrijver beschikt over een beveiligingstestbeleid dat in bovenstaande informatiebehoefte voorziet. Dit beveiligingstestbeleid wordt in de verificatieperiode bij de beste Inschrijver opgevraagd.

10. Continuïteit en continuïteitstesten

Opdrachtgever vindt het van belang te weten welke maatregelen getroffen zijn om eventuele onbeschikbaarheid te voorkomen én mocht onbeschikbaarheid toch groter zijn dan gepland, hoe snel de Gegevens beschikbaar zijn dan wel de PSM-Oplossing weer volledig operationeel kan zijn. Het gaat hierbij dus niet om de beschikbaarheidseisen waar het vooral draait om wanneer de PSM-Oplossing wel of niet te gebruiken is, maar om de excepties dat het mis gaat.

Calamiteit

Een Calamiteit kan optreden als de Productie-omgeving, of de Gegevens daarop, volledig onbeschikbaar worden. In een dergelijke situatie mag er geen sprake zijn van inbreuk op Integriteit en Vertrouwelijkheid van de Gegevens. Opdrachtnemer is hierop voorbereid door het opstellen van een Calamiteitenplan (Disaster Recovery Plan).

Het is noodzakelijk minimaal 1x per jaar een test uit te voeren om te controleren of de PSM-Oplossing naar aanleiding van gesimuleerde noodsituaties kan worden hersteld en daarna kan blijven functioneren, zoals overeengekomen.

Opdrachtnemer werkt mee aan het implementeren van eventuele verbeterpunten die van toepassing zijn op de PSM-Oplossing zelf.

Afspraken hierover worden in een DAP met de IDV Belastingdienst vastgelegd.

Vereiste

58	Opdrachtnemer conformeert zich aan bovenstaande alinea m.b.t. het uitvoeren en de uitkomsten van een Disaster Recovery Test.

11. Monitoring, Alerting & Logging

De Opdrachtgever wil zicht hebben op afwijkingen op de werking van de PSM-Oplossing om herstelacties te kunnen formuleren en zo mogelijk in de toekomst te voorkomen. Denk aan (ongeautoriseerde) toegang tot de PSM-Oplossing, maar ook inzage, wijziging of verwijdering van Gegevens. Speciale aandacht voor gevoelige Gegevens, zoals Persoonsgegevens. Ook, bijvoorbeeld, financiële Gegevens kunnen extra aandacht nodig hebben.

De PSM-Oplossing (inclusief raakvlaksystemen en tooling) wordt volcontinu gemonitord op verstoringen en beveiligingsinbreuken zodat er direct adequaat gereageerd kan worden op (beveiligings)incidenten. Er is een alertingproces ingericht om direct (prio 1) te kunnen handelen in geval van incidenten en (dreigende) verstoringen.

Excepties, zoals bijvoorbeeld in geval van blokkerende applicatieve fouten, worden gelogd. Beveiligingsinbreuken worden daarnaast gelogd voor forensisch onderzoek.

Inbreuken worden vastgelegd en acties worden genomen de ontstane risico’s te mitigeren.

Logregels bevatten minimaal:

- Datum en tijd;
- IP-adres of hostnaam van het device dat de informatie logt;
- IP-adres van het remote systeem (indien met een ander systeem wordt gecommuniceerd);
- Identificatie van de gebruiker of het proces;
- Beschrijving van de activiteit of gebeurtenis;
- Het resultaat van de activiteit of gebeurtenis.

Gebeurtenissen die gelogd moeten worden zijn:

- Authenticatie/autorisatie pogingen, inloggen en uitloggen;
- Acties die betrekking hebben op gebruikersprofielen, bestanden en databases of systeemservices;
- Transacties tussen systemen;
- Activatie en/of de-activatie van beveiligingsfunctionaliteit;
- Niet gespecificeerd gedrag van systemen en applicaties (uitzonderingen, fouten en storingen);
- Beveiligingsincidenten.

Logbestanden zijn beveiligd tegen ongeautoriseerde toegang/wijziging en zijn geschikt om forensisch onderzoek te verrichten. Logbestanden in het kader van technische beveiligingslogging worden minimaal 18 maanden bewaard. Logbestanden die onderdeel uitmaken van forensisch onderzoek naar een beveiligingsincident worden bewaard, zolang het onderzoek niet afgesloten is.

Logregels bevatten geen informatie waarmee de beveiliging van de PSM-Oplossing gecompromitteerd kan worden

Via alerting wordt direct adequaat gereageerd op excepties om de situatie te onderzoeken en eventuele risico's te mitigeren. Onder excepties vallen ook incidenten rond ongeautoriseerde toegang en wijziging van logbestanden.

Afspraken hiervoor moeten worden beschreven in een DAP met de IDV Belastingdienst.

Vereisten

59	De PSM-Oplossing voldoet aan de voorwaarden zoals beschreven in bovenstaande alinea's.
60	Opdrachtnemer levert op verzoek inzicht in de logging.
61	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald op minimaal 6 maanden en maximaal 18 maanden (voor bijvoorbeeld het SOC). Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
62	De IDV Belastingdienst dient de beschikking te krijgen over de logging. Zie ook 2.12 van https://intranet.belastingdienst.nl/iv-werkgebieden/files/2023/05/20200127-CTOO-Standaard-technische-beveiligingslogging-IV-v2.1-ondertekend.pdf
63	Voor forensisch onderzoek moet het mogelijk zijn om per gebruiker (wanneer nodig) te kunnen achterhalen wat (bestandnaam), wanneer en waar hij een bepaald document heeft afgedrukt. Deze functionaliteit is beperkt tot gebruikers met een specifieke rol.
64	De PSM-Oplossing ondersteunt het instellen van loglevels en onderscheidt hier minimaal info-, error- en fatal-meldingen in.
65	De PSM-Oplossing biedt de mogelijkheid om na een foutsituatie Gegevens te herstellen zodat de gebruiker zijn/haar werk kan hervatten.

12. Autorisatie & Authenticatie

Vereisten

66	Voor authenticatie sluit de PSM-Oplossing aan op SSOn Rijk via een SAMLv2/OpenID Connect aansluiting.

67	De communicatie over het netwerk van de wachtwoorden van gebruikers in relatie met de PSM-Oplossing is versleuteld.

Toegang tot PSM-Oplossing en Gegevens van de Aanbestedende dienst vindt plaats op basis van need-to-know en least privilege. Anders gezegd: gebruikers van zowel Opdrachtgever als Opdrachtnemer krijgen alleen die rechten die nodig zijn voor het uitoefenen van hun vastgestelde taken voor wat betreft Gegevens en functionaliteit van de PSM-Oplossing. Dit is overigens ook van toepassing op raakvlaksystemen (koppelende applicaties).

Een belangrijk aspect hierbij is dat de technische Beheerders geen toegang krijgen tot data in de Productieomgeving.

De PSM-Oplossing is technisch zodanig ingericht zodat deze principes zijn voldaan.

Vereiste

68	De PSM-Oplossing voldoet aan wat in bovenstaande alinea is beschreven.

Administratieve toegang tot PSM-Oplossing is beveiligd met MFA (Multi Factor Authenticatie) en waar gebruik gemaakt wordt van SSOn Rijk wordt een vergelijkbaar trust level afgedwongen. Indien de PSM-Oplossing een SSO-recovery procedure bevat (bijvoorbeeld waarmee SSO gedeactiveerd kan worden in geval van problemen met de SSO koppeling) is die ook voorzien van MFA.

Vereiste

69	De PSM-Oplossing bevat maatregelen om ongeautoriseerde toegang tot de PSM-Oplossing uit te sluiten.