Bijlage E2
Europese aanbesteding CKTO

Programma van Eisen – Informatiebeveiliging en Privacy

S V B voor het leven
Sociale Verzekeringsbank

Inhoudsopgave

1 Inleiding

In deze bijlage staan de Informatiebeveiligings- en privacy-eisen met betrekking tot de gevraagde dienstverlening beschreven. Voordat wordt ingegaan op deze eisen wordt kort de positie van informatiebeveiliging binnen de SVB geschetst. Dit is van belang omdat u als leverancier deel gaat uitmaken van de informatieketen van de SVB.

Het Programma van Eisen bevat eisen aan de uitvoering van de opdracht. De SVB beoogt dat de Opdrachtnemer, dus de leverancier die zich inschrijft (= hoofdaannemer), de verantwoordelijkheid draagt voor het uitvoeren van de opdracht conform de gestelde eisen. Oók als een onderaannemer (waaronder ook wordt verstaan een dochter of zusteronderneming) een deel van de opdracht uitvoert. Opdrachtnemer treedt op als hoofdaannemer indien zij een of meerdere onderaannemers inschakelt. Opdrachtnemer is te allen tijde verantwoordelijk voor de borging van de gestelde eisen en dient als aanspreekpunt voor de SVB tijdens de gevraagde dienstverlening.

1.1 Achtergrond

De belangrijkste doelstelling van de SVB bij het uitvoeren van de sociale verzekeringen en in de zorg is ervoor te zorgen dat alle uitkeringen rechtmatig en tijdig worden uitbetaald. Om deze doelstelling te realiseren maakt de SVB gebruikt van mensen, processen, middelen en vertrouwelijke en persoonlijke informatie, die zij uitwisselt met klanten en ketenpartners ten behoeve van het uitvoeren van haar dienstverlening.

De SVB onderkent haar rol in de Nederlandse samenleving en neemt haar verantwoordelijkheid om de belangen van haar klanten en stakeholders goed te beschermen, en het vertrouwen wat haar gegund is waar te maken. Informatiebeveiliging, bedrijfscontinuïteit, cyber weerbaarheid en privacy maken integraal deel uit van de wijze waarop de SVB opereert.

1.2 Informatiebeveiligingsprincipes

Als onderdeel van het SVB informatiebeveiligings en privacybeleid is een viertal informatiebeveiligingsprincipes vastgesteld welke de basis vormen voor de wijze waarop informatiebeveiliging, bedrijfscontinuïteit en privacy binnen de SVB worden vormgegeven:

I Wij **beschermen te allen tijde**, **de belangen van burgers** en andere stakeholders.

Wij zorgen dat we op ieder moment en op iedere plek in onze processen, de informatie van de burger op transparante en aantoonbare wijze beschermen en dat die informatie alleen toegankelijk is voor bevoegden, niet verloren kan gaan en/of ongewild wordt veranderd.

II Wij **gebruiken** alleen **informatie waarvoor** die **bedoeld** is en zijn daar transparant in.

Wij gebruiken de informatie van burgers niet voor andere zaken dan waar een rechtmatige grondslag voor is (zoals wettelijke grondslag of toestemming van de burger).

III Wij hebben **robuuste** en **betrouwbare processen en IT-systemen**.

Bij het ontwikkelen en het in standhouden van processen en IT-systemen, zorgen wij er voor dat er afdoende maatregelen zijn genomen, die het belang van deze processen en systemen waarborgen.

IV Wij zijn **voorbereid** op onverwachte **verstoringen** van **onze dienstverlening**.

Wij zien alle verstoring die zich voordoen en hebben de organisatie voorbereid (processen, middelen en vaardigheden) om daar op een adequate wijze mee om te gaan, zodat de belangen van de stakeholders gewaarborgd zijn.

Bovenstaande principes zijn dan ook direct van toepassing op de wijze waarop de Opdrachtnemer haar werkzaamheden dient uit te voeren en moeten integraal verwerkt zijn in de werkwijze en processen van de Opdrachtnemer.

1.3 Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van de SVB is gebaseerd op de NEN-ISO/IEC 27001 norm en de NEN-ISO/IEC 27002 best-practice. Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NENISO/ IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

De hoofdstukken 2 t/m 5 dienen ter verduidelijking van de eerder genoemde normen. In voorvallen waar de hoofdstukken 2 t/m 5 de genoemde normen afzwakken of tegenspreken prevaleren de genoemde normen altijd.

1.4 Wet- en regelgeving

De SVB is, onder meer, gehouden aan alle voorschriften uit relevante regelgeving waarbij de volgende wetten het meeste raakvlak hebben met informatiebeveiliging en privacy:

- AVG (Algemene Verordening Gegevensbescherming) – direct van toepassing op de leverancier.
- Wet en Regeling SUWI (Wet structuur uitvoeringsorganisatie werk en inkomen) – (onderdelen) alleen van toepassing indien expliciet opgenomen in dit programma van eisen.
- De BIO (Baseline Informatiebeveiliging Overheid). In het kader van ketenverantwoordelijkheid verwachten wij dit ook van Opdrachtnemers.

2 Eisen aan personeel van Opdrachtnemer

De Opdrachtnemer zet personeel in voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend. De volgende eisen worden met betrekking tot de medewerkers van de Opdrachtnemer gesteld.

Eis	*Omschrijving*
IBP-2.1	Alle medewerkers van Opdrachtnemer die participeren in de levering van de gevraagde dienstverlening moeten aantoonbaar bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn.
IBP-2.2	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een geheimhoudingsovereenkomst ondertekenen en hier naar handelen.
IBP-2.3	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de gevraagde dienstverlening een Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document, hebben die geldig is tijdens de duur van de uitvoering van de werkzaamheden.

3 Beveiliging van Diensten

3.1 Algemeen

Informatiebeveiliging moet als proces binnen de organisatie geborgd zijn om de informatie met de passende technische en organisatorische maatregelen te kunnen beveiligen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.1.1	De gevraagde dienstverlening moet opgezet en geleverd worden vanuit het basis principe “Secure-by-design” en "Privacy-by-design and default".
IBP-3.1.2	Opdrachtnemer heeft informatie-beveiliging en bedrijfscontinuïteit aantoonbaar gestandaardiseerd, gestructureerd en procesmatig in alle lagen van de organisatie en gevraagde dienstverlening ingericht, waarbij gericht wordt op continue verbetering.
IBP-3.1.3	De gevraagde dienstverlening moet adequaat zijn beveiligd door het implementeren en onderhouden van een set van technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening en de daarop opgeslagen en/of verwerkte informatie borgt.
IBP-3.1.4	Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de gevraagde dienstverlening. Dit dient periodiek toegepast te worden, minimaal binnen de 3-jaarlijkse cyclus en daarnaast ook altijd opnieuw bij significante wijzigingen.
IBP-3.1.5	Voor het uitvoeren van onderhoud en/of aanpassingen moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”) waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen.
IBP-3.1.6	Opdrachtnemer dient zorg te dragen dat software, welke gebruikt wordt als onderdeel van de gevraagde dienstverlening, altijd wordt ondersteund door de leverancier van de software. Indien software wordt geïmplementeerd binnen de SVB-infrastructuur zelf, dan dient deze in de desbetreffende werkomgeving te functioneren.
IBP-3.1.7	Voor zover de verantwoordelijkheid van Opdrachtnemer strekt voor de geleverde dienst aan de SVB, dient Opdrachtnemer de SVB voortdurend in staat te stellen om minimaal aan de eisen op niveau BBN-2 van de BIO te voldoen.
IBP-3.1.8	Opdrachtnemer treedt op als hoofdaannemer indien zij een of meerdere onderaannemers (waaronder een dochter of zusteronderneming) inschakelt. Opdrachtnemer is te allen tijde verantwoordelijk voor de borging van de overeengekomen eisen van de gevraagde dienstverlening en dient als aanspreekpunt voor de SVB.

3.2 Risicoanalyses

De wendbaarheid van de gevraagde dienstverlening komt voort uit de adequate wijze waarop risico’s worden beheerst waardoor het makkelijker is om op korte termijn risicogestuurde besluiten te nemen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.2.1	Opdrachtnemer heeft procedures om analyseren van risico's te borgen voor de gevraagde dienstverlening. De (opvolging van de) voor de SVB relevante (IB)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.

3.3 Logische toegangsbeveiliging

Logische toegangsbeveiliging richt zich op het administreren en beheren van gebruikers en resources inclusief toegangsrechten en toegangscontrole. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.3.1	De ingezette logische toegangsbeveiligingsmiddelen moeten betrouwbare en effectieve mechanismen leveren voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, en het controleerbaar maken van het gebruik van deze middelen.
IBP-3.3.2	De gevraagde dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is (“need to know”, “need to use”, “least privilege”) en ze hiervoor herleidbaar geautoriseerd zijn.
IBP-3.3.3	Opdrachtnemer is verantwoordelijk voor het periodiek controleren van de toegangsrechten van de eigen medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening en legt hierover verantwoording af als onderdeel van de periodieke rapportage.

3.4 Vulnerability management

Het tijdig informatie verkrijgen over technische kwetsbaarheden van de gebruikte informatiesystemen is van vitaal belang bij de beveiliging van de gevraagde dienstverlening. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor de mitigatie van de daarmee samenhangende risico’s. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.4.1	Er is een proces ingericht om kwetsbaarheden continu inzichtelijk te maken en adequaat en tijdig op te lossen op alle ICT componenten die behoren bij de gevraagde dienstverlening.
IBP-3.4.2	Voor in gebruik name van een nieuwe dienst / ICT component en bij een significante wijziging moet een kwetsbaarhedenscan uitgevoerd worden en moeten de bevindingen opgelost worden.
IBP-3.4.3	Opdrachtnemer rapporteert op hoofdlijnen periodiek over de voor de SVB relevante resultaten van de kwetsbaarhedenscans en de daarbij behorende (voorgestelde) mitigerende maatregelen.

3.5 Patch management

Patch management is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening systematisch voorzien worden van de vereiste patches. Het zorgt voor het verwerven, testen en installeren van patches. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.5.1	Opdrachtnemer moet procesmatig borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd en zorgt dat installatie van nieuwe patches geen afbreuk doet aan de

	continuïteit en beschikbaarheid, integriteit en vertrouwelijkheid van de gevraagde dienstverlening.
IBP-3.5.2	Opdrachtnemer rapporteert periodiek over de resultaten van het patch management proces en de daarbij behorende (eventuele) afwijkingen en/of risico's.

3.6 Security hardening

Security hardening is het proces dat ervoor zorgt dat alle componenten (ICT-systemen) ingezet voor de gevraagde dienstverlening op gestandaardiseerde wijze worden ingericht en structureel beheerd waarbij de insteek is om de veiligheidsrisico's zoveel mogelijk te elimineren. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.6.1	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening.
IBP-3.6.2	Bij het vaststellen en toepassen van de security hardening richtlijnen moet minimaal onderscheid gemaakt worden tussen de volgende ICT componenten: ▪ Applicaties; ▪ Middleware en databases; ▪ Platformen / infrastructuur; ▪ Netwerken; en ▪ Connectiviteit
IBP-3.6.3	Opdrachtnemer gebruikt voor de dienstverlening aan de SVB security hardening standaarden (zoals bijvoorbeeld de CIS-benchmarks) als basis voor het vaststellen van de security hardening richtlijn voor de ICT componenten.
IBP-3.6.4	Opdrachtnemer toetst periodiek alle ICT componenten op basis van de vastgestelde richtlijn en rapporteert de resultaten als onderdeel van de kwartaalrapportage. Geconstateerde afwijkingen worden hierin, na analyse, op basis van risico inschatting benoemd.

3.7 Penetratietesten

Met het uitvoeren van penetratietesten kan met een beperkte mate van zekerheid ingeschat worden in hoeverre de ICT componenten als onderdeel van de gevraagde dienstverlening kwetsbaar zijn voor inbraak. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.7.1	Opdrachtnemer heeft een procedure om bij significante wijzigingen (bijvoorbeeld in gebruikname nieuwe dienst/ICT componenten) in het kader van de gevraagde dienstverlening af te wegen of deze wijziging moet worden onderworpen aan een penetratietest. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
IBP-3.7.2	De SVB heeft het recht om een penetratietest uit te laten voeren om de beveiliging te testen in het kader van de gevraagde dienstverlening. De SVB kiest hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.

3.8 Beveiliging webapplicaties

Het beveiligen van webapplicaties heeft tot doel om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.8.1	Bij het ontwikkelen, implementeren en beheren van een webapplicatie moet gebruik gemaakt worden van Secure Software Development technieken om de beveiliging van de webapplicatie te borgen.
IBP-3.8.2	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid zodat de gevraagde dienstverlening voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties.
IBP-3.8.3	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid om de op basis van de OWASP top tien meest kritische beveiligingsrisico's binnen een webapplicatie te vermijden voor wat betreft de gevraagde dienstverlening.
IBP-3.8.4	In het kader van opslag en/of transport van persoonsgegevens moet de Oplossing van Opdrachtnemer voldoen aan de cryptografische beveiligingsvoorzieningen zoals voorgeschreven in de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS).

3.9 Infrastructurele beveiligingseisen

De doelstelling is te waarborgen dat de infrastructuur werkt zoals beoogd, ingericht is volgens specifieke beleidsuitgangspunten, en voldoet aan de eisen ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.9.1	De SVB hanteert een defense-in-depth strategie. Opdrachtnemer dient de SVB in staat te stellen onderbouwd aan te kunnen tonen dat bij de gevraagde dienstverlening daarbij aangesloten wordt.
IBP-3.9.2	De componenten die deel uitmaken van de gevraagde dienstverlening en de diensten die hierover aangeboden worden moeten worden beschermd tegen aanvallen op de beschikbaarheid, integriteit en vertrouwelijkheid.
IBP-3.9.3	In de ICT infrastructuur moeten signaleringsfuncties (registratie/logging en detectie) actief, efficiënt, effectief en beveiligd ingericht zijn.
IBP-3.9.4	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen, behorende bij de dienstverlening aan de SVB, moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd aan de SVB, als onderdeel van het informatiebeveiliging incidentenproces.
IBP-3.9.5	Indien voor de gevraagde dienstverlening gebruik gemaakt wordt van SVB-infrastructuur, dan moet deze alleen toegankelijk zijn via door de SVB goedgekeurde end-points en op de SVB goedgekeurde wijze.

3.10 Cloud

De veiligheid van de SVB gegevens is van kritiek belang bij het gebruik van dienstverlening die vanuit "de Cloud" wordt aangeboden, waarbij er in dezen vanuit wordt gegaan dat vertrouwelijke informatie en/of

persoonsgegevens onderdeel zijn van deze gegevens. Het is dan ook belangrijk om naast de al gestelde eisen, een aantal specifieke eisen voor Cloud leveranciers te stellen. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-3.10.1	Verwerking van data van de SVB moet uitsluitend plaatsvinden binnen de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland).
IBP-3.10.2	Alle koppelingen tussen applicaties (interoperabiliteit) moet op basis van open standaarden plaatsvinden en worden standaard via de SVB koppelpunten geleid.
IBP-3.10.3	Opdrachtnemer moet garanderen en aantonen dat de SVB gegevens logisch en functioneel gescheiden zijn van de overige afnemers.
IBP-3.10.4	De gevraagde dienstverlening biedt een oplossing om gegevens versleuteld in de cloud op te slaan waarbij gebruik gemaakt wordt van de geldende 'best practices' (afhankelijk van de stand der techniek) m.b.t. versleuteling.
IBP-3.10.5	De bij Opdrachtnemer gebruikte encryptiesleutels voor het encrypten van de data binnen de Oplossing moet op elk moment in het proces per direct ingetrokken of onbruikbaar kunnen worden gemaakt.
IBP-3.10.6	Opdrachtnemer zorgt ervoor dat in de gevraagde dienstverlening alle verwerkte gegevens (incl. relevante verbanden) en documenten exporteerbaar is in een gestructureerd en gangbaar bestandsformaat op zodanige wijze dat dit de SVB in staat stelt om de gegevens, verbanden en documenten zonder onredelijke inspanningen te transporteren naar een andere (met Opdrachtnemer vergelijkbare) dienstverlener.

4 Privacy

Zie bijlage E voor de privacy eisen.

5 Uitvoeringsaspecten

5.1 Beveiligingsincidenten en datalekken

Een beveiligingsincident is iedere handeling in strijd met het vastgestelde informatiebeveiligingsbeleid (van Opdrachtnemer en/of de SVB), of een gebeurtenis, met (mogelijk) nadelige gevolgen voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van systemen en/of informatie, die vallen onder de verantwoordelijkheid en/of het beheer van de SVB en/of Opdrachtnemer. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-5.1.1	Opdrachtnemer meldt datalekken direct en in ieder geval binnen 24 uur per e-mail bij de SVB Servicedesk, op het emailadres: servicedesk@svb.nl. Dit geldt ook voor andere informatiebeveiligingsincidenten voor zover het voor de dienstverlening van SVB van belang is om daarvan op de hoogte te zijn en/of om (samen met de leverancier) bij te dragen aan de oplossing.
IBP-5.1.2	Opdrachtgever heeft monitoring, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens) te detecteren, melden en de gevolgen daarvan te mitigeren.
IBP-5.1.3	Opdrachtnemer verleent medewerking bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot

	het incident (in het kader van de gevraagde dienstverlening) ter beschikking aan de SVB. De informatie dient minimaal 60 dagen na aanval nog beschikbaar te zijn. Deze informatie wordt ook beschikbaar gesteld bij eventueel onderzoek door een derde partij.

5.2 Controle en audits

Ter ondersteuning van de eisen die de SVB stelt aan haar Opdrachtnemer, moet gedurende de looptijd van het contract met de Opdrachtnemer een aantal controles en/of audits uitgevoerd worden. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-5.2.1	SVB heeft het recht om bij Opdrachtnemer een onderzoek (of audit) in te stellen met betrekking tot de naleving van de overeengekomen verplichtingen aangaande de gevraagde dienstverlening. SVB kan het onderzoek (minimaal één keer per jaar) zelf uitvoeren of laten uitvoeren door onafhankelijke deskundigen.
IBP-5.2.2	Minimaal jaarlijks levert Opdrachtnemer een recente formele auditverklaring die past bij de aard van de gevraagde dienstverlening (zoals een ISO27001:2017, of gelijkwaardig) op, die is afgegeven door een onafhankelijke gecertificeerde auditor en waarmee de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de gevraagde dienstverlening wordt aangetoond. In geval een 'gelijkwaardig' systeem voor informatiebeveiliging wordt geleverd, dient door de opdrachtnemer te worden toegelicht waarom het systeem gelijkwaardig is aan een gecertificeerd managementsysteem (comply or explain).

5.3 Overleg & rapportage

Als onderdeel van de besturing van de door Opdrachtnemer geleverde dienstverlening vindt regulier overleg plaats tussen de SVB en Opdrachtnemer en levert Opdrachtnemer periodiek rapportages op. De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Eis	*Omschrijving*
IBP-5.3.1	Opdrachtnemer stelt een vaste contactpersoon aan die voor de gevraagde dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-5.3.2	Gestructureerd en periodiek overleg tussen Opdrachtnemer en SVB moet plaatsvinden om zowel de informatiebeveiligingsrapportages als (eventuele) issues te bespreken.
IBP-5.3.3	Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen (comply or explain) en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de geleverde dienstverlening.
IBP-5.3.4	Periodiek moeten onderstaande rapportagevereisten worden ingevuld (specifiek voor de geleverde dienstverlening): • Een overzicht van de voor de SVB relevante beveiligingsincidenten (inclusief datalekken) inclusief trends, evaluaties en (root cause) analyses; • Rapportages van de voor de SVB relevante risico's, kwetsbaarheden (vulnerability scan resultaten), patch management, hardening afwijkingen en voortgangsrapportages over bijbehorende remediation plannen; en • Analyse van de voor de SVB relevante logging en monitoring informatie.
IBP-5.3.5	Jaarlijks moeten onderstaande rapportagevereisten worden ingevuld (specifiek voor de geleverde dienstverlening):

	▪ De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; ▪ Overzicht van afwijkingen ten opzichte van beleid of contract; en ▪ Overzicht van de risico acceptatie.

5.4 Behandeling van logdata

Met betrekking tot de behandeling van logdata dienen er afspraken gemaakt te worden tussen de SVB en de Opdrachtnemer. Afhankelijk van dienst die de SVB afneemt, gelden er de volgende eisen:

Eis	*Omschrijving*
IBP-5.4.1	Als de SVB gebruik maakt van een door de Opdrachtnemer geleverde en beheerde applicatie en/of dienst, dan dient de Opdrachtnemer de log-events met betrekking tot het gedrag van de SVB-gebruikers en de toegang en handeling op de SVB-data binnen die dienst en/of applicatie beschikbaar te stellen aan de SVB. Dit middels een nader overeen te komen timing, gangbaar format en overdrachtsmechanisme tussen de SVB en de Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.
IBP-5.4.2	Als de SVB eigen componenten (hardware, software en elke combinatie hiervan) plaatst in de door de Opdrachtnemer beheerde en aan SVB beschikbaar gestelde omgeving, dan dient de Opdrachtnemer alle log-events met betrekking tot deze SVB componenten aan de SVB beschikbaar te stellen. Dit middels een nader overeen te komen timing, gangbaar format en overdrachtsmechanisme tussen de SVB en de Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.