Sociale Verzekeringsbank
Bijlage A2 Programma van Eisen (PvE)

Informatiebeveiliging & Privacy

Aanbestedingsnummer: EA2023048

Inhoudsopgave

1 Inleiding

In deze bijlage staan de Informatiebeveiligings- & Privacy (IB&P) eisen met betrekking tot de geleverde oplossing/dienstverlening beschreven. Voordat wordt ingegaan op deze eisen wordt kort de positie van IB&P binnen de Sociale Verzekeringsbank (SVB) geschetst. Dit is van belang omdat u als dienstverlener deel gaat uitmaken van de informatieketen van de SVB.

Inschrijver dient elke pagina voor akkoord te paraferen en op de laatste pagina van deze bijlage, het kader volledig in te vullen en te voorzien van een origineel gescande handgeschreven handtekening.

1.1 Achtergrond

De belangrijkste doelstelling van de SVB bij het uitvoeren van haar taken m.b.t. de sociale verzekeringen en in de zorg is ervoor zorg te dragen dat alle uitkeringen rechtmatig en tijdig worden uitbetaald. Om deze doelstelling te realiseren maakt de SVB gebruik van mensen, processen, middelen en persoonlijke en/of vertrouwelijke 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 belanghebbenden 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 Informatiebeveiliging & Privacy (IB&P) principes

Als onderdeel van het SVB informatiebeveiliging- en privacybeleid zijn een viertal principes 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 burgers, medewerkers en andere stakeholders 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 we zijn daar transparant in.
Wij gebruiken de informatie van burgers en medewerkers niet voor andere zaken dan waar een wettelijke grondslag voor is (zoals de uitvoering van een publieke taak 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 ervoor dat er afdoende maatregelen zijn genomen, die het belang en de continuïteit van onze processen en systemen waarborgen.

IV Wij zijn **voorbereid** op onverwachte **verstoringen van onze dienstverlening**.
Wij zien alle verstoringen 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 Informatiebeveiliging & Privacybeleid

Het informatiebeveiliging & Privacybeleid van de SVB, hierna te noemen opdrachtgever, is gebaseerd op de laatste NEN-ISO/IEC 27001 norm en NEN-ISO/IEC 27002 best practices. Opdrachtnemer dient haar IB&P-beleid te baseren op de meest actuele versies van hiervoor genoemde standaarden of opvolgende c.q. gelijkwaardige normeringen.

1.4 Relevante wet- en regelgeving

De opdrachtgever is, onder meer, gehouden aan alle voorschriften uit relevante regelgeving waarbij de volgende wetten het meeste raakvlak hebben met Informatiebeveiliging en Privacy:

- **Van algemene aard** - Nederlandse wetgeving met bijbehorende jurisprudentie (AVG, Archiefwet, enz.).
- **Vanwege het uitvoeren van betalingen** - SWIFT.
- **Vanwege het klant zijn van DigiD** - DigiD-normenkader.
- **Vanwege het zijn van een zelfstandig bestuursorgaan (ZBO) -** Baseline Informatiebeveiliging Overheid (BIO), Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) en Forum voor Standaardisatie.

De hoofdstukken 2 t/m 6 dienen ter verduidelijking van de eerdergenoemde normen. In het geval waar de hoofdstukken 2 t/m 6 de genoemde normen afzwakken of tegenspreken prevaleren de genoemde normen.

1.5 Basisbeveiligingsniveau (BBN)

Binnen de Baseline Informatiebeveiliging Overheid (BIO) wordt op basis van generieke schade en bedreigingen voor de Rijksoverheid, een onderscheid gemaakt in drie basisbeveiligingsniveaus, ook wel BBN's genoemd. De BBN's bouwen voort op het vorige niveau. Dus hoe hoger het niveau, hoe hoger de potentiële impact en hoe meer c.q. stringentere maatregelen er geïmplementeerd dienen te worden.

De geleverde oplossing/dienstverlening dient minimaal geschikt te zijn om informatie te verwerken op beveiligingsniveau BBN2. BBN2 is van toepassing indien er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en wanneer de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

1.6 Categorisering eisen

In deze bijlage zijn de navolgende prefixen gebruikt ter categorisering van de eisen:

Prefix	Type eis
IBPA	Algemeen (generiek)
IBPB	T.a.v. het beheer (zowel bij intern, extern als gemeenschappelijk beheer)
IBPD	T.a.v. het ontwerp en/of de inrichting van de oplossing
IBPP	T.a.v. ingehuurd personeel

2 Generieke eisen ten aanzien van personeel van de opdrachtnemer

Inzet door de opdrachtnemer van personeel dient aan hieronder staande eisen te worden voldaan:

Eis	Omschrijving
IBPP-2.1	Opdrachtnemer is te allen tijde het primaire aanspreekpunt voor de opdrachtgever en draagt de volledige eindverantwoordelijkheid voor het nakomen en waarborgen van alle overeengekomen afspraken en verplichtingen met betrekking tot de oplossing/dienstverlening. Deze verantwoordelijkheid geldt onverminderd, ook indien de opdrachtnemer derden inschakelt, zoals onderaannemers of gelieerde partijen (bijvoorbeeld dochter- of zusterondernemingen).
IBPP-2.2	Medewerkers van de opdrachtnemer die in aanraking komen met vertrouwelijke informatie van de opdrachtgever dienen bij de opdrachtgever een geheimhoudingsovereenkomst (Non Discloser Agreement) te hebben ondertekend en op basis hiervan te handelen.
IBPP-2.3	Alle medewerkers van de opdrachtnemer die betrokken zijn bij de levering van de overeengekomen oplossing/dienstverlening, dienen te beschikken over een relevante, geldige Verklaring Omtrent Gedrag (VOG) of een gelijkwaardig document, dat aantoonbaar niet ouder is dan 36 maanden op het moment dat zij met de werkzaamheden starten. De opdrachtnemer draagt zorg voor het aanvragen, actualiseren en administreren van deze documenten, inclusief het bewaren en verstrekken van kopieën indien de opdrachtgever hierom vraagt. De kosten van de VOGs en de administratie hieromtrent zijn volledig voor de voor rekening van de opdrachtnemer.
IBPP-2.4	Medewerkers van de opdrachtnemer dienen bij het betreden van locaties van de opdrachtgever zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs.
IBPP-2.5	Medewerkers die namens of in opdracht van de opdrachtnemer betrokken zijn bij de levering van de oplossing/dienstverlening, dienen volledig op de hoogte te zijn van de voor hun werkzaamheden relevante contractuele afspraken en verplichtingen met betrekking tot informatiebeveiliging en privacy, zoals vastgelegd in de overeenkomst tussen opdrachtgever en opdrachtnemer. De opdrachtnemer is verantwoordelijk voor het waarborgen dat deze medewerkers adequate training en instructies hebben ontvangen over deze afspraken en verplichtingen, en dat zij deze begrijpen en naleven.
IBPP-2.6	Opdrachtnemer dient vastgelegd te hebben wat de rollen, taken en verantwoordelijkheden van haar medewerkers zijn op het gebied van Informatiebeveiliging en Privacy in relatie tot de geleverde oplossing/dienstverlening.
IBPP-2.7	Medewerkers van de opdrachtnemer en eventuele onderaannemers die betrokken zijn bij de levering van de oplossing/dienstverlening, dienen een relevante bewustzijnsopleiding en/of -training te hebben gevolgd met betrekking tot organisatiebeleid en procedures op het gebied van informatiebeveiliging, privacy, en andere voor hun functie relevante onderwerpen. Deze training moet passend zijn voor de specifieke functie of rol van de medewerker en toegespitst zijn op de risico's en verantwoordelijkheden die horen bij hun bijdrage aan de oplossing/dienstverlening.

3 Generieke eisen ten aanzien van Informatiebeveiliging (IB)

3.1 Algemeen

Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van data / informatie en heeft tot doel om informatie met passende maatregelen te beschermen / beveiligen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.1.1	De geleverde oplossing/dienstverlening dient gedurende de gehele looptijd van de overeenkomst te voldoen aan de op de opdrachtgever van toepassing zijnde wet- en regelgeving, waaronder de AVG (Algemene Verordening Gegevensbescherming) en de Cyberbeveiligingswet (Cbw) op het moment dat die van kracht wordt. De Cbw is de Nederlandse wetgeving die is gebaseerd op de NIS2 (Europese wetgeving m.b.t. Network and Information Security). De opdrachtgever kan in dit kader nadere eisen stellen.
IBPA-3.1.2	De geleverde oplossing/dienstverlening dient adequaat te zijn beveiligd door middel van een set van beveiligingsmaatregelen die gebaseerd zijn op internationaal erkende normen, zoals ISO 27001 en/of de NIST Cybersecurity Framework. Deze maatregelen moeten de beschikbaarheid, integriteit en vertrouwelijkheid van de oplossing waarborgen, inclusief alle betrokken ICT-componenten en de informatie die daarop wordt opgeslagen of verwerkt. Beveiligingsmaatregelen dienen onder andere, maar niet uitsluitend, de volgende aspecten te omvatten: * Toegangsbeheer; * Cryptografie; * Patchmanagement; * Logging en monitoring; * Back-up en recovery.
IBPA-3.1.3	De geleverde oplossing/dienstverlening mag uitsluitend (software)componenten bevatten die op het moment van levering actief worden ondersteund door de fabrikant(en) of de eigenaar van de broncode. Dit houdt in dat de fabrikant of eigenaar regelmatig updates, bugfixes en beveiligingspatches verstrekt, en dat deze ondersteuning gegarandeerd is gedurende de volledige contractperiode. Indien een component niet langer wordt ondersteund gedurende de contractperiode, is de opdrachtnemer verplicht deze tijdig te vervangen door een ondersteund alternatief, zonder extra kosten voor de opdrachtgever.
IBPA-3.1.4	(Eventueel) betrokken gegevens bij de realisatie van een oplossing/dienstverlening en in het bijzonder persoonsgegevens dienen zorgvuldig te zijn gekozen, te worden beschermd en vernietigd indien niet meer noodzakelijk.
IBPA-3.1.5	De opdrachtnemer is verantwoordelijk voor het vaststellen, documenteren en implementeren van duidelijke gebruiksregels met betrekking tot het veilige gebruik van informatie, bedrijfsmiddelen en faciliteiten die verband houden met de geleverde dienstverlening. De opdrachtnemer dient de gebruiksregels beschikbaar te stellen aan alle betrokken medewerkers en onderaannemers, en ervoor te zorgen dat deze worden nageleefd.

Eis	Omschrijving
IBPA-3.1.6	Opdrachtnemer dient ervoor te zorgen dat met betrekking tot haar kantoren, ruimten en/of faciliteiten en thuiswerkplekken, zover als betrokken bij de dienstverlening, passende beveiligingsmaatregelen zijn geïmplementeerd.
IBPD-3.1.7	De opdrachtnemer dient de opdrachtgever te informeren en gedetailleerde documentatie te verstrekken waarin wordt uitgelegd hoe in de aangeboden oplossing/dienstverlening is voldaan aan de basisprincipes '***Security by Design***' en '***Security by Default***'. Deze documentatie moet de volgende onderdelen bevatten: *'Security by Design'* Een beschrijving van hoe beveiliging vanaf de eerste fase van het ontwerp en de ontwikkeling van de applicaties en/of systemen is geïntegreerd. Dit omvat: * Risicoanalyse: Hoe beveiligingsrisico's in kaart zijn gebracht en geadresseerd tijdens het ontwerp en de ontwikkeling. * Beveiligingseisen: Specifieke beveiligingseisen die zijn opgenomen in de technische architectuur, zoals encryptie, toegangsbeheer en netwerkbeveiliging. * Veilige ontwikkelprocessen: Beschrijving van de ontwikkelmethodologieën en -praktijken (zoals secure coding practices, code reviews en geautomatiseerde beveiligingstests) die zijn toegepast om kwetsbaarheden tijdens de ontwikkeling te minimaliseren. * Penetratietesten en kwetsbaarheidsbeoordelingen: Informatie over welke beveiligingstests en -audits zijn uitgevoerd, inclusief de resultaten en hoe kwetsbaarheden zijn verholpen. *'Security by Default'* Een gedetailleerde uitleg van hoe de standaardinstellingen van de applicaties en/of systemen zijn geconfigureerd om de best mogelijke beveiliging te bieden, zonder dat gebruikers extra maatregelen hoeven te nemen. Dit omvat: * Standaardbeveiligingsinstellingen: Welke instellingen standaard zijn ingeschakeld (bijv. standaard versleuteling, toegangscontroles en logging) en hoe deze de vertrouwelijkheid, integriteit en beschikbaarheid van de oplossing/dienstverlening beschermen. * Minimale toegangsrechten: Toepassing van het "least privilege"-principe, waarbij gebruikers en systemen standaard de minimale toegangsrechten krijgen die nodig zijn om hun taken uit te voeren. * Configuratiebeperkingen: Beperkingen die zijn ingesteld om te voorkomen dat gebruikers of beheerders de beveiliging per ongeluk verlagen, zoals het voorkomen van het uitschakelen van beveiligingsfuncties of het beperken van toegang tot risicovolle configuraties. * Automatische updates en patchmanagement: Hoe de oplossing/dienstverlening is ingericht om automatisch updates en beveiligingspatches te ontvangen en te implementeren zonder handmatige interventie.
IBPD-3.1.8	De geleverde oplossing/dienstverlening dient gevoelige en/of vertrouwelijke gegevens '***in transit***' en '***at rest***' te versleutelen op basis van algemeen geaccepteerde best practices en in lijn met de adviezen van het Nationaal Cyber Security Centrum (NCSC).

Eis	Omschrijving
IBPD-3.1.9	De geleverde oplossing/dienstverlening dient bij gebruik van encryptiesleutels en/of certificaten ervoor zorg te dragen dat het gebruik voor de opdrachtgever inzichtelijk is, en dat het per direct intrekken of onbruikbaar maken van encryptiesleutels en/of certificaten mogelijk is.
IBPB-3.1.10	Opdrachtnemer dient voor het onderhoud en/of doorvoeren van aanpassingen met betrekking tot de geleverde oplossing/dienstverlening een wijzigingsproces te hebben en te hanteren, waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen en/of onderbrekingen tijdens het doorvoeren van veranderingen.
IBPB-3.1.11	Opdrachtnemer dient Informatiebeveiliging en bedrijfscontinuïteit gestandaardiseerd, gestructureerd en gebaseerd op een cyclus van continue verbeteren in alle lagen van de organisatie en de geleverde oplossing/dienstverlening te hebben ingericht.
IBPB-3.1.12	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben voor het veilig beheren en aanbieden van de oplossing/dienstverlening.
IBPB-3.1.13	Opdrachtnemer dient procedures te hebben, uit te voeren en over de resultaten te rapporteren met betrekking tot het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de geïmplementeerde maatregelen ter beveiliging van de geleverde dienstverlening. Dit dient periodiek, minimaal iedere 3 jaar, en daarnaast ook altijd opnieuw bij significante wijzigingen te gebeuren.
IBPB-3.1.14	Opdrachtnemer dient de continuïteit van de geleverde oplossing/dienstverlening te waarborgen in geval van calamiteiten en/of rampen. Opdrachtnemer zorgt in dit kader voor back-up en restoremogelijkheden zodat er maximaal 24 uur dataverlies kan optreden en de oplossing niet langer dan 44 uur niet beschikbaar is. Leverancier is verantwoordelijk voor controle van de integriteit van die back-ups, alsmede het waarborgen van de vertrouwelijkheid en beschikbaarheid daarvan. De eisen voor de Productie omgeving zijn: Recovery Point Objective = 24 uur Recovery Time Objective = 44 uur
IBPD-3.1.15	De opdrachtnemer dient aan de opdrachtgever inzicht te geven in de toegepaste Security Architectuur (SA) van de aangeboden oplossing/dienstverlening.

3.2 Risicoanalyses

Risicoanalyses hebben tot doel om alle mogelijk relevante dreigingen / risico's en gevolgen in kaart te brengen. Een risico is niet direct een gevaar, maar kan dit in de toekomst wel worden. Eventueel kunnen op basis van de uitkomsten van een risicoanalyse mitigerende maatregelen worden geïmplementeerd om de kans en/of de impact van het optreden van een risico te beperken. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.2.1	Opdrachtnemer dient actief mee te werken aan het inzichtelijk maken en het mitigeren van risico's welke samenhangen met de oplossing.

Eis	Omschrijving
IBPA-3.2.2	Opdrachtnemer dient structureel risicoanalyses uit te voeren in het bouw- en implementatietraject, bij grote onderhoudstrajecten en bij significante wijzigingen in de geleverde oplossing / dienstverlening.
IBPA-3.2.3	Opdrachtnemer dient aantoonbaar onderkende risico's vast te leggen voorzien van de geplande mitigerende maatregelen inclusief een verwachte implementatie / oplosdatum en actiehouder.
IBPB-3.2.4	Opdrachtnemer dient conform afspraken in de overeenkomst te rapporteren over de status van de onderkende risico's en de bijbehorende voortgang van de geplande te implementeren mitigerende maatregelen.
IBPB-3.2.5	Opdrachtnemer dient opdrachtgever op de hoogte te stellen, via het overeengekomen communicatiekanaal en tijdslijnen, van risico's die een directe impact op de opdrachtgever (kunnen) hebben.

3.3 Logische toegangsbeveiliging

Logische toegangsbeveiliging heeft tot doel de toegang tot data / informatie, IT-voorzieningen en bedrijfsprocessen op grond van de bedrijfsbehoeften en Informatiebeveiligings- en Privacy te beheersen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.3.1	De geleverde oplossing/dienstverlening dient te beschikken over passende, betrouwbare en effectieve mechanismen, gebaseerd op algemeen geaccepteerde standaarden, ten aanzien van identificatie, authenticatie, autorisatie en verantwoording / controle (IAAA).
IBPD-3.3.2	De geleverde oplossing/dienstverlening dient aan te sluiten op de aanwezige directory service (Microsoft Active Directory (AD)) van de opdrachtgever waarbij de opdrachtgever altijd eindverantwoordelijk blijft voor het vaststellen van de gedeelde attributen. Indien aansluiting niet mogelijk is dient dit formeel geaccepteerd te worden door de opdrachtgever.
IBPD-3.3.3	De geleverde oplossing/dienstverlening dient voor authenticatie Multi-factor authenticatie (MFA) en single sign-on (SSO) op basis van standaard protocollen (bv. OAUTH2, SAML, etc.) te ondersteunen.
IBPD-3.3.4	De geleverde oplossing/dienstverlening dient zo ingericht te zijn dat gebruikers alleen toegang hebben tot gegevens voor zover dat voor de uitoefening van hun taken noodzakelijk is (autorisatie principes '***least privilege***', '***need-to-know***', '***need-to-use***' en '***Separation of duties***') en dat toegang c.q. activiteiten altijd herleidbaar zijn tot één uniek persoon.
IBPD-3.3.5	De opdrachtnemer mag alleen door de opdrachtgever goedgekeurde autorisatiematrices implementeren.
IBPB-3.3.6	Opdrachtnemer dient beleid en ondersteunende (beveiligings-)maatregelen te hebben geïmplementeerd om de veiligheid te kunnen garanderen van gegevens die wordt benaderd, verwerkt en/of opgeslagen in opdracht van de opdrachtgever.

3.4 Security hardening

Security hardening heeft tot doel om de kwetsbaarheid van ICT-componenten te reduceren / minimaliseren en daarmee het aanvalsoppervlak te verkleinen. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPD-3.4.1	Hardening met betrekking tot de geleverde oplossing/dienstverlening dient in geval van uiteindelijk beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen plaats te vinden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld de CIS-benchmarks) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.4.2	Opdrachtnemer dient volgens een beschreven en geïmplementeerd Security hardening beleid en proces de hardening van alle ICT-componenten die betrokken zijn bij de geleverde oplossing te controleren en/of uit te voeren en gepaste maatregelen te nemen op basis van geconstateerde bevindingen.

3.5 Vulnerability Management

Vulnerability Management heeft tot doel om middels scanning inzicht te krijgen in de (technische) kwetsbaarheden van de gebruikte ICT-componenten binnen de IT-infrastructuur om op basis van deze informatie mitigerende maatregelen te kunnen nemen ter beperking van de risico's. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.5.1	Vulnerability Management met betrekking tot de geleverde oplossing/dienstverlening dient in geval van beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.5.2	Opdrachtnemer dient voor in gebruik name van een nieuwe of significante aanpassing op de oplossing/dienstverlening een kwetsbaarheidsscan uit te voeren en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.5.3	Opdrachtnemer dient volgens een beschreven en geïmplementeerd Vulnerability Management beleid en proces met een gepaste frequentie kwetsbaarheidsscans uit te voeren op alle ICT-componenten die betrokken zijn bij de geleverde oplossing/dienstverlening en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.

3.6 Lifecycle en Patch Management

Lifecycle en Patch Management heeft tot doel de laatste (beveiligings-)patches en updates voor componenten in de IT-infrastructuur te verwerven, testen en uit te rollen met minimale verstoring van het productieproces. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.6.1	Lifecycle en Patch Management met betrekking tot de geleverde oplossing/dienstverlening dient in geval van beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPB-3.6.2	Opdrachtnemer dient volgens een beschreven Patch Management beleid en proces met een gepaste frequentie (beveiligings-) patches en updates door te voeren op alle ICT-componenten die betrokken zijn bij de geleverde oplossing/dienstverlening.
IBPB-3.6.3	Opdrachtnemer dient ervoor te zorgen dat alle bij de oplossing/dienstverlening betrokken ICT-componenten voorzien zijn van de laatste (beveiligings-)patches en updates en dient indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBPB-3.6.4	Opdrachtnemer dient bij beschikbaarheid van een (beveiligings-)patch en updates, voorafgaand aan de implementatie, de implementatierisico's te beoordelen en de patch of update te testen op een niet productieomgeving alvorens deze in productie door te voeren.
IBPB-3.6.5	Opdrachtnemer dient indien geen (beveiligings-)patch c.q. update beschikbaar is gepaste mitigerende maatregelen te implementeren opdat het restrisico tot een acceptabel niveau wordt teruggebracht.

3.7 Penetratietesting

Het doel van penetratietesting (binnendringingstesten) is om te toetsen of een applicatie, component of infrastructuur kwetsbaarheden heeft en of het ook mogelijk is deze kwetsbaarheden te misbruiken. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen.

Eis	Omschrijving
IBPA-3.7.1	Penetratietesting met betrekking tot de geleverde oplossing/dienstverlening dient in geval van beheer door de opdrachtgever aan te sluiten op haar beleid en processen en in alle andere gevallen ingericht te zijn c.q. uitgevoerd te worden op basis van een onafhankelijk toetsbare internationale standaard (zoals bijvoorbeeld OWASP) welke tevens compliant is met de laatste versie van de BIO waaraan de opdrachtgever moet voldoen.
IBPA-3.7.2	Opdrachtgever heeft het recht om te allen tijde een penetratietest uit te laten voeren, door een door haar te bepalen onafhankelijke derde partij, met betrekking tot de geleverde oplossing/dienstverlening waar de opdrachtnemer medewerking aan dient te verlenen.
IBPB-3.7.3	Opdrachtnemer dient volgens een beschreven Penetratietesting beleid en proces penetratietest uit te laten voeren door een externe partij op alle ICT-componenten van de geleverde oplossing/dienstverlening.
IBPB-3.7.4	Opdrachtnemer dient voor in gebruik name van een nieuwe dienst / ICT-component of bij een significante wijziging daarvan, maar minimaal jaarlijks, een penetratietest uit te (laten) voeren en geconstateerde relevante bevindingen te mitigeren c.q. op te lossen.
IBPB-3.7.5	Opdrachtnemer dient conform afspraken in de overeenkomst te rapporteren over de uitgevoerde penetratietesten inclusief de status van de opvolging / afhandeling van de geconstateerde bevindingen.

3.8 Infrastructuur

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. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.8.1	De geleverde oplossing/dienstverlening dienen op een gepaste wijze te worden beschermd tegen aanvallen op de gebieden beschikbaarheid, integriteit en vertrouwelijkheid.
IBPD-3.8.2	De opdrachtnemer informeert de opdrachtgever ter beoordeling over hoe binnen de aangeboden oplossing/dienstverlening invulling is gegeven aan het concept ‘Defense in depth’ door de inrichting van meerdere beveiligingslagen en/of maatregelen (lees toegepaste preventieve, detectieve en/of correctieve maatregelen).
IBPD-3.8.3	De geleverde oplossing/dienstverlening dient efficiënte, effectieve, beveiligde en knoeivrije / niet muteerbare signaleringsfuncties (registratie / logging en detectie) te hebben.
IBPD-3.8.4	De geleverde oplossing/dienstverlening dient audit / logbestanden minimaal 15 maanden te bewaren voor toekomstig onderzoek en toegangscontrole.

Eis	Omschrijving
IBPD-3.8.5	De geleverde oplossing/dienstverlening dient alleen toegankelijk te zijn voor door de opdrachtgever geautoriseerde personen en/of partijen.
IBPD-3.8.6	De geleverde oplossing/dienstverlening dient de mogelijkheid van afluisteren van netwerkverbindingen en/of het wijzigen van datastromen te verhinderen gebruikmakend van algemeen geaccepteerde best practices.
IBPD-3.8.7	Opdrachtnemer dient gebruik te maken van een veilige ontwikkel- en integratieomgeving ter beheersing van de ontwikkeling c.q. de aanpassing van informatiesystemen.
IBPB-3.8.8	Opdrachtnemer dient loggings- en detectie-informatie (registraties en alarmeringen) en de beveiligingsstatus van ICT-componenten actief te monitoren (bewaking en analyse) en eventuele bevindingen te rapporteren en op te volgen volgens een proces.
IBPB-3.8.9	Opdrachtnemer dient media en/of ICT-componenten gerelateerd aan de oplossing/dienstverlening middels een formele procedure op een veilige manier te verwijderen / af te voeren.

3.9 Cloud en/of External Service Provider (ESP)

De veiligheid van de data / informatie is van essentieel belang bij het gebruik van oplossing die vanuit de cloud en/of door een ESP wordt aangeboden. Het is dan ook belangrijk om naast de al gestelde eisen, een aantal specifieke eisen hieromtrent op te nemen. Het geleverde dient minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-3.9.1	Opdrachtnemer dient te waarborgen dat opdrachtgever te allen tijde eigenaar blijft van haar data en tevens haar verantwoordelijkheden als eigenaar kan blijven uitoefenen in alle fases van de data-lifecycle.
IBPD-3.9.2	De geleverde oplossing/dienstverlening dient logisch en functioneel gescheiden te zijn van mogelijk andere afnemers / klanten. Dit betekent onder andere zonder afhankelijkheden in geval van onderhoud en releasewerkzaamheden en/of in geval van een technische uitwijk.
IBPD-3.9.3	De geleverde oplossing/dienstverlening dient voor de gebruiker en het beheer van de digitale identiteit en de toegangsrechten zo ingericht te zijn zodat transparant is waar deze wordt gehost.
IBPD-3.9.4	De geleverde oplossing/dienstverlening dient in het kader van dataportabiliteit voorzieningen te hebben voor het exporteren van data in een algemeen gangbaar formaat (lees XML, CSV, enz.) inclusief datamodel. In geval van beëindiging van de overeenkomst dient data van de opdrachtgever welke nog in het bezit is van de opdrachtnemer na overdracht aan de opdrachtgever vervolgens op verzoek van de opdrachtgever conform daarvoor geldende internationale standaarden vernietigd te worden.
IBPD-3.9.5	De geleverde oplossing/dienstverlening dient ervoor zorg te dragen dat aangeleverde documenten tijdens het gebruik, in lijn met de retentie-policy van de opdrachtgever, altijd in het aangeleverde formaat beschikbaar blijven.

Eis	Omschrijving
IBPD-3.9.6	De geleverde oplossing/dienstverlening dient elke koppeling tussen applicaties / services en ICT-componenten in te richten op basis van algemeen geaccepteerde standaarden waarbij uitwisselingen tussen verschillende security domeinen verloopt via gedefinieerde koppelpunten van de opdrachtgever.
IBPB-3.9.7	Opdrachtnemer dient op verzoek van de opdrachtgever specifieke (log)data te leveren aan de (externe) Security Operations Center (SOC) en Management Operations Center (MOC) functie van de opdrachtgever.
IBPB-3.9.8	Opdrachtnemer dient voor voorspelbare beveiligingsincidenten (lees bijvoorbeeld malware-uitbraken en ((distributed) denial-of-service attacks ((D)DoS)) standaard periodiek geteste scenario's / playbooks beschikbaar te hebben welke per direct kunnen worden geactiveerd.

3.10 Webapplicaties

Het beveiligen van webapplicaties heeft tot doel om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van en voldoen aan de eisen die door de opdrachtgever zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPD-3.10.1	De geleverde oplossing/dienstverlening dient qua standaarden en technische specificaties te voldoen aan de standaarden zoals opgesteld door het World Wide Web Consortium (W3C), dan wel de logische opvolgers daarvan.
IBPD-3.10.2	De geleverde oplossing/dienstverlening dient qua (cryptografische) beveiligings-maatregelen te voldoen aan de NCSC-beveiligingsrichtlijnen, dan wel de logische opvolger daarvan.
IBPD-3.10.3	De geleverde oplossing/dienstverlening dient aantoonbaar geen kwetsbaarheden / kritische beveiligingsrisico's te bevatten zoals beschreven in de meest recente OWASP top 10.
IBPA-3.10.4	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben en te hebben geïmplementeerd voor het veilig ontwikkelen van software / (web)applicaties en systemen welke onderdeel uit maken van de geleverde oplossing/dienstverlening.
IBPA-3.10.5	Opdrachtnemer dient bij het ontwikkelen van (web)applicaties betrokken bij de geleverde oplossing/dienstverlening gebruik te maken van Secure Software Development (SSD) methodiek om de Informatiebeveiligings- en Privacyaspecten te borgen.
IBPA-3.10.6	Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben voor het veilig beheren en aanbieden van software / (web)applicaties welke onderdeel uitmaakt van de geleverde oplossing/dienstverlening.

4 Generieke eisen ten aanzien van Privacy (P)

De AVG beschermt de grondrechten en de fundamentele vrijheden van levende natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit hoofdstuk worden niet de eisen herhaald die al zijn beschreven in de voorgaande hoofdstukken. Het geleverde dient additioneel op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-4.1	De geleverde oplossing/dienstverlening dient op het gebied van Informatiebeveiliging en Privacy maatregelen te hebben geïmplementeerd, op basis van een aantoonbaar uitgevoerde (Data) Privacy Impact Assessment ((D)PIA), passend bij de soort persoonsgegevens die worden verwerkt en in lijn met algemeen geaccepteerde standaarden.
IBPD-4.2	De opdrachtnemer informeert de opdrachtgever ter beoordeling over hoe binnen de aangeboden oplossing/dienstverlening invulling is gegeven aan de basisprincipes '***Privacy by Design',*** '***Privacy by Default***', '***Data Protection by Design***', '***Data Protection by Default***' en '***Data (collection and processing) minimalization***'.
IBPD-4.3	De geleverde oplossing/dienstverlening dient mogelijkheden te bieden om te allen tijde te voldoen aan verzoeken in het kader van de rechten van betrokkenen.
IBPD-4.4	De geleverde oplossing/dienstverlening dient mogelijkheden te bieden om aan personen gerelateerde gegevenselementen die niet of niet meer noodzakelijk zijn voor (latere) verwerkingen of waarvoor geen doelbinding / rechtsgrond meer aanwezig is te verwijderen.
IBPD-4.5	De geleverde oplossing/dienstverlening dient mogelijkheden te bieden om aan de data gerelateerde retentie-policies zelfstandig in te regelen of in te laten regelen.
IBPD-4.6	De geleverde oplossing/dienstverlening dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan binnen de Europese Economische Ruimte (EER). Tevens dienen de eventuele (privacy) restrisico's tot binnen de Risk Tolerance van de opdrachtgever gereduceerd te zijn. Dit geldt ook voor eventuele back-ups!
IBPA-4.7	De locatie van de geleverde oplossing/dienstverlening en de daarbij betrokken medewerkers dienen zich binnen de Europese Economische Ruimte (EER) te bevinden.
IBPA-4.8	In de geleverde oplossing/dienstverlening dient bij de verwerking van persoonsgegevens, zonder de uitdrukkelijke schriftelijke voorafgaande toestemming van de opdrachtgever, geen gebruik te worden gemaakt van subverwerkers.
IBPA-4.9	Opdrachtnemer dient een geïmplementeerd privacybeleid te hebben met daarin de doelstellingen, rollen en verantwoordelijkheden met betrekking tot privacy welke in overstemming zijn met van toepassing zijnde wet- en regelgeving en in lijn met algemeen geaccepteerde privacy principes.
IBPB-4.10	Voorafgaand aan in productie name van de geleverde oplossing/dienstverlening dient een verwerkersovereenkomst afgesloten te zijn tussen de opdrachtgever als verwerkingsverantwoordelijke en de opdrachtnemer als verwerker indien er persoonsgegevens worden verwerkt door de opdrachtnemer.
IBPB-4.11	Opdrachtnemer dient de van opdrachtgever ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de opdrachtgever te verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeenkomen.

Eis	Omschrijving
IBPA-4.12	Opdrachtnemer dient bij beëindiging van de dienstverlening de voor de opdrachtgever verwerkte persoonsgegevens te retourneren dan wel op verzoek van de opdrachtgever te vernietigen, tenzij er sprake is van een wettelijke bewaarplicht.
IBPB-4.13	Opdrachtnemer dient een proces te hebben en te hebben geïmplementeerd om datalekken onverwijld, maar uiterlijk binnen 24 uur, aan de opdrachtnemer te melden.
IBPB-4.14	Opdrachtnemer dient opdrachtgever op verzoek te allen tijde te ondersteunen bij de uitoefening van de rechten van betrokkenen en/of de opvolging of afhandeling van datalekken.
IBPB-4.15	Opdrachtnemer dient de opdrachtgever onverwijld, maar uiterlijk binnen 24 uur, over verzoeken tot aanlevering van (persoons)gegevens door buitenlandse inlichtingen- en opsporingsdiensten in het kader van de geleverde dienstverlening te informeren.

5 Generieke eisen ten aanzien van uitvoeringsaspecten

5.1 Beveiligingsincidenten

Een security of privacy incident is iedere handeling in strijd met het vastgestelde informatiebeveiligings- en/of privacybeleid van de opdrachtnemer, of een gebeurtenis, met (mogelijk) nadelige gevolgen voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van systemen en/of data / informatie, die vallen onder de verantwoordelijkheid en/of het beheer van de opdrachtnemer. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.1.1	Alle bij de oplossing/dienstverlening betrokken medewerkers dienen een informatiebeveiligings- en/of privacy incident onmiddellijk volgens de standaardprocedure te melden en in ieder geval per mail bij de Servicedesk van de opdrachtgever, op het emailadres: ICT.Servicedesk@svb.nl.
IBPB-5.1.2	Opdrachtnemer dient bij een informatiebeveiligings- en/of privacy incident zo snel als mogelijk passende maatregelen te treffen om de gevolgen en de schade voor alle betrokkenen te beperken en/of te voorkomen.
IBPB-5.1.3	Opdrachtnemer dient te allen tijde volledige medewerking te verlenen bij het onderzoeken en oplossen van informatiebeveiligings- en/of privacy incidenten en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan de opdrachtgever.

5.2 Compliance

Ter ondersteuning van de eisen die de opdrachtgever stelt aan haar opdrachtnemer, moet gedurende de looptijd van de overeenkomst met de opdrachtnemer een aantal controles en/of audits uitgevoerd worden. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.2.1	Opdrachtnemer dient de opdrachtgever het recht te verlenen om een onderzoek (of audit) in te stellen met betrekking tot de naleving van het ***'Beschrijvend document'***, ***'De overeenkomst van Opdracht'*** en de ***'Bijlagen opgenomen verplichtingen aangaande de geleverde dienstverlening'***. De audit wordt altijd door een onafhankelijke derde partij (auditor) uitgevoerd in samenspraak met de opdrachtnemer.
IBPB-5.2.2	Opdrachtnemer dient gedurende de looptijd van de overeenkomst minimaal te beschikken over een of meerdere overeengekomen geldige certificaten en/of gelijkwaardige normeringen (zoals ISO 27001 en/of de NIST Cybersecurity Framework) en bijbehorende recente formele audit-verklaringen die passend zijn bij de aard van de geleverde dienstverlening (zoals een ISAE3402 of SOC2 type 2 rapportage).

5.3 Overleg & rapportage

Als onderdeel van de besturing van de door opdrachtnemer geleverde dienstverlening vindt regulier overleg plaats met opdrachtnemer en levert deze periodiek rapportages op. Het geleverde dient op dit onderdeel minimaal aan de hieronder staande eisen te voldoen:

Eis	Omschrijving
IBPA-5.3.1	Opdrachtnemer draagt in het kader van de gevraagde oplossing/dienstverlening jaarlijks zorg voor inzicht (in overleg e/o in rapportage) in onderstaande onderwerpen: ▪ De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; ▪ Overzicht van afwijkingen ten opzichte van beleid of contract; ▪ Overzicht van risico acceptaties waarin de afwijkingen tov het beleid en contract zijn vastgelegd en vastgesteld.
IBPA-5.3.2	Opdrachtnemer dient zorg te dragen voor een periodieke rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligings- en privacymaatregelen en het gerealiseerde beveiligingsniveau. Daartoe dient periodiek gestructureerd overleg plaats te vinden om issues, rapportages (comply or explain) en ontwikkelingen te bespreken over de gevraagde oplossing/dienstverlening met de volgende onderwerpen: ▪ onderkende risico's inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ security hardening proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ vulnerability management proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ lifecycle & patchmanagement proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ uitgevoerde penetratietesten inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ loggings- en detectie-informatie monitoringsbevindingen van ICT-Componenten en de status van de opvolging /afhandeling van geconstateerde bevindingen; ▪ de resultaten van de periodieke controle van de toegangsrechten van de eigen medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening.