Sociale Verzekeringsbank
Bijlage G2
Programma van Eisen Informatiebeveiliging en privacy

Europese aanbesteding WAN- en internetconnectiviteit en aanverwante dienstverlening

Versie 1.0

S V B voor het leven
Sociale Verzekeringsbank

Inhoudsopgave

1 Inleiding

In deze bijlage staan de informatiebeveiligingseisen met betrekking tot de gevraagde dienstverlening beschreven. Deelnemer dient de laatste pagina van deze Bijlage te voorzien van een rechtsgeldige ondertekening.

Voordat wordt ingegaan op deze eisen wordt kort de positie van informatiebeveiliging binnen de SVB geschetst.

2 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 gebruik 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.

2.1 Informatiebeveiligingsprincipes

Als onderdeel van het SVB informatiebeveiligingsbeleid 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 informatie** alleen **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 stand houden 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.

2.2 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. Tevens dient Opdrachtnemer, of minimaal dat deel van de organisatie wat betrokken is bij de dienstverlening aan de SVB, ISO27001 gecertificeerd te zijn.

2.3 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 dienstverlener.
- Wet en Regeling SUWI (Wet structuur uitvoeringsorganisatie werk en inkomen) – (onderdelen) alleen van toepassing indien expliciet opgenomen in dit Programma van Eisen.

Het informatiebeveiliging- en privacybeleid van de SVB zelf is gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid).

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

3 Eisen aan personeel van Opdrachtnemer

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.

Nr.	Omschrijving
IBP-3.1	Alle medewerkers die namens/in opdracht van Opdrachtnemer participeren in de levering van de gevraagde dienstverlening moeten bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn.
IBP-3.2	Opdrachtnemer draagt zorg dat medewerkers die participeren in de levering van de diensten aan de SVB bij indiensttreding bij de Opdrachtnemer een geheimhoudingsovereenkomst hebben ondertekend en dat zij hier naar handelen.
IBP-3.3	Opdrachtnemer draagt zorg dat medewerkers die participeren in de levering van de diensten aan de SVB, bij indiensttreding bij de Opdrachtnemer een Verklaring Omtrent Gedrag (VOG) of een gelijkwaardig document hebben overlegd, dat niet ouder is dan 12 maanden.
IBP-3.4	Bij het betreden van een locatie van de SVB dienen medewerkers van of namens de Opdrachtnemer zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs.
IBP-3.5	Opdrachtnemer heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
IBP-3.6	Alle medewerkers van Opdrachtnemer en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
IBP-3.7	Medewerkers van of namens Opdrachtnemer betreden alleen onder begeleiding de SVB locaties.

4 Beveiliging van Diensten

4.1 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.

Nr.	Omschrijving
IBP-4.1.1	De gevraagde dienstverlening moet opgezet en geleverd worden vanuit het basis principe “Secure-by-Design”.
IBP-4.1.2	Opdrachtnemer heeft informatiebeveiliging en bedrijfscontinuïteit aantoonbaar gestandaardiseerd, gestructureerd, continu en cyclus procesmatig (PDCA cyclus) in alle lagen van de organisatie en gevraagde dienstverlening ingericht.
IBP-4.1.3	De gevraagde dienstverlening moet adequaat zijn beveiligd door het implementeren en onderhouden van een set van technische, procedurele en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de dienstverlening en de daarop opgeslagen en/of verwerkte informatie borgt.
IBP-4.1.4	Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de gevraagde dienstverlening.
IBP-4.1.5	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-4.1.6	Opdrachtnemer dient zorg te dragen dat software welke gebruikt wordt als onderdeel van de gevraagde dienstverlening, altijd wordt ondersteund door de fabrikant van de software, dan wel de eigenaar van de sourcecode.
IBP-4.1.7	Opdrachtnemer garandeert testgegevens, betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.
IBP-4.1.8	Opdrachtnemer heeft voor het aanvaardbaar gebruik van: - informatie en - van bedrijfsmiddelen die samenhangen met informatie en - informatie verwerkende faciliteiten, regels geïdentificeerd, gedocumenteerd en geïmplementeerd.
IBP-4.1.9	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.

4.2 Bedreigingen

De gevraagde dienstverlening is onderhevig aan een dreigingsbeeld. De SVB heeft hiervoor zelf risico-management processen geïmplementeerd. Veranderingen in het dreigingsbeeld moeten tijdig gesignaleerd worden om deze risico-management processen kwalitatief goed te kunnen blijven uitvoeren.

Nr.	Omschrijving
IBP-4.2.1	Opdrachtnemer moet de SVB direct op de hoogte stellen van bedreigingen die een directe en/of grote impact op de SVB kunnen vormen en waarbij de mitigerende maatregelen op dat moment onvoldoende zijn. Afspraken hierover (o.a. contactpersonen, telefoonnummers) worden vastgelegd in het DAP.

4.3 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.

Nr.	Omschrijving
IBP-4.3.1	Opdrachtnemer dient patches op de ICT-componenten die onderdeel uitmaken van de dienst voor de SVB, tijdig en conform leveranciersadviezen aan te brengen.

4.4 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.

Nr.	Omschrijving
IBP-4.4.1	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de gevraagde dienstverlening.
IBP-4.4.2	Opdrachtnemer dient de componenten die onderdeel uitmaken van de dienst voor de SVB te hardenen. De te hanteren volgorde is: ICT componenten waarvoor CIS Benchmarks beschikbaar zijn, behoren te voldoen aan deze CIS Benchmark. ICT componenten waarvoor geen CIS-benchmarks beschikbaar zijn, zullen worden geconfigureerd conform de beveiligingsrichtlijnen van de leverancier van de apparatuur.

4.5 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.

Nr.	Omschrijving

IBP-4.5.1	Opdrachtnemer verleent medewerking aan een tevoren schriftelijk aangekondigd attack & penetrationtest op de componenten die deel uitmaken van de dienstverlening naar de SVB. Uit te voeren door een derde partij die door de SVB is geselecteerd.

4.6 Beveiliging (SVB portaalfunctionaliteit)

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.

Nr.	Omschrijving
IBP-4.6.1	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-4.6.2	De gevraagde dienstverlening moet voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties (September 2015), dan wel de logische opvolgers daarvan (https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html).
IBP-4.6.3	Opdrachtnemer moet de OWASP top tien (https://owasp.org/Top10/), dan wel de logische opvolgers daarvan, structureel hanteren om de meest kritische beveiligingsrisico's binnen een webapplicatie te vermijden.
IBP-4.6.4	De cryptografische beveiligingsvoorzieningen van de gevraagde dienstverlening moeten voldoen aan de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS), dan wel logische opvolgers daarvan (https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html).

4.7 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.

Nr.	Omschrijving
IBP-4.7.1	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-4.7.2	In de ICT infrastructuur moeten signaleringsfuncties (registratie/logging en detectie) actief, efficiënt, effectief en beveiligd ingericht zijn.
IBP-4.7.3	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces.

Nr.	Omschrijving
IBP-4.7.4	Opdrachtnemer draagt zorg dat de netwerkverbindingen zowel fysiek als logisch zijn beveiligd tegen ongeautoriseerde toegang door derden. Hiertoe worden binnen de branche gebruikelijke maatregelen toegepast. Opdrachtnemer dient op aanvraag van Opdrachtgever inzichtelijk te maken welke maatregelen geïmplementeerd zijn en hoe deze gecontroleerd worden.

5 Privacy

De Algemene Verordening Gegevensbescherming (AVG) beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. In dit overzicht zijn niet de bepalingen herhaald die zijn opgenomen zijn in artikel 8 van de Overeenkomst (Gegevensbescherming & Privacy). De gevraagde dienstverlening moet aan de volgende eisen voldoen.

Nr.	Omschrijving
IBP-5.1	De gevraagde dienstverlening moet gedurende de gehele looptijd van de Overeenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBP-5.2	In lijn met de Verwerkersovereenkomst moet Opdrachtnemer de van de SVB ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de SVB verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeengekomen, en zal Opdrachtnemer de persoonsgegevens dus niet gebruiken voor: ▪ Het uitvoeren van tests; en ▪ Het uitvoeren van data-analyses.
IBP-5.3	De gevraagde dienstverlening moet de mogelijkheid bieden om gegevenselementen die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding/rechtsgrond aanwezig is te verwijderen.
IBP-5.4	Opdrachtnemer dient de integriteit en vertrouwelijkheid van het over zijn netwerk getransporteerde gesprek/verkeer van de SVB te waarborgen. Aan de hand van zowel fysieke als logische maatregelen voorkomt Opdrachtnemer de mogelijkheid tot het afluisteren van netwerkverbindingen en borgt zij de integriteit van het verkeer.

6 Uitvoeringsaspecten

6.1 Beveiligingsincidenten

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.

Nr.	Omschrijving
IBP-6.1.1	Opdrachtnemer meldt informatiebeveiligingsincidenten onverwijld per email bij de SVB Servicedesk, op het emailadres: servicedesk@svb.nl.

IBP-6.1.2	In het geval van een informatiebeveiligingsincident moet Opdrachtnemer redelijkerwijs maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het incident.
IBP-6.1.3	Opdrachtnemer moet volledige medewerking geven bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot het incident ter beschikking aan de SVB.

6.2 Controle en audits

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

Nr.	Omschrijving
IBP-6.2.1	De SVB heeft het recht om bij Opdrachtnemer een onderzoek (of audit) in te stellen met betrekking tot de naleving van de in de Overeenkomst met bijhorende Bijlagen opgenomen verplichtingen. De audit wordt altijd door een onafhankelijke derde partij (auditor) uitgevoerd.
IBP-6.2.2	Minimaal jaarlijks levert Opdrachtnemer een recente formele audit-verklaring op die past bij de aard van de gevraagde dienstverlening (zoals een ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principes, of gelijkwaardig). Deze verklaring is afgegeven door een onafhankelijke geaccrediteerde auditor en toont de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van de gevraagde dienstverlening aan.

6.3 Overleg & rapportage

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

Nr.	Omschrijving
IBP-6.3.1	Opdrachtnemer stelt een vaste contactpersoon aan die voor de gevraagde dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-6.3.2	Periodiek (minimaal eens per jaar) vindt een gestructureerd overleg tussen Opdrachtnemer en de SVB plaats om informatiebeveiliging en de daarop betrekking hebbende rapportages te bespreken.
IBP-6.3.3	Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de geleverde dienstverlening.

7 Ondertekening

Naar waarheid, stellig en zonder voorbehoud ondertekend:

Bedrijfsnaam Deelnemer: ……
Plaats: ……. Datum:……
Naam ondergetekende: …….. Functie:……
Handtekening: ……