

Nummer	Categorie	Requirement
EF-01	Algemeen	De Oplossing voldoet aan de algemene verwachtingen die een Gebruiker, gezien wat gangbaar is voor dit soort service management applicaties, gezien de betreffende markt en gezien andere vergelijkbare applicaties, aan de Oplossing mag hebben. Dit in ieder geval wat betreft betrouwbaarheid, functionaliteit, uitbreidbaarheid, en gebruikersgemak.
EF-02	Asset Management	De Oplossing maakt het mogelijk om specifieke data automatisch te verwijderen of te anonimiseren na een door de SVB in te stellen periode (bijvoorbeeld de naam van degene die een Aanvraag of een Melding heeft ingediend).
EF-03	Asset Management	De Oplossing maakt het mogelijk om hiertoe aangegeven Assets te reserveren via een reserveringsfunctie op basis van een planbord.
EF-04	Asset Management	De Oplossing ondersteunt het vastleggen en bijhouden van de status van Assets, de relatie tot elkaar en de Diensten. De relaties en de status zijn tevens te visualiseren t.b.v. een actueel status inzicht van de dienstenketen en impact bij verstoringen.
EF-05	Asset Management	De CMDB van de Oplossing faciliteert het opslaan van geoormerkte bijlagen inclusief doorzoekbare metadata per Assets - in het bijzonder PDF, XLSX, DOCX, PNG, JPG.
EF-06	Facilities Management	De Oplossing biedt een webportaal waar Eindgebruikers enkele of groepen (bulk) bezoekers kunnen aan/afmelden, waarbij persoonlijke gegevens van bezoekers worden geregistreerd in de Oplossing (zoals naam, contactgegevens, bedrijfsnaam, bezoeksdatum en -tijd, en het doel van het bezoek).
EF-07	Oplossing	De Oplossing ondersteunt ITIL processen/practises in de versies 3 en 4.
EF-08	Oplossing	De Oplossing wordt aangeboden als SAAS-dienst, waarbij de functionele configuratie door de SVB gedaan kan worden, zonder tussenkomst van de Opdrachtnemer, in aspecten als Portaal, pagina's, formulieren, mail templates, etc.
EF-09	Oplossing	De Oplossing kan gebruikt worden door meerdere Domeinen met een scheiding van data-opslag, datastromen, configuraties en rollen/rechten.
EF-10	Oplossing	De Oplossing biedt de gewenste functionaliteit zonder maatwerk of additionele applicaties.
EF-11	Oplossing	De Oplossing biedt een integraal geheel waarbij Meldingen/Aanvragen en kennisitems gerelateerd kunnen worden aan Diensten en bijbehorende SLA afspraken, Gebruikersgroepen, beheerteams en Assets uit de CMDB.
EF-12	Oplossing	De Oplossing is online via een browser toegankelijk. Er is een mobile enabled versie of app (IOS&Android) beschikbaar met functionaliteit voor Eindgebruikers om Meldingen/Aanvragen te doen en te volgen, en voor Behandelaars om deze af te handelen.
EF-13	Oplossing	De Oplossing biedt de functionaliteit om (na een door de SVB te bepalen termijn of ten behoeve van acceptatie- en testomgevingen), bepaalde gekenmerkte gegevens automatisch te anonimiseren. Daarbij blijft de meta data en de aantallen beschikbaar t.b.v. rapportages.
EF-14	Oplossing	De Oplossing zorgt er voor dat er geen data verloren gaat ingeval dat er door meerdere Behandelaars op hetzelfde moment aan hetzelfde item (zoals Melding, Aanvraag, Asset, rapportage, etc.) gewerkt wordt.
EF-15	Rapportage	De Oplossing maakt het mogelijk om te rapporteren onder andere per Domein en externe service provider (ESP.) Ook als Meldingen/Aanvragen en workflows door meerdere Domeinen en/of ESP's zijn behandeld.
EF-16	Security	De Oplossing voorziet standaard in een niet-muteerbare audit-trail, waarin automatische registratie en opslag van de volgende gegevens plaatsvindt: • De desbetreffende Gebruiker, datum en tijd van de uitvoering van de handeling. • Alle handelingen die door Gebruikers met betrekking tot metagegevens, processen, documenten, procesregistraties of andere objecten worden verricht. De Oplossing voorziet standaard een geïntegreerde voorziening voor het leesbaar presenteren van deze audit-trail.
EF-17	Security	De Oplossing maakt het mogelijk om informatie af te schermen voor het specifieke Domein en specifieke Behandelaars. Dan wel via volledige afscherming van Meldingen/Aanvragen en/of delen van Meldingen/Aanvragen. Deze afscherming treedt in werking bij een combinatie van kenmerken uit minimaal de Dienst, SLA, melder en Oplosgroep.
EF-18	Service Management	De Oplossing heeft een servicescatalogus waarin Diensten per Domein kunnen worden beschreven en zowel voor de Behandelaar als voor specifieke Eindgebruikers-groepen in het Portaal beschikbaar kan worden gemaakt (bijvoorbeeld een dienst die alleen in Utrecht kan worden afgenomen is enkel zichtbaar voor medewerkers uit Utrecht). Hieruit zijn onderdelen van deze Diensten via een bestelcatalogus aan te vragen en kan toegang gegeven worden op basis van gegevens uit de Behandelaar- en Eindgebruikersadministratie.
EF-19	Service Management	De Oplossing faciliteert de relatie tussen contracten/SLA's en de bijbehorende servicewindow en prioriteitenmatrix per Dienst, in combinatie met Eindgebruikers-groepen en hiertoe aangemerkte Assets. Mede t.b.v. het automatisch instellen van Prioriteit/doorlooptijd van Meldingen.
EF-20	Service Management	De Oplossing ondersteunt het starten van een Workflow op basis van een Melding of Aanvraag zodat een opdracht uitgezet kan worden bij een interne of externe partij (Oplosgroep of leverancier). De inhoud van die opdracht is zowel vrij (tekstveld) door de Behandelaar of vast (template) door de Beheerder te bepalen.

Nummer	Categorie	Omschrijving
NF-01	Beschikbaarheid	De Oplossing heeft 24x7 een beschikbaarheid van ten minste 99,5% voor de productieomgeving. Met beschikbaarheid wordt bedoeld: de totale tijdsduur waarin de Gebruikers iedere maand daadwerkelijk (i.e. performant en overig in overstemming met de afgesproken eisen) gebruik hebben kunnen maken van de Oplossing. De beschikbaarheid wordt gemeten over iedere periode van één (1) kalendermaand.
NF-02	Beschikbaarheid	Gepland onderhoud (waardoor de Dienstverlening wordt onderbroken) gaat niet ten kosten van de beschikbaarheid van de Oplossing, mits op Werkdagen uitgevoerd tussen 21:00u en 6:00u en wordt minimaal 7 kalenderdagen vooraf gecommuniceerd aan de SVB.
NF-04	Compatibiliteit	De Oplossing kan bouwtekeningen inlezen en/of exports van een tekening conform vaste standaarden importeren t.b.v. assetmanagement en ruimteadministratie - in het bijzonder AutoCad. De Oplossing moet voorzien in de hiërarchische relatiestructuur van dependances, gebouwen, ruimten en de relatie met de Assets binnen een ruimte.
NF-05	Documentatie	Opdrachtnemer stelt een functioneel-technische handleiding beschikbaar van alle beheerdersfunctionaliteit binnen de Oplossing, waaronder informatie over Koppelingen, rapportages en gebruikersbeheer, in het Nederlands of Engels.
NF-06	Documentatie	De Opdrachtnemer stelt naast standaard documentatie van de Oplossing specifieke documentatie beschikbaar, met betrekking tot de Implementatie van de Oplossing voor de SVB.
NF-07	Documentatie	De Opdrachtnemer stelt documentatie voor (technisch) gebruikersbeheer beschikbaar waarin de mogelijkheden voor authenticatie, autorisatie en eventuele user provisioning staan beschreven
NF-08	Koppelingen	Bij testen en accepteren van nieuwe of gewijzigde functionaliteiten en Koppelingen, kan de Oplossing gebruikmaken van geanonimiseerde testdata uit de corresponderende T-A omgevingen van de diverse aanleverende en afnemende systemen van de SVB.
NF-10	Koppelingen	API's moeten een versiebeleid hebben.
NF-11	Koppelingen	Koppelingen die van belang zijn voor de Oplossing en in beheer zijn bij Opdrachtnemer (of toeleveranciers van de Opdrachtnemer) hebben duidelijke specificaties (descriptor documents). Voor elke Integratie en Connector met een interne of externe applicatie wordt minimaal het volgende beschreven: - Functie(s) - Wijze toegang - Aanroep - Berichtsoorten en -inhoud - Technische limieten
NF-12	Koppelingen	De Oplossing moet 'Create-Read-Update-Delete' (CRUD) functies ondersteunen via interfaces (API's).
NF-13	Koppelingen	Opdrachtnemer zorgt dat alle (maatwerk- en standaard) Koppelingen blijven werken bij nieuwe releases en upgrades van de Oplossing. Deze Koppelingen maken tevens deel uit van het informatiebeveiligingsbeleid van Opdrachtnemer en vallen binnen de scope van de SLA.
NF-14	Koppelingen	De Oplossing integreert probleemloos met ServiceNow middels een door de Opdrachtnemer geleverde (en ook te onderhouden) Koppeling waarbij updates in beide systemen automatisch worden gesynchroniseerd (bi-directioneel).
NF-15	Koppelingen	Opdrachtnemer levert een Koppeling met Priva BlueID als onderdeel van de Oplossing. Na Gunning worden de (API) specificaties bepaald en besloten hoe deze Koppeling tot stand wordt gebracht. Opdrachtnemer zal hiervoor 36 uur opnemen in de Implementatie-kosten. Indien Opdrachtnemer aan kan tonen dat een Koppeling meer uren zal kosten, dan mogen deze kosten na akkoord van de SVB worden gefactureerd als zijnde Optimalisatie-kosten.
NF-16	Koppelingen	Opdrachtnemer levert een Koppeling met ESM van Heijmans (IRIS) als onderdeel van de Oplossing. Na Gunning worden de (API) specificaties bepaald en besloten hoe deze Koppeling tot stand wordt gebracht. Opdrachtnemer zal hiervoor 36 uur opnemen in de Implementatie-kosten. Indien Opdrachtnemer aan kan tonen dat een Koppeling meer uren zal kosten, dan mogen deze kosten na akkoord van de SVB worden gefactureerd als zijnde Optimalisatie-kosten.
NF-17	Koppelingen	De Oplossing integreert probleemloos met Power BI , middels een door de Opdrachtnemer geleverde (en ook te onderhouden) Integratie.
NF-18	Koppelingen	Opdrachtnemer levert een Koppeling met ProActis als onderdeel van de Oplossing. Na Gunning worden de (API) specificaties bepaald en besloten hoe deze Koppeling tot stand wordt gebracht. Opdrachtnemer zal hiervoor 36 uur opnemen in de Implementatie-kosten. Indien Opdrachtnemer aan kan tonen dat een Koppeling meer uren zal kosten, dan mogen deze kosten na akkoord van de SVB worden gefactureerd als zijnde Optimalisatie-kosten.
NF-19	Koppelingen	De Oplossing biedt een Koppeling voor geautomatiseerde aanlevering van loggegevens naar Dynatrace en Splunk.
NF-20	Koppelingen	Koppelingen die in beheer zijn bij Opdrachtnemer stellen de SVB in staat om ten aanzien van de A en P-omgeving near-realtime data uit te wisselen.
NF-21	Opdrachtnemer	De Opdrachtnemer van de Oplossing biedt tijdens kantooruren (07h - 19h Nederlandse tijd) Helpdesk ondersteuning in de Nederlandse taal.
NF-22	Oplossing	De Oplossing ondersteunt out-of-the-box geautomatiseerde user provisioning zodat Gebruikers geautomatiseerd kunnen worden aangemaakt, geautoriseerd, gemuteerd en verwijderd/gearchiveerd.
NF-23	Oplossing	De presentatielaag van de Oplossing (browser) functioneert met minimaal de laatste twee versies van Google Chrome en Microsoft Edge, en moet overige marktconforme browsers ondersteunen, dwz als deze een aandeel heeft van 5% van de browsermarkt (volgens W3.org) of de natuurlijke opvolger is van een bestaande marktconforme browser).
NF-24	Oplossing	De Opdrachtnemer levert identieke test-, acceptatie-, en productieomgevingen aan, waarbij de test- en acceptatieomgeving(en) logisch gescheiden is/zijn van de productieomgeving.
NF-25	Oplossing	Er is kennis en ervaring aanwezig van de Oplossing op de Nederlandse markt voor een best practice Implementatie en ondersteuning.
NF-26	Oplossing	De presentatielaag van de Oplossing functioneert zonder aanvullende propriety plugins of extensies.
NF-27	Oplossing	Opdrachtnemer geeft vooraf inzage in de wijzigingen die bij elke nieuwe software-release worden uitgerold en de invloed ervan op het gebruik van de Oplossing voor de SVB. Bij releases met impact op het gebruik van de software voor de SVB communiceert Opdrachtnemer dit minimaal 1 maand van te voren.
NF-28	Performance	De P-omgeving van de Oplossing moet schaalbaar zijn tegen gelijkblijvende performance, en in overeenstemming blijven met de SLA.
NF-29	Performance	Batchverwerking binnen de Oplossing mag de performance van de Oplossing voor Eindgebruikers en Behandelaars niet negatief beïnvloeden.
NF-30	Rapportage	Opdrachtnemer geeft periodiek inzicht (ten minste éénmaal per maand) in de geleverde prestaties, dmv een SLA rapportage op de afgesproken Service Levels.

NF-31	Rapportage	Direct na inwerkingtreding van de Overeenkomst zal de Opdrachtnemer met de SVB afspraken maken over de invulling van een Dossier Afspraken en Procedures (DAP), waarin nadere invulling wordt gegeven aan gemaakte operationele afspraken.
NF-32	Rapportage	Opdrachtnemer rapporteert regelmatig over de voortgang van alle verbeterplannen.
NF-33	Retransitie	Alle aanwezige SVB data en gegevens in de Oplossing worden binnen twee weken na beëindiging van de Overeenkomst kosteloos geretourneerd aan de SVB, in een gangbaar en marktconform formaat.
NF-34	Retransitie	Voor alle geretourneerde SVB-data- en gegevens wordt een bestandsbeschrijving meegestuurd.
NF-35	Retransitie	Opdrachtnemer verleent alle medewerking die noodzakelijk is voor een soepele overdracht van de Dienstverlening naar een nieuwe leverancier.
NF-36	Retransitie	Opdrachtnemer zal op verzoek van de SVB een senior consultant aanbieden tegen de geldende Tarieven, voor eventuele nazorg of begeleiding bij de overdracht.
NF-37	Retransitie	Opdrachtnemer levert een blauwdruk van de meest actuele systeemconfiguratie en de inrichting van de Oplossing. Deze blauwdruk kan worden geïmporteerd in een eventuele nieuwe instantie van gebruikte software, onder beheer van een nieuwe leverancier. Als import niet mogelijk is dan geeft de blauwdruk tenminste voldoende informatie om een nieuwe instantie van de software zodanig (handmatig) te configureren en in te richten dat deze identiek is aan de Oplossing en dezelfde functionaliteiten biedt. Hiermee wordt geborgd dat bij beëindiging van de Overeenkomst de tijd en kennis die is geïnvesteerd tijdens configuratie en inrichting van de Oplossing, nimmer verloren gaat.
NF-38	Retransitie	Na beëindiging van de Overeenkomst wordt alle aanwezige SVB-data- en gegevens in de Oplossing permanent verwijderd conform AVG richtlijnen en na bevestiging van ontvangst van de data door de SVB. Alle kosten, boetes en herstelbetalingen, voortvloeiende uit het niet permanent verwijderen van de SVB data en gegevens uit de Oplossing welke leiden tot een datalek voor de SVB zullen verhaald worden op de Opdrachtnemer.
NF-39	Retransitie	De Opdrachtnemer stelt in overleg met de SVB een exitplan op waarin de continuïteit van de Oplossing en de werkzaamheden en verplichtingen bij het aflopen of beëindigen van de Overeenkomst vastgelegd worden.
NF-40	Performance	Opdrachtnemer zal een SLA beschikbaar stellen die onderdeel zal worden van de Overeenkomst die ten minste voldoet aan dit programma van eisen.
NF-41	Performance	De Opdrachtnemer biedt de SVB een 'single point of contact' voor escalaties ten aanzien van de Dienstverlening.
NF-42	Performance	Opdrachtnemer voorziet in technische en organisatorische maatregelen, voor het direct registreren, administreren en rapporteren van incidenten, problemen, wijzigingen, en vergelijkbare correspondentie met betrekking tot de Dienstverlening. Opdrachtnemer zorgt ervoor dat de SVB te allen tijde toegang heeft tot de status van incidenten, problemen, wijzigingen, en bijbehorende correspondentie.
NF-43	Performance	Bij het niet halen van de afgesproken service levels voor P1, start Opdrachtnemer onverwijld een onderzoek naar de oorzaak en rapporteert hierover schriftelijk aan de SVB. Dit rapport bevat tenminste een RCA (root cause analysis) en een verbeterplan, waarin de volgende elementen zijn opgenomen: • Start- en eindtijd van de verstoring. • Beschrijving van de verstoring en het aantal getroffen Gebruikers. • Beschrijving van de oorzaak van het de verstoring. • Beschrijving van de tijdelijke oplossing. • Beschrijving en planning van de permanente maatregelen.
NF-44	Standaarden	De Oplossing biedt een directe mailfunctionaliteit via Microsoft 365 m.b.v. het SMTP protocol met ondersteuning van Modern Authentication. In de toekomst is aansluiting via Exchange Web Services met Modern Authentication vereist.
NF-45	Standaarden	De Oplossing ondersteunt het aansturen van printers middels de standaarden PDF/A, PCL en AFP.
NF-46	Standaarden	Koppelingen zijn tijdens transport minimaal beveiligd volgens de standaard TLS 1.2 of hoger.
NF-47	Standaarden	De Koppelingen met andere systemen van de SVB zijn mogelijk via queueing in IBM MQ en ActiveMQ en webservices in SOAP/XML en REST/JSON.
NF-48	Standaarden	Voor REST API Koppelingen wordt de open standaard OpenAPI Specification (OAS) gebruikt voor het specificeren en documenteren van de API. Zie : https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification .
NF-49	Standaarden	Voor het specificeren van REST API's wordt de standaard OpenAPI Specification (OAS) toegepast ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit binnen de publieke sector.
NF-50	Standaarden	Voor het documenteren van de REST API worden de standaard REST-API Design Rules gebruikt.
NF-51	Toegankelijkheid	Een Gebruiker kan de Oplossing benaderen via een webbased applicatie (browser). Dit houdt in dat er naast de browser geen aanvullende software of scripts vereist zijn voor het gebruik van de Oplossing.
NF-52	Toegankelijkheid	De Oplossing is gebruikersvriendelijk. Dit houdt ten minste in dat het aantal handelingen dat nodig is om een taak uit te voeren zo beperkt mogelijk is, dat de user interface overzichtelijk is, dat de user interface en de user experience intuïtief zijn en beperkte training vereisen, dat er een eenvoudig en snelle zoekfunctie beschikbaar is voor gebruikers waarmee informatie en functies eenvoudig vindbaar zijn.
NF-53	Toegankelijkheid	De Oplossing kan overweg met Role Based Access Control (RBAC): • Role claim (in de role claim worden alle rollen van de Eindgebruiker / Behandelaar (van alle applicaties) bij de applicatie aangeboden), EN • Role assignment (de rol van de Gebruiker wordt aan een specifieke claim toegewezen die de applicatie begrijpt).
NF-54	Toegankelijkheid	De Oplossing sluit aan op de standaarddienst (autorisatie): 'SVB eenmalig aanloggen'. Nu gerealiseerd door Azure AD SSO/MFA (QS Solutions). Aansluiten op 1 van de verplichte standaarden van de overheid (PTOLU): SAML 2.0 of Oauth 2.0/OpenID Connect 1.0. Alternatief: WS-Federation v1.2 Voor on-premise applicaties dient aangesloten te worden op de (lokale) active directory voor SSO.

Nummer	Categorie	Omschrijving
IBP-01	Informatiebeveiliging & Privacy	De Opdrachtnemer is voor de SVB altijd eerste aanspreekpunt en eindverantwoordelijk voor de borging van de overeengekomen afspraken / verplichtingen met betrekking tot de Dienstverlening ook indien zij één of meerdere Onderaannemers (waaronder een dochter of zusteronderneming) inschakelt.
IBP-02	Informatiebeveiliging & Privacy	Medewerkers van de Opdrachtnemer die in aanraking komen met vertrouwelijke informatie van de SVB dienen een geheimhoudingsovereenkomst te hebben ondertekend en op basis hiervan te handelen.
IBP-03	Informatiebeveiliging & Privacy	Medewerkers van de Opdrachtnemer die participeren in de levering van de Dienstverlening dienen te beschikken over een relevante geldige Verklaring Omtrent Gedrag (VOG) of een gelijkwaardig ander document welke niet ouder is dan 36 maanden. De kosten van de VOG's en de administratie hieromtrent zijn voor rekening van de Opdrachtnemer.
IBP-04	Informatiebeveiliging & Privacy	Medewerkers die namens en/of in opdracht van Opdrachtnemer participeren in de levering van de Dienstverlening dienen bekend te zijn met voor hun werk relevante contractueel overeengekomen afspraken / verplichtingen op het gebied van informatiebeveiliging, geheimhouding en privacy.
IBP-05	Informatiebeveiliging & Privacy	De 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 Dienstverlening.
IBP-06	Informatiebeveiliging & Privacy	Medewerkers van de Opdrachtnemer en eventuele onderaannemer(s) dienen een passende bewustzijnsopleiding en/of -training te hebben gehad en dienen regelmatig bijscholing van organisatie beleidsregels en procedures te krijgen, voor zover relevant voor hun functie/rol in relatie tot de geleverde Dienstverlening.
IBP-07	Informatiebeveiliging & Privacy	De Oplossing dient minimaal te voldoen aan de BBN2-eisen zoals beschreven in de laatste versie van de Baseline Informatiebeveiliging Overheid (BIO). Echter wanneer binnen de Oplossing data wordt opgeslagen of verwerkt met een hoge(re) classificering dan BBN2, dienen minimaal de betrokken onderdelen van de Oplossing deze BBN-classificering te ondersteunen.
IBP-08	Informatiebeveiliging & Privacy	De Oplossing dient adequaat te zijn beveiligd middels een set van maatregelen gebaseerd op algemeen geaccepteerde standaarden, welke de beschikbaarheid, integriteit en vertrouwelijkheid van de Oplossing (inclusief de toegepaste ICT-componenten) en de daarop opgeslagen en/of verwerkte informatie borgt.
IBP-09	Informatiebeveiliging & Privacy	De Oplossing dient alleen (software) componenten te bevatten welke: - worden ondersteund door de fabrikant(en) en/of de eigenaar van de source code; - correct en veilig functioneren binnen en/of in samenwerking met de omgeving van de SVB.
IBP-10	Informatiebeveiliging & Privacy	(Eventueel) betrokken gegevens bij de realisatie van de Oplossing en in het bijzonder persoonsgegevens dienen zorgvuldig te zijn gekozen, te worden beschermd en vernietigd indien niet meer noodzakelijk.
IBP-11	Informatiebeveiliging & Privacy	De Opdrachtnemer dient ervoor te zorgen dat ten aanzien van het veilig gebruik van informatie, bedrijfsmiddelen en/of faciliteiten die samenhangen met de Dienstverlening gebruiksregels zijn geïdentificeerd, gedocumenteerd en geïmplementeerd.
IBP-12	Informatiebeveiliging & Privacy	De 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.
IBP-13	Informatiebeveiliging & Privacy	De Opdrachtnemer informeert de SVB ter beoordeling over hoe binnen de aangeboden Oplossing invulling is gegeven aan de basisprincipes 'Secure / Security by Design' en 'Secure / Security by Default' bij de ontwikkeling van applicaties en/of systemen welke onderdeel zijn van de Oplossing.
IBP-14	Informatiebeveiliging & Privacy	De Oplossing 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).
IBP-15	Informatiebeveiliging & Privacy	De Oplossing dient bij gebruik van encryptiesleutels en/of certificaten ervoor zorg te dragen dat het gebruik voor de SVB inzichtelijk is en dat het per direct intrekken of onbruikbaar maken van encryptiesleutels en/of certificaten mogelijk is.
IBP-16	Informatiebeveiliging & Privacy	De Opdrachtnemer dient voor het onderhoud en/of doorvoeren van aanpassingen met betrekking tot de Oplossing 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.
IBP-17	Informatiebeveiliging & Privacy	De Opdrachtnemer heeft de informatiebeveiliging en bedrijfscontinuïteit gestandaardiseerd, gestructureerd en gebaseerd op een cyclus van continue verbeteren, in alle lagen van de organisatie en te leveren Dienstverlening.
IBP-18	Informatiebeveiliging & Privacy	De Opdrachtnemer dient beleid, beleids- en beheersingsrichtlijnen en processen te hebben voor het veilig beheren en aanbieden van de Dienstverlening.
IBP-19	Informatiebeveiliging & Privacy	De 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.
IBP-20	Informatiebeveiliging & Privacy	De Opdrachtnemer dient actief mee te werken aan het inzichtelijk maken en het mitigeren van risico's welke samenhangen met de Oplossing.
IBP-21	Informatiebeveiliging & Privacy	De Opdrachtnemer dient structureel risicoanalyses uit te voeren in het bouw- en implementatietraject, bij grote onderhoudstrajecten en bij significante wijzigingen in de dienstverlening.
IBP-22	Informatiebeveiliging & Privacy	De Opdrachtnemer dient aantoonbaar onderkende risico's vast te leggen voorzien van de geplande mitigerende maatregelen inclusief een verwachte implementatie / oplosdatum en actiehouders.
IBP-23	Informatiebeveiliging & Privacy	De 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.
IBP-24	Informatiebeveiliging & Privacy	De Opdrachtnemer dient de SVB op de hoogte te stellen, via het overeengekomen communicatiekanaal en tijdslijnen, van risico's die een directe impact op de SVB (kunnen) hebben.
IBP-25	Informatiebeveiliging & Privacy	De Oplossing dient te beschikken over passende, betrouwbare en effectieve mechanismen, gebaseerd op algemeen geaccepteerde standaarden, ten aanzien van identificatie, authenticatie, autorisatie en verantwoording / controle (IAAA).
IBP-26	Informatiebeveiliging & Privacy	De Oplossing dient aan te sluiten op de aanwezige directory service (Microsoft Active Directory (AD)) van de SVB waarbij de SVB altijd eindverantwoordelijk blijft voor het vaststellen van de gedeelde attributen. Indien aansluiting niet mogelijk is dient dit formeel geaccepteerd te worden door de SVB.
IBP-27	Informatiebeveiliging & Privacy	De Oplossing dient voor authenticatie Multi-factor authenticatie (MFA) en single sign-on (SSO) op basis van standaard protocollen (bv. OAUTH2, SAML, etc.) te ondersteunen.
IBP-28	Informatiebeveiliging & Privacy	De Oplossing 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.
IBP-29	Informatiebeveiliging & Privacy	De Opdrachtnemer mag alleen door de SVB goedgekeurde autorisatiematrixen implementeren.

IBP-30	Informatiebeveiliging & Privacy	De Opdrachtnemer dient conform afspraken in de Overeenkomst de toegangsrechten van zijn medewerkers die werkzaamheden uitvoeren ten behoeve van de geleverde Dienstverlening te controleren (SOLL / IST vergelijking) en eventuele afwijkingen onmiddellijk te corrigeren.
IBP-31	Informatiebeveiliging & Privacy	Hardening met betrekking tot de Oplossing dient in geval van uiteindelijk beheer door de SVB 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 SVB moet voldoen.
IBP-32	Informatiebeveiliging & Privacy	De Opdrachtnemer dient volgens een beschreven en geïmplementeerd Security hardening beleid en proces de hardening van alle ICT-component die betrokken zijn bij de Oplossing te controleren en/of uit te voeren en gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBP-33	Informatiebeveiliging & Privacy	De Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over afgesproken relevante KPI's (af te stemmen na Gunning) met betrekking tot het security hardening proces inclusief de status van de opvolging/afhandeling van geconstateerde bevindingen.
IBP-34	Informatiebeveiliging & Privacy	Vulnerability Management met betrekking tot de Oplossing dient in geval van beheer door de SVB 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 SVB moet voldoen.
IBP-35	Informatiebeveiliging & Privacy	De Opdrachtnemer dient voor in gebruikname van een nieuwe of significante aanpassing op de Oplossing een kwetsbaarheidsscanner uit te voeren en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBP-36	Informatiebeveiliging & Privacy	De 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 Oplossing en indien noodzakelijk gepaste maatregelen te nemen op basis van geconstateerde bevindingen.
IBP-37	Informatiebeveiliging & Privacy	De Opdrachtnemer dient conform afspraken in de overeenkomst te rapporteren over afgesproken relevante KPI's (afstemmen na Gunning) met betrekking tot vulnerability management inclusief de status van de opvolging/afhandeling van geconstateerde bevindingen.
IBP-38	Informatiebeveiliging & Privacy	Lifecycle en Patch Management met betrekking tot de Oplossing dient in geval van beheer door de SVB 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 SVB moet voldoen.
IBP-39	Informatiebeveiliging & Privacy	De 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 Oplossing.
IBP-40	Informatiebeveiliging & Privacy	De Opdrachtnemer dient ervoor te zorgen dat alle bij de Oplossing 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.
IBP-41	Informatiebeveiliging & Privacy	De 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.
IBP-42	Informatiebeveiliging & Privacy	De 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.
IBP-43	Informatiebeveiliging & Privacy	De Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over afgesproken relevante KPI's (afstemmen na Gunning) met betrekking tot de Lifecycle en Patch Management processen inclusief de status van de opvolging / afhandeling van geconstateerde bevindingen.
IBP-44	Informatiebeveiliging & Privacy	Penetratietesting met betrekking tot de Oplossing dient in geval van beheer door SVB 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 SVB moet voldoen.
IBP-45	Informatiebeveiliging & Privacy	De SVB 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 Oplossing waar de Opdrachtnemer medewerking aan dient te verlenen.
IBP-46	Informatiebeveiliging & Privacy	De Opdrachtnemer dient volgens een beschreven Penetratietesting beleid en proces penetratietest uit te laten voeren door een externe partij op alle ICT-componenten van de Oplossing.
IBP-47	Informatiebeveiliging & Privacy	De Opdrachtnemer dient voor in gebruikname 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.
IBP-48	Informatiebeveiliging & Privacy	De Opdrachtnemer dient conform afspraken in de Overeenkomst te rapporteren over de uitgevoerde penetratietesten inclusief de status van de opvolging/afhandeling van de geconstateerde bevindingen.
IBP-49	Informatiebeveiliging & Privacy	De Oplossing dienen op een gepaste wijze te worden beschermd tegen aanvallen op de gebieden beschikbaarheid, integriteit en vertrouwelijkheid.
IBP-50	Informatiebeveiliging & Privacy	De Opdrachtnemer informeert de SVB ter beoordeling over hoe binnen de aangeboden Oplossing 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).
IBP-51	Informatiebeveiliging & Privacy	De Oplossing dient efficiënte, effectieve, beveiligde en knoeivrije /niet muteerbare signaleringsfuncties (registratie/logging en detectie) te hebben.
IBP-52	Informatiebeveiliging & Privacy	De Oplossing dient audit/logbestanden minimaal 15 maanden (op alle voor de dienstverlening relevante logbestanden) te bewaren voor toekomstig onderzoek en toegangsccontrole.
IBP-53	Informatiebeveiliging & Privacy	De Oplossing dient alleen toegankelijk te zijn voor door de SVB geautoriseerde personen en/of partijen.
IBP-54	Informatiebeveiliging & Privacy	De Oplossing dient de mogelijkheid van af luisteren van netwerkverbindingen en/of het wijzigen van datastromen te verhinderen gebruikmakend van algemeen geaccepteerde best practices.
IBP-55	Informatiebeveiliging & Privacy	De Opdrachtnemer dient gebruik te maken van een veilige ontwikkel- en integratieomgeving ter beheersing van de ontwikkeling c.q. de aanpassing van informatiesystemen.
IBP-56	Informatiebeveiliging & Privacy	De 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.

IBP-57	Informatiebeveiliging & Privacy	De Opdrachtnemer dient media en/of ICT-componenten gerelateerd aan de Oplossing middels een formele procedure op een veilige manier te verwijderen/af te voeren in lijn met een internationaal geaccepteerde standaard.
IBP-58	Informatiebeveiliging & Privacy	De Opdrachtnemer dient te waarborgen dat SVB te allen tijde eigenaar blijft van haar data en tevens haar verantwoordelijkheden als eigenaar kan blijven uitoefenen in alle fases van de data-lifecycle.
IBP-59	Informatiebeveiliging & Privacy	De Oplossing 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.
IBP-60	Informatiebeveiliging & Privacy	De Oplossing 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.
IBP-61	Informatiebeveiliging & Privacy	De Oplossing 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 SVB welke nog in het bezit is van de Opdrachtnemer na overdracht aan de SVB vervolgens op verzoek van de SVB conform daarvoor geldende internationale standaarden vernietigd te worden.
IBP-62	Informatiebeveiliging & Privacy	De Oplossing dient ervoor zorg te dragen dat alle aangeleverde documenten tijdens het gebruik, in lijn met de retentie-policy (moeten door SVB ingesteld kunnen worden, dus variabel) van de SVB, altijd in het aangeleverde formaat beschikbaar blijven.
IBP-63	Informatiebeveiliging & Privacy	De Oplossing 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 SVB.
IBP-64	Informatiebeveiliging & Privacy	De Opdrachtnemer dient op verzoek van de SVB specifieke (log)data, indien nodig realtime, te leveren aan de (externe) Security Operations Center (SOC) en Management Operations Center (MOC) functie van de SVB.
IBP-65	Informatiebeveiliging & Privacy	De 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.
IBP-66	Informatiebeveiliging & Privacy	De Oplossing 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.
IBP-67	Informatiebeveiliging & Privacy	De Oplossing dient qua (cryptografische) beveiligingsmaatregelen te voldoen aan de NCSC-beveiligingsrichtlijnen, dan wel de logische opvolger daarvan.
IBP-68	Informatiebeveiliging & Privacy	De Oplossing dient aantoonbaar geen kwetsbaarheden/kritische beveiligingsrisico's te bevatten zoals beschreven in de meest recente OWASP top 10.
IBP-69	Informatiebeveiliging & Privacy	De 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 Oplossing.
IBP-70	Informatiebeveiliging & Privacy	Opdrachtnemer dient bij het ontwikkelen van (web)applicaties betrokken bij De Oplossing gebruik te maken van Secure Software Development (SSD) methodiek om de Informatiebeveiligings- en Privacyaspecten te borgen.
IBP-71	Informatiebeveiliging & Privacy	De 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 Oplossing.
IBP-72	Informatiebeveiliging & Privacy	De Oplossing dient gedurende de gehele looptijd van de Overeenkomst te voldoen aan van toepassing zijnde wet- en regelgeving, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBP-73	Informatiebeveiliging & Privacy	De Oplossing dient op het gebied van informatiebeveiliging en privacy passende 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.
IBP-74	Informatiebeveiliging & Privacy	De Opdrachtnemer informeert de SVB ter beoordeling over hoe binnen de aangeboden Oplossing 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'.
IBP-75	Informatiebeveiliging & Privacy	De Oplossing dient mogelijkheden te bieden om te allen tijde te voldoen aan verzoeken in het kader van de rechten van betrokkenen.
IBP-76	Informatiebeveiliging & Privacy	De Oplossing 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.
IBP-77	Informatiebeveiliging & Privacy	De Oplossing dient mogelijkheden te bieden om aan de data gerelateerde retentie policies zelfstandig in te regelen of in te laten regelen.
IBP-78	Informatiebeveiliging & Privacy	De Oplossing dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan binnen de Europese Economische Ruimte (EER). Tevens dienen de eventuele (privacy) risico's tot binnen de 'risk tolerance' van de SVB gereduceerd te zijn. Dit geldt ook voor eventuele back-ups!
IBP-79	Informatiebeveiliging & Privacy	De locatie van de Oplossing en de daarbij betrokken medewerkers dienen zich binnen de Europese Economische Ruimte (EER) te bevinden.
IBP-80	Informatiebeveiliging & Privacy	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.
IBP-81	Informatiebeveiliging & Privacy	Voorafgaand aan in productie name van de Oplossing dient een verwerkersovereenkomst afgesloten te zijn tussen de SVB als verwerkingsverantwoordelijke en de Opdrachtnemer of diens onderaannemer als verwerker indien er persoonsgegevens worden verwerkt door de Opdrachtnemer.
IBP-82	Informatiebeveiliging & Privacy	De Opdrachtnemer dient de van SVB ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de SVB te verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeengekomen.
IBP-83	Informatiebeveiliging & Privacy	De Opdrachtnemer dient bij beëindiging van de Dienstverlening de voor de SVB verwerkte persoonsgegevens te retourneren dan wel op verzoek van de SVB te vernietigen, tenzij er sprake is van een wettelijke bewaarplicht.
IBP-84	Informatiebeveiliging & Privacy	De Opdrachtnemer dient een proces te hebben en te hebben geïmplementeerd om datalekken onverwijld, maar uiterlijk binnen 24 uur, aan de Opdrachtnemer te melden.
IBP-85	Informatiebeveiliging & Privacy	De Opdrachtnemer dient de SVB op verzoek te allen tijde te ondersteunen bij de uitoefening van de rechten van betrokkenen en/of de opvolging of afhandeling van datalekken.
IBP-86	Informatiebeveiliging & Privacy	Alle betrokken medewerkers van Opdrachtnemer bij de Dienstverlening dienen een informatiebeveiligings- en/of privacy incident onmiddellijk volgens de standaardprocedure te melden en in ieder geval per mail bij de Servicedesk van de SVB, op het emailadres: servicedesk@svb.nl.

IBP-87	Informatiebeveiliging & Privacy	De 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.
IBP-88	Informatiebeveiliging & Privacy	De 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 SVB en/of aan een door de SVB aangewezen derde partij.
IBP-89	Informatiebeveiliging & Privacy	De Opdrachtnemer dient de SVB het recht te verlenen om een onderzoek (of audit) in te stellen met betrekking tot de naleving van de Overeenkomst. De audit wordt altijd door een onafhankelijke derde partij (auditor) uitgevoerd in samenspraak met de Opdrachtnemer.
IBP-90	Informatiebeveiliging & Privacy	De Opdrachtnemer dient gedurende de looptijd van de Overeenkomst minimaal te beschikken over een of meerdere overeengekomen geldige certificaten en/of gelijkwaardige normeringen en bijbehorende recente formele audit-verklaringen die passend zijn bij de aard van de geleverde dienstverlening (zie voor verdere informatie bijlage 1). De audit-verklaring(en) dient te zijn afgegeven door een onafhankelijke geaccrediteerde auditor waarmee opzet, het bestaan en de werking van een passend stelsel van beveiligings- en privacy maatregelen ten aanzien van de geleverde dienstverlening wordt aangetoond.
IBP-91	Informatiebeveiliging & Privacy	Opdrachtnemer dient een vaste contactpersoon aan te stellen die ten aanzien van de geleverde Dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy (inclusief de wijze van toegang tot deze contactpersoon) voor aanvang van de dienstverlening aan de SVB te communiceren.
IBP-92	Informatiebeveiliging & Privacy	De Opdrachtnemer dient in samenspraak met de SVB een overlegstructuur inclusief periodiek overleggen in te richten om minimaal de overeengekomen opgeleverde rapportages, eventuele issues en ontwikkelingen rond de geleverde dienstverlening te bespreken.
IBP-93	Informatiebeveiliging & Privacy	De Opdrachtnemer dient verantwoording af te leggen over de mate van invulling en effectiviteit van de getroffen beveiligings- en privacy maatregelen en het gerealiseerde beveiligings- & privacy niveau binnen de scope van de geleverde dienstverlening.
IBP-94	Informatiebeveiliging & Privacy	De Opdrachtnemer dient regelmatig te rapporteren behaalde Service levels.
IBP-95	Informatiebeveiliging & Privacy	De Opdrachtnemer moet de continuïteit van de Oplossing waarborgen, ook in geval van calamiteiten en rampen.
IBP-96	Informatiebeveiliging & Privacy	De Opdrachtnemer informeert de SVB, binnen het wettelijke kader, over verzoeken tot aanlevering van persoonsgegevens door buitenlandse inlichtingen- en opsporingsdiensten in het kader van de gevraagde Dienstverlening.
IBP-97	Informatiebeveiliging & Privacy	De Opdrachtnemer dient een proces te hebben geïmplementeerd om security incidenten, betrekking hebbende op de gevraagde Dienstverlening, onverwijld en uiterlijk binnen 24 uur aan de Opdrachtnemer te melden.