Security Annex

Introductie

Schiphol Nederland B.V. (SNBV) erkent dat leveranciers een cruciale rol spelen in het waarborgen van de digitale veiligheid van onze organisatie. Om de risico's van cyberdreigingen te beheersen en een veilige samenwerking te garanderen, hanteert SNBV specifieke voorwaarden en eisen waaraan alle leveranciers moeten voldoen. Deze richtlijnen maken integraal onderdeel uit van onze contractuele afspraken. Leveranciers zijn verplicht om te voldoen aan de vastgestelde beveiligingsstandaarden, inclusief naleving van relevante wet- en regelgeving, implementatie van passende technische en organisatorische maatregelen en het tijdig melden van beveiligingsincidenten.

Deze Security Annex heeft als doel de minimale beveiligingseisen vast te leggen waaraan leveranciers moeten voldoen bij de levering van producten en diensten aan SNBV. SNBV is onderdeel van de nationale kritieke infrastructuur en heeft als essentiële entiteit een zorgplicht vanuit de Cyberbeveiligingswet (Cbw). Daarnaast valt SNBV onder de regels vanuit Part-IS, vastgesteld door het Europees Agentschap voor de veiligheid van de luchtvaart (EASA). De eisen in deze Security Annex zijn gebaseerd op gangbare internationale standaarden, waaronder ISO/IEC 27001, ISF SOGP en het NIST Cybersecurity Framework, en sluiten aan bij deze wettelijke verplichtingen en regels.

Verstoring van onze digitale processen heeft directe gevolgen voor de veiligheid van passagiers, de continuïteit van het luchtverkeer en het vertrouwen in de Nederlandse mainport. Een aanzienlijk deel van onze digitale keten loopt via leveranciers; daarmee worden zij een integraal onderdeel van ons aanvalsoppervlak.

De belangrijkste risicoscenario's die SNBV in haar leveranciersbeleid adresseert zijn onder meer:

- Supply chain-aanvallen, waarbij kwaadwillenden via een gecompromitteerde update, of software-component van een leverancier toegang krijgen tot de omgeving van SNBV.
- Misbruik van leveranciersaccounts en remote access, bijvoorbeeld via gestolen inloggegevens, ontbrekende multifactor-authenticatie (MFA) of te ruime toegangsrechten van beheerders op afstand.
- Ransomware en uitval bij de leverancier, die direct doorwerken in de beschikbaarheid van diensten die voor SNBV bedrijfskritisch zijn.
- Kwetsbaarheden in software, firmware en hardware van derden, inclusief onvoldoende of te traag patchmanagement en het gebruik van end-of-life componenten.
- Datalekken en verlies van vertrouwelijkheid, doordat (persoons)gegevens of operationele informatie van SNBV bij de leverancier onvoldoende beschermd worden opgeslagen, verwerkt of doorgegeven aan subverwerkers.
- Onveilige koppelingen en integraties, zoals onvoldoende beveiligde API's, VPN-verbindingen of beheerinterfaces tussen leverancier en SNBV.
- Insider threats en personeelsrisico's bij de leverancier, waaronder onvoldoende screening, ontoereikende awareness en het niet tijdig intrekken van toegang bij uitdiensttreding.
- Vertraagde of uitblijvende incidentmelding, waardoor SNBV niet tijdig kan reageren, escaleren naar toezichthouders of maatregelen kan treffen om verdere schade te beperken.
- Derde en N-partijrisico's, doordat leveranciers zelf afhankelijk zijn van onderaannemers en Cloud partijen die buiten het zicht van SNBV opereren.

Deze scenario's kunnen zich manifesteren via de leverancierskeketen. Omdat de potentiële impact op luchthavenoperaties, passagiersveiligheid en maatschappelijke continuïteit onevenredig groot is, hecht SNBV er uitermate veel waarde aan dat leveranciers aantoonbaar passende cybersecuritymaatregelen hebben getroffen. Het beheersen van het leveranciersrisico is voor SNBV geen aanvullende wens, maar een randvoorwaarde voor samenwerking met leveranciers.

Niet-naleving van de eisen uit deze Security Annex kan gevolgen hebben voor de contractuele relatie, waaronder het recht van SNBV om audits uit te voeren, de levering op te schorten of in ernstige gevallen de Overeenkomst te beëindigen, onverminderd eventuele aansprakelijkheid van de Leverancier voor schade die voortvloeit uit niet-naleving.

SNBV behoudt zich het recht voor om deze Security Annex periodiek te actualiseren naar aanleiding van gewijzigde wet- en regelgeving, nieuwe dreigingen of voortschrijdend inzicht. Leveranciers worden via hun SNBV-contactpersoon of via de SNBV-website geïnformeerd over materiële wijzigingen. De meest recente versie van deze Security Annex is te allen tijde beschikbaar op de website van SNBV.

De Security Annex is van toepassing op de (informatie)beveiliging van aan [Leverancier] opgedragen (i) levering van goederen, Documentatie, Hardware of Software en (ii) levering of uitvoering van diensten, waaronder SaaS of Onderhoud, zoals bepaald in de Overeenkomst, hierna te noemen: de '**Levering(en)'**.

Deze Security Annex vormt een integraal onderdeel van de Overeenkomst tussen SNBV en de Leverancier en komt tot stand door aanvaarding van de Algemene Inkoopvoorwaarden (IT & Systemen), hierna AIV en/of ondertekening van de Overeenkomst.

Indien SNBV en de Leverancier dit wensen, kunnen zij een aangepaste Security Annex overeenkomen en als bijlage opnemen bij de Overeenkomst of bij een verwerkersovereenkomst. In dat geval vervangt de aangepaste Security Annex deze Security Annex.

Deze Security Annex is van toepassing zolang de Leverancier de Levering(en) aan SNBV levert conform de Overeenkomst en eindigt wanneer de Overeenkomst eindigt, onverminderd verplichtingen die naar hun aard de Overeenkomst overleven (zoals vertrouwelijkheid en veilige teruggave/vernietiging).

De eisen in deze Security Annex zijn van toepassing op de Levering(en) die de [Leverancier] aan SNBV levert, alsmede op alle systemen, personeel, processen en omgevingen die worden ingezet om deze Levering(en) te leveren, te ondersteunen of die de beveiliging daarvan wezenlijk kunnen beïnvloeden. De eisen worden niet ongericht opgelegd aan de gehele organisatie van de Leverancier, maar zijn gericht op de specifieke dienstverlening en de daaraan verbonden risico's.

Welke eisen van toepassing zijn en hoe streng deze worden toegepast, hangt af van de risicoclassificatie (tiering) van de betreffende Levering(en). Bij deze classificatie spelen de volgende factoren een rol: de gevoeligheid van de verwerkte gegevens, de mate van koppeling met de SNBV-omgeving, het belang voor de bedrijfsvoering en de inzet van onderaannemers.

Een aantal eisen geldt echter op organisatieniveau, omdat de Levering deze noodzakelijkerwijs erft en de beveiliging ervan hiervan afhankelijk is. Het betreft onder meer eisen ten aanzien van governance en een managementsysteem voor informatiebeveiliging (zoals ISO 27001-certificering), het beveiligingsbeleid, personele beveiliging, incidentmanagement en de verplichting tot het melden van beveiligingsincidenten en datalekken

De versie van deze Security Annex die van toepassing is, betreft de versie die online beschikbaar is op het moment van (i) aanvaarding van de AIV, of (ii) indien de AIV niet van toepassing is, ondertekening van de Overeenkomst. Indien beide momenten van toepassing zijn, geldt het vroegste moment. SNBV publiceert elke versie van deze Security Annex op haar website met vermelding van de ingangsdatum. Alle eerdere versies blijven digitaal toegankelijk, zodat kan worden vastgesteld welke versie op een specifieke rechtsverhouding van toepassing is geweest.

1. **Definities**
   - 1.1. Begrippen die in deze Security Annex met een hoofdletter zijn aangeduid, maar niet zijn gedefinieerd, hebben de betekenis die daaraan is toegekend in de Overeenkomst en de Algemene Inkoopvoorwaarden (IT & Systemen). Daarnaast hebben de onderstaande begrippen met een hoofdletter aangeduide begrippen de volgende betekenis:
   - 1.2. Security Annex: deze Annex toeziend op de Cyber Security Eisen en Cyber Security Maatregelen.
   - 1.3. Cyber Security Eisen: de concrete, toetsbare vereisten (controls/requirements) op het gebied van informatiebeveiliging die in deze Security Annex zijn opgenomen en die Leverancier dient na te leven
   - 1.4. Cyber Security Maatregelen: de organisatorische en technische maatregelen op het gebied van informatiebeveiliging die Leverancier implementeert en onderhoudt ter naleving van (i) toepasselijke wet- en regelgeving, (ii) de Cyber Security Eisen, en (iii) de Overeenkomst. Daarnaast hanteert Leverancier, voor zover relevant en proportioneel voor de uitvoering van de Overeenkomst, gangbare industry best practices voor de branche waarin Leverancier werkzaam is (zoals ISO/IEC 27000-serie, IEC 62443, ISAE 3402, SOC2, ISF en NIST).
   - 1.5. Cyber Security Risico's: risico's ten aanzien van (het bewaken van) de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, bedrijfsmiddelen, systemen van en dienstverlening aan SNBV.

1.6. Zelfcertificering (CYRA): Het in kaart brengen van het niveau van Informatiebeveiliging via een online zelfevaluatie met de mogelijkheid voor onafhankelijke certificering (https://hetccv.nl/keurmerken/cybersecurity/cyra/).

2. **Risicoprofiel Leveranciers**

2.1. Leverancier is verplicht mee te werken aan (en, indien door SNBV verzocht, informatie te verstrekken ten behoeve van) een door SNBV uit te voeren risicobeoordeling, op basis waarvan SNBV het risicoprofiel van de Leveringen vaststelt. SNBV hanteert drie (3) risicoprofielen:

2.2. **Classificatie Laag:** bij een risicoprofiel 'Laag' verifieert SNBV of de af te nemen Levering voldoet aan de Cyber Security Eisen. Als onderbouwing verstrekt Leverancier op verzoek van SNBV ten minste (i) een (CYRA) zelfverklaring of certificaat en/of (ii) een geldig ISO 27001-certificaat(indien aanwezig). Door SNBV vastgestelde tekortkomingen worden voorafgaand aan de start van de dienstverlening met Leverancier besproken en door Leverancier binnen een door SNBV (na overleg) vast te stellen termijn verholpen, tenzij SNBV deze tekortkomingen schriftelijk als acceptabel risico accepteert.

2.3. **Classificatie Medium:** bij een risicoprofiel 'Medium' verifieert SNBV of de af te nemen Levering voldoet aan de Cyber Security Eisen. Leverancier beschikt gedurende de looptijd van de Overeenkomst over geldige en op de Levering(en) van toepassing zijnde certificeringen en indien daar aanleiding toe is auditrapportages van een onafhankelijke derde, zijnde (i) een ISO/IEC 27001-certificaat of (ii) een SOC 2-rapport (indien door SNBV vereist, Type II), dan wel een door SNBV schriftelijk als gelijkwaardig geaccepteerd certificaat/rapport. Indien de Levering(en) industriële automatiserings- en besturingssystemen (IACS) omvatten, beschikt Leverancier tevens over een aantoonbare implementatie/certificering conform IEC 62443 (relevante onderdelen), zoals door SNBV gespecificeerd. Leverancier verstrekt een kopie van de toepasselijke certificaten/rapporten aan SNBV. De scope daarvan dekt ten minste de dienst/productonderdelen en ondersteunende processen die relevant zijn voor de Levering(en). Door SNBV vastgestelde tekortkomingen worden voorafgaand aan de start van de dienstverlening besproken en door Leverancier binnen een door SNBV (na overleg) vast te stellen termijn verholpen, tenzij SNBV deze tekortkomingen schriftelijk als acceptabel risico accepteert.

2.4. **Classificatie Hoog:** bij een risicoprofiel 'Hoog' verifieert SNBV of de af te nemen Levering voldoet aan de Cyber Security Eisen. Leverancier beschikt gedurende de looptijd van de Overeenkomst over geldige en op de Levering(en) van toepassing zijnde certificeringen en/of auditrapportages van een onafhankelijke derde bestaande uit (i) een ISO/IEC 27001-certificaat of gelijkwaardig en daarnaast (ii) een SOC 2 Type II-rapport of ISAE 3402-rapport, dan wel een door SNBV schriftelijk als gelijkwaardig geaccepteerde assurance-rapportage. Indien de Levering(en) industriële automatiserings- en besturingssystemen (IACS) omvatten, beschikt Leverancier tevens over aantoonbare implementatie/certificering conform IEC 62443 (relevante onderdelen), zoals door SNBV gespecificeerd. Leverancier verstrekt aan SNBV een kopie van de toepasselijke certificaten en de bijbehorende (audit)rapportages. De scope daarvan dekt ten minste de (online) dienst en/of het product en de ondersteunende processen die relevant zijn voor de Levering(en). Door SNBV vastgestelde tekortkomingen worden voorafgaand aan de start van de dienstverlening besproken en door Leverancier binnen een door SNBV (na overleg) vast te stellen termijn verholpen, tenzij SNBV deze tekortkomingen schriftelijk als acceptabel risico accepteert.

2.5. **Geldigheid Overeenkomst:** Indien Leverancier zich niet houdt aan een door SNBV vastgestelde en schriftelijk bevestigde tijdlijn voor het verhelpen van tekortkomingen (i), of (ii) de vereiste certificeringen en/of auditrapportages niet (tijdig) kan overleggen, niet langer geldig zijn, of worden geschorst of ingetrokken, is SNBV gerechtigd de Overeenkomst geheel of gedeeltelijk op te zeggen na schriftelijke ingebrekestelling en het ongebruikt verstrijken van een redelijke hersteltermijn. SNBV is gerechtigd de Overeenkomst met onmiddellijke ingang geheel of gedeeltelijk te beëindigen zonder rechterlijke tussenkomst indien (a) de tekortkoming naar haar aard niet herstelbaar is, of (b) onmiddellijke beëindiging redelijkerwijs noodzakelijk is ter beperking van (cyber)security-, continuïteits- of compliance-risico's. Leverancier heeft in geval van beëindiging op grond van dit artikel geen aanspraak op enige (schade)vergoeding wegens die beëindiging.
Leverancier toont ten minste jaarlijks en daarnaast op verzoek van SNBV aan dat de in het toepasselijke risicoprofiel genoemde certificeringen en/of auditrapportages nog geldig zijn.

3. **Verantwoordelijkheden en naleving Cyber Security Eisen**

3.1. De Leverancier is gehouden om voor haar eigen rekening en risico tijdens de looptijd van de Overeenkomst de Cyber Security Maatregelen te implementeren, na te komen, te evalueren, in stand te houden en op verzoek hierover te rapporteren aan SNBV.

3.2. De Leverancier beschikt over een gedocumenteerd beleid voor basismaatregelen op het gebied van cyberhygiëne dat minimaal de volgende onderwerpen omvat:
- Het bijhouden van een actuele inventaris van software, hardware en digitale activa die worden ingezet bij de Levering(en) aan SNBV;
- Het verwijderen of wijzigen van standaard (factory default) inloggegevens op alle systemen voorafgaand aan productie-inzet;
- Het uitschakelen van onnodige services, protocollen en netwerkpoorten op alle voor de Levering(en) gebruikte systemen;
- Een procedure voor het veilig buiten gebruik stellen en het wissen van data op systemen die worden afgestoten of hergebruikt.

3.3. De Leverancier ziet er actief op toe dat zijn medewerkers en eventuele bij de uitvoering van de Overeenkomst betrokken derden, zoals onder-opdrachtnemers, toeleveranciers, adviseurs en financiers voldoen aan Cyber Security Eisen en Leverancier verstrekt hen daartoe een kopie van de Security Annex.

3.4. De Leverancier controleert en evalueert periodiek of zijn onderneming en de in het kader van de Overeenkomst door hem geleverde producten en/of diensten voldoen aan de verplichtingen volgend uit deze Security Annex. Indien en zodra de Leverancier gedurende de looptijd van de Overeenkomst niet of niet langer kan voldoen c.q. verwacht te kunnen voldoen aan één of meer verplichtingen volgend uit deze Security Annex, stelt hij SNBV hiervan direct schriftelijk op de hoogte. Partijen bespreken in dat geval of Leverancier alternatieve Cyber Security Maatregelen kan nemen die voor SNBV acceptabel zijn.

3.5. Op verzoek van SNBV verstrekt de Leverancier schriftelijke rapportages die aantonen dat Leverancier en eventuele door hem bij de uitvoering van de Overeenkomst betrokken derden voldoen aan de verplichtingen uit deze Security Annex.

3.6. De Leverancier is verantwoordelijk voor het voorkomen en beheersen van alle Cyber Security Risico's die zich (kunnen) voordoen in het kader van de uitvoering van de Overeenkomst door de Leverancier. De Leverancier zet riskmanagement in om de Cyber Security Risico's te identificeren en te mitigeren door het treffen van organisatorische en technische risicobeperkende Cyber Security Maatregelen en de werking hiervan te evalueren.

3.7. Indien de Leverancier bij de uitvoering van de Overeenkomst een Cyber Security Risico constateert, rapporteert de Leverancier SNBV hier schriftelijk over binnen 7 kalenderdagen na constatering van het betreffende risico. Een dergelijke rapportage bevat minimaal het volgende:
   a. Omschrijving van het cyber security risico;
   b. Een voorstel voor beheersmaatregelen om het risico te voorkomen, weg te nemen, te mitigeren of over te dragen;
   c. De termijn waarbinnen de onder b) genoemde maatregelen zullen worden uitgevoerd.

3.8. Op verzoek daartoe van SNBV, ondersteunt de Leverancier SNBV bij het nakomen van de verplichtingen die gelden voor Royal Schiphol Group N.V. als 'aanbieder van een essentiële dienst' op grond van de Cyberbeveiligingswet (NIS2-richtlijn) en het bijbehorende besluit.

3.9. De Leverancier stelt SNBV voorafgaand op de hoogte van voorgenomen materiële wijzigingen in zijn informatiebeveiligingsmanagementsysteem (ISMS) die van invloed kunnen zijn op de veiligheid, beschikbaarheid of luchtvaart veiligheid gerelateerde aspecten van de Levering(en) aan SNBV. Materiële wijzigingen omvatten onder meer:
- Wijziging van uitbestede beveiligingsdiensten (zoals SOC, SIEM of incident response provider);
- Vervanging of migratie van Cloud infrastructuur die wordt gebruikt voor de Levering(en);
- Reorganisatie van de structuur en besturing voor informatiebeveiliging binnen de organisatie van de Leverancier;
- Significante aanpassingen aan de scope of risicobeheermethode van het ISMS.

3.10. Voor luchtvaart veiligheid gerelateerde Leveringen meldt de Leverancier materiële ISMS-wijzigingen tevens bij de bevoegde autoriteit conform IS.D.OR.255 / IS.I.OR.255 en informeert SNBV over de inhoud en het tijdstip van die melding.

4. **IT Service Management**
   4.1. De Leverancier draagt er zorg voor om *industry best practices* rondom IT Service Management te implementeren en te onderhouden, zoals beschreven in frameworks zoals ITIL. Deze *industry best practices* moeten ervoor zorgen dat de IT-diensten van de Leverancier effectief en efficiënt worden beheerd en geleverd, in lijn met de eisen en verwachtingen van SNBV.

5. **Medewerkers en Ingeschakelde derden**
   5.1. De Leverancier draagt er zorg voor dat alle bij de uitvoering van de Overeenkomst betrokken medewerkers en door hem ingeschakelde derden zowel bij aanvang als tijdens de looptijd van de Overeenkomst, training(en) op het gebied van cyber security ontvangen, passend bij hun functie en hun verantwoordelijkheden bij het verrichten van de werkzaamheden in het kader van de Overeenkomst. Om aan deze verplichting te kunnen voldoen, verzorgt de Leverancier in ieder geval een security awareness programma, opleidingen en trainingsactiviteiten op basis van op dat moment geldende *industry best practices*.
   5.2. De Leverancier draagt er zorg voor dat vóór aanvang van de Overeenkomst een antecedentenonderzoek is uitgevoerd bij de bij de uitvoering van de Overeenkomst betrokken medewerkers en/of ingeschakelde derden. Slechts in geval van een positieve uitkomst krijgen deze personen/instanties toegang tot (de voor de Overeenkomst relevante) informatie, bedrijfsmiddelen, systemen en dienstverlening van SNBV. Dit onderzoek dient te worden uitgevoerd volgens geldende wet- en regelgeving en ethische normen en dient in verhouding te staan tot de aard en omvang van de toegang die de betreffende medewerkers en/of ingeschakelde derden (nodig) zullen hebben tot de informatie, bedrijfsmiddelen, systemen en dienstverlening van SNBV.
   5.3. De Leverancier draagt er zorg voor dat gedurende de looptijd van de Overeenkomst een formele disciplinaire procedure van toepassing is op haar rechtsverhouding met medewerkers en ingeschakelde derden welke procedure de gevolgen bepaalt van het niet voldoen aan Cyber Security Eisen door een medewerker of ingeschakelde derde. De disciplinaire procedure dient te zijn opgesteld volgens de geldende *industry best practice*. Deze procedure voorziet in ieder geval in de bevoegdheid van de Leverancier tot onmiddellijke schorsing en intrekking van toegangsrechten en privileges tot de informatie en systemen van SNBV in geval er een vermoeden is dat de voor omschreven schending het gevolg is van opzet of bewuste roekeloosheid. De Leverancier dient dergelijke gevallen per omgaande schriftelijk te rapporteren aan SNBV.

6. **Toegangsbeheer**
   6.1. De bij de uitvoering van de Overeenkomst ingezette medewerkers en/of ingeschakelde derden hebben slechts toegang tot die onderdelen van de informatie, bedrijfsmiddelen en systemen en tot de locaties van de dienstverlening van SNBV voor zover benodigd voor de uitvoering van hun werkzaamheden binnen hun functie en in het kader van de Overeenkomst (het zogenoemde *least privilege*-principe).
   6.2. De Leverancier zorgt ervoor dat elk account persoonsgebonden is – dus persoonlijk uitgegeven aan een individuele gebruiker en niet aan een groep of afdeling – zodat altijd traceerbaar is welke gebruiker wat heeft gedaan. Groepsaccounts en functionele accounts zijn niet toegestaan, tenzij SNBV hier expliciet aan de Leverancier toestemming voor heeft gegeven.
   6.3. De Leverancier houdt een lijst bij van alle bij de dienstverlening betrokken medewerkers en ingeschakelde derden die toegang hebben tot informatie, bedrijfsmiddelen, en systemen van SNBV. Gedurende de dienstverlening controleert de Leverancier deze lijst ten minste elke 90 dagen om ervoor te zorgen dat het least-privilege-principe nagekomen wordt en achtergebleven/overtollige accounts worden verwijderd.

7. **Risicoanalyses, technische risk assessments en audits (Right to Audit)**
   7.1. SNBV heeft gedurende looptijd van de Overeenkomst het recht om voor haar rekening risicoanalyses, technische risk assessments (waaronder penetratietests) en audits op de dienstverlening van de Leverancier — uit te voeren of te laten uitvoeren door onafhankelijke derde partijen. De Leverancier is gehouden hieraan zijn medewerking te verlenen en deze risicoanalyses, technische risk assessments en audits mogelijk te maken, onder andere door relevante informatiebeveiligingsbeleidsstukken, standaarden, procesomschrijvingen, documentatie en informatie tijdig en volledig beschikbaar te stellen aan SNBV.
   7.2. Een risicoanalyse, technische risk assessment of audit als bedoeld in lid 1 van dit artikel vindt: (a) maximaal eenmaal per jaar plaats; en (b) leidt tot opstelling van een vertrouwelijk rapport. SNBV verstrekt een kopie van het rapport aan Leverancier.

De Leverancier voert binnen de afgesproken tijdsperiode alle preventieve en/of correctieve acties uit op bevindingen die geïdentificeerd zijn als resultaat van de bedoelde risicoanalyses, technische risk assessments en audits.

7.3. Voor zover de Levering(en) activiteiten betreffen die vallen binnen de reikwijdte van EASA Part-IS (IS.D.OR.235 of IS.I.OR.235), erkent de Leverancier dat SNBV als luchthavenoperator te allen tijde verantwoordelijk (accountable) blijft voor de naleving van de toepasselijke Part-IS verplichtingen jegens de bevoegde autoriteit (ILT of EASA), ook wanneer uitvoerende taken zijn uitbesteed aan de Leverancier. De Leverancier verleent op eerste verzoek medewerking aan audits en inspecties uitgevoerd door of namens de bevoegde autoriteit die betrekking hebben op de Levering(en), en stelt daartoe alle benodigde documentatie, systemen en medewerkers beschikbaar.

8. **Netwerk-, Communicatie- en Endpoint beveiliging**

8.1. De Leverancier neemt alle beheersmaatregelen conform de meest recente *industry best practices* die nodig zijn om de beschikbaarheid, vertrouwelijkheid en integriteit van gegevens die via fysieke netwerken of draadloze netwerken worden verstuurd, aangesloten systemen en applicaties te beschermen. Geschikte beheersmaatregelen betreffen onder andere Firewalls, Proxies, Intrusion Detection System en Intrusion Prevention Systems, netwerk segmentatie en monitoring oplossingen.

8.2. De Leverancier neemt alle beheersmaatregelen die nodig zijn om alle voor de dienstverlening gebruikte endpoints (b.v. servers, werkstations en laptops) te beschermen tegen malware. In dat kader voorziet de Leverancier de endpoints van anti-malware managementsoftware, waarvan de signatures minimaal eenmaal per dag automatisch worden bijgewerkt, en monitort hij het continue op verdachte activiteiten.

8.3. In aanvulling op het voorgaande voorziet de Leverancier alle endpoints die toegang hebben tot of gebruikt worden voor de verwerking van SNBV-informatie van een Endpoint Detection and Response (EDR) of gelijkwaardige oplossing die voorziet in continue monitoring, detectie van geavanceerde aanvalstechnieken en mogelijkheid tot geautomatiseerde of handmatige response (zoals isolatie van een endpoint). Detecties die kunnen wijzen op een beveiligingsincident met betrekking tot de Levering(en) of SNBV-informatie worden behandeld conform artikel 15.

8.4. De Leverancier dient gebruik te maken van cryptografische bewerkingen om de gegevens die hij verwerkt te beveiligen. Leverancier past encryptie (versleuteling) toe bij verzending van gegevens via netwerken, bij de opslag van gegevens op (draagbare) apparatuur, en op verwijderbare media, zoals usb-sticks en in andere situaties waar gegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld gegevens die via het internet kunnen worden benaderd). Hiervoor wordt encryptie op basis van actuele standaarden gebruikt die bijgewerkt wordt wanneer blijkt dat de gebruikte standaarden niet meer voldoen aan gestelde eisen:

a) Voor opslag van data is het gebruik van veilige technologie zoals de Advanced Encryption Standard (AES) technologie met 256 bits sleutels of langer verplicht. Alle sleutels die hiervoor gebruikt worden moeten adequaat beheerd worden, zodat ze niet toegankelijk zijn voor ongeautoriseerden en/of misbruikt worden.

b) Voor websites, -applicaties en -services maakt de Leverancier gebruik van beveiligde verbindingen, om het netwerkverkeer tussen de cliënt en de webserver te beschermen tegen inzage of wijziging door derden. De Leverancier draagt er zorg voor dat zijn websites, -applicaties en -services gebruik maken van certificaten die zijn uitgegeven door een erkende publieke Certificate Authority (CA), zoals Digicert. Het certificaat voldoet aan de courante eisen van de CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. Self-signed certificaten zijn niet toegestaan.

9. **Wachtwoorden**

9.1. De Leverancier draagt er zorg voor dat wachtwoorden van alle accounts, zowel van beheerders als gebruikers die de Leverancier inschakelt, worden opgeslagen met een veilig, actueel one-way-hash mechanisme (inclusief unieke salt).

9.2. De Leverancier zorgt ervoor dat wachtwoorden voor user accounts met toegang tot SNBV-data en systemen sterk zijn en voldoen aan de richtlijnen en best practices zoals die zjjn opgesteld door het National Institute of Standards and Technology (NIST SP 800-63B Guidelines). Wachtwoorden worden vervangen bij een vermoeden van inbreuk of een beveiligingsincident. Voorzieningen zoals multi-factor authenticatie (MFA) en een wachtwoordkluis worden aanbevolen om de toegang verder te beveiligen.

9.3. Wachtwoorden voor beheeraccounts die door de Leverancier gebruikt worden moeten ten minste 16 karakters lang zijn en voldoen aan de richtlijnen conform NIST SP 800-63B. Nieuwe en bestaande wachtwoorden worden gescreend tegen een actuele blocklist van veelvoorkomende en in datalekken aangetroffen wachtwoorden, en geweigerd indien daarop voorkomend. Wachtwoorden worden niet

periodiek vervangen, maar uitsluitend bij een vermoeden van inbreuk of een beveiligingsincident, of indien de blocklist-screening dit alsnog vereist. Bij voorkeur dient de Leverancier gebruik te maken van een Privileged Access Management (PAM) systeem om de toegang tot beheeraccounts te beheren en monitoren.

9.4. De Leverancier zorgt ervoor dat sterke authenticatie (zoals MFA) wordt gebruikt voor (i) accounts met verhoogde rechten van de Leverancier, (ii) toegang tot systemen die gevoelige gegevens verwerken, en (iii) toegang op afstand via het internet.

9.5. Indien de Leverancier andere methoden en maatregelen wil hanteren ter bescherming van accounts, die het gebruik van wachtwoorden vervangen, dient SNBV deze maatregelen vooraf eerst goed te keuren.

10. **Patching & hardening**

10.1. De software die de Leverancier inzet of levert bij de uitvoering van de Overeenkomst (OS, database, middleware en applicatiesoftware) is voorzien van alle bekende security patches zoals door de Leverancier, ontwikkelaar of programmeur zijn uitgebracht en deze worden bij het uitkomen van de patches conform onderstaande tabel toegepast of geleverd:

Categorie	CVSS v3 Base score	Hersteltijd voor internet verbonden applicatie.	Hersteltijd voor niet internet verbonden applicaties
Laag	0,0 - 3,9	Zo snel als mogelijk	Zo snel als mogelijk
Medium	4,0 - 6,9	1 maand	2 maanden
Hoog	7,0 – 8.9	2 weken	1 maand
Kritiek	9.0 -10	Uiterlijk binnen 48 uur	2 weken

10.2. De Leverancier verzorgt hardening van de systemen en software in lijn met de CIS-benchmark hardingstandaarden (en indien die niet beschikbaar zijn, dan volgens de hardingstandaarden van de leverancier) om een veilige configuratie te borgen.

10.3. De Leverancier verzorgt automatische periodieke controle op eventuele missende patches met een tool op de systemen om te controleren of security patches volgens bovenstaande schema worden uitgevoerd en rapporteert hierover.

a. Maandelijks wordt een rapportage opgesteld waarin de status van de laatste patches en hardening activiteiten wordt beschreven. Dit rapport wordt opgesteld door de Leverancier en op aanvraag geleverd aan SNBV.

b. Het rapport bevat informatie over de laatste patches die zijn uitgebracht, welke systemen zijn gepatcht en welke systemen nog moeten worden gepatcht. Daarnaast wordt informatie gegeven over de hardening activiteiten die zijn uitgevoerd, welke systemen zijn gehardened en welke systemen nog moeten worden gehardened.

10.4. Indien er kritieke kwetsbaarheden worden ontdekt, maakt de Leverancier hier direct melding van aan SNBV en worden er meteen aanvullende maatregelen genomen om deze kwetsbaarheden te verhelpen.

10.5. De Leverancier houdt een release kalender bij voor alle hiervoor genoemde software en hardware en anticipeert op ‘end of life’ notificaties door ten minste 12 maanden voor einde support met SNBV te overleggen over een passend upgrade project.

11. **Accountbeheer**

11.1. De Leverancier dient voor de onder de Overeenkomst geleverde producten en/of diensten de SNBV Identity Acces Management omgeving (SCIM-compliant) te gebruiken voor accountbeheer.

11.2. Indien de Leverancier niet (langer) aan de SNBV Identity Acces Management procedure kan voldoen, bespreken Partijen gezamenlijk een alternatieve procedure voor accountbeheer, waarna de Leverancier het voorstel voor een alternatieve procedure ter acceptatie voorlegt aan SNBV. Na schriftelijke acceptatie door SNBV van dit alternatief, draagt de Leverancier er zelf zorg voor dat hij formele procedures heeft en in stand houdt voor het tijdig aanmaken, muteren en verwijderen van (beheer)accounts, waarbij onder ‘tijdig’ wordt verstaan binnen 92 kalenderdagen.

12. **Vernietigen en migratie van gegevens**

12.1. In aanvulling op de bepalingen in de Overeenkomst die toezien op persoonsgegevens, geldt dat de Leverancier alle uit hoofde van of in verband met de Overeenkomst verkregen overige gegevens van SNBV

niet langer bewaren dan noodzakelijk en na afloop van de Overeenkomst of op verzoek van SNBV vernietigen, met inachtneming van de wettelijke bewaartermijnen.

12.2. Bij beëindiging van het contract wordt de intrekking van fysieke en logische toegangsrechten tot de informatie van de organisatie uitgevoerd.

12.3. Leverancier is verplicht mee te werken aan de datamigratie naar een andere leverancier of naar de eigen systemen van SNBV.

13. **Continuïteit**

13.1. De Leverancier neemt alle noodzakelijke IT technische maatregelen ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen en zo de continuïteit van zijn verplichtingen tot leveren van producten en/of diensten onder de Overeenkomst aan SNBV te waarborgen. Geschikte maatregelen betreffen onder andere het implementeren van een robuust back-up systeem om gegevensverlies te voorkomen, het opstellen en regelmatig testen van een noodherstelplan (disaster recovery en restore plan), en het zorgen voor voldoende en gekwalificeerd personeel om de dienstverlening te waarborgen, zelfs bij ziekte of afwezigheid van sleutelpersonen.

13.2. De Leverancier zorgt voor bedrijfscontinuïteitsplannen en noodherstelregelingen die betrekking hebben op de Levering(en) aan SNBV.

13.3. Op verzoek worden testen uitgevoerd op basis van realistische scenario's die aansluiten bij de mate van belangrijkheid van de Levering(en) voor SNBV. Scenario's omvatten ten minste: uitval van een primaire datacenterlocatie, ransomware-aanval en verlies van kritieke sleutelfunctionarissen.

13.4. Op verzoek stelt de Leverancier binnen 30 kalenderdagen na afronding van de test een samenvatting beschikbaar van de testresultaten, inclusief geïdentificeerde tekortkomingen en het bijbehorende herstelplan.

14. **Bedrijfsmiddelen**

14.1. Alle apparatuur van de Leverancier die opslagmedia bevat, zoals laptops of smartphones, wordt door de Leverancier ontdaan van de nog eventueel aanwezige gegevens, alvorens het apparaat te verwijderen of hergebruiken. De gegevens moeten onherstelbaar worden gewist of, als de media niet onherstelbaar gewist kan worden dan moet de media onherstelbaar en aantoonbaar worden vernietigd.

14.2. De Leverancier zorgt ervoor dat de gevoelige gegevens niet bekend worden gemaakt aan onbevoegde partijen.

14.3. De Leverancier beschikt over een (Software) Bill of Materials ((S)BOM). Indien gevraagd door SNBV kan aangegeven worden of er gebruik gemaakt wordt van specifieke componenten.

15. **Beveiligingsincidenten en meldplicht**

15.1. Indien de Leverancier een beveiligingsincident met betrekking tot informatie, bedrijfsmiddelen en systemen (van SNBV en/of Leverancier) of dienstverlening uit hoofde van de Overeenkomst heeft geïdentificeerd, dient de Leverancier dit exclusief en onmiddellijk, maar in ieder geval binnen 24 uur nadat de Leverancier daarmee bekend is geraakt, aan de SNBV ICT Servicedesk te melden.

15.2. Meldingen die worden gedaan onder deze Security Annex dient Leverancier te richten aan de ICT Servicedesk van SNBV:
ICT Servicedesk
Tel: +31 (0) 20 – 6014445
e-mail: itservicedesk@schiphol.nl
De ICT Servicedesk is 24 uur per dag, 7 dagen per week telefonisch bereikbaar. Indien een melding onder deze Security Annex wordt gedaan, dient de Leverancier daarnaast ook de contactpersoon zoals opgenomen in de Overeenkomst op de hoogte te stellen.

15.3. Een melding aan de ICT Servicedesk dient ten minste de volgende informatie te bevatten:

- Begin-, en eindtijd, begin-, en einddatum en de locatie van de gebeurtenis;
- Aard en de omvang van de gebeurtenis;
- De afdeling of gedeelte van het systeem, waar de gebeurtenis zich voordeed;
- De tijd, benodigd om de schade door het incident vast te stellen;
- De aard en omvang van de getroffen gegevens;
- Soort en (inschatting van) aantal getroffen betrokkenen, componenten en systemen
- De te verwachten gevolgen, met inbegrip van de gevolgen voor betrokkenen, componenten en systemen en een voorstel om schade en andere negatieve gevolgen te voorkomen;
- Getroffen en nog te treffen maatregelen om gevolgen van het incident te mitigeren; én

- De naam en contactgegevens van de functionaris gegevensbescherming of ander contactpersoon, waar additionele informatie betreffende het incident kan worden verkregen.

15.4. Indien SNBV hierom verzoekt, dient de Leverancier een onderzoek naar het informatiebeveiligingsincident toe te staan en te ondersteunen.

15.5. De Leverancier verstrekt SNBV tijdig alle informatie die SNBV nodig heeft om te voldoen aan zijn eigen meldplicht jegens het Nationaal Cyber Security Centrum (NCSC) en/of de bevoegde toezichthouder op grond van de Cyberbeveiligingswet. De meldinformatie volgt het onderstaande schema:

15.6. Binnen 24 uur na ontdekking (Vroegtijdige Waarschuwing): een eerste melding met (i) de aard van het incident, (ii) een indicatie of het incident vermoedelijk kwaadwillend van aard is, en (iii) of mogelijke grensoverschrijdende gevolgen niet kunnen worden uitgesloten;

- Binnen 72 uur na ontdekking (Incidentmelding): een nadere melding met (i) een initiële impactbeoordeling (ernst en reikwijdte), (ii) beschikbare indicatoren van compromittering (IoC's), en (iii) de getroffen systemen, diensten en gegevens;
- Binnen één maand na ontdekking (Eindverslag): een definitief verslag met (i) een volledige beschrijving van het incident inclusief vermoedelijke oorzaak, (ii) de toegepaste en nog te treffen maatregelen, en (iii) de geleerde lessen.
- Indien een beveiligingsincident tevens een datalek betreft in de zin van de AVG, stelt de Leverancier SNBV hiervan onverwijld op de hoogte, zodat SNBV tevens kan beoordelen of een melding bij de Autoriteit Persoonsgegevens vereist is binnen de daarvoor geldende termijn van 72 uur.

15.7. De Leverancier voorziet in een vast contactpunt, Single Point of Contact (SPOC) welke 24/7 bereikbaar is voor SNBV in geval van een significant incident en welke gemachtigd is om namens de Leverancier te handelen in het kader van de meldingsprocedure. Het vaste contactpunt heeft voldoende senioriteit en competentie om beveiligingskwesties effectief aan te pakken.

15.8. Voor zover de Leverancier een door EASA gecertificeerde organisatie is of anderszins onder het toepassingsbereik van EASA Part-IS valt, en een informatiebeveiligingsincident verband houdend met de Levering(en) aan SNBV wordt door hem geclassificeerd als significant in de zin van IS.D.OR.230 of IS.I.OR.230, stelt de Leverancier SNBV hiervan onverwijld en in elk geval binnen 24 uur op de hoogte. De Leverancier informeert SNBV tevens zodra een dergelijk incident door hem is gerapporteerd aan de bevoegde autoriteit (ILT of EASA), inclusief de inhoud van de melding voor zover dit de Levering(en) aan SNBV betreft. Deze verplichting bestaat naast en onverminderd de meldplicht op grond van artikel 15.1 t/m 15.7.

16. ECAC Common Evaluation Practice goedgekeurde middelen

16.1. Securitycomponenten goedgekeurd door de European Civil Aviation Conference (ECAC) en gebaseerd op het ‘Common Evaluation Process’ (https://www.ecac-ceac.org/activities/security/common-evaluation-process-cep-of-security-equipment) zijn uitgezonderd van best practices/standaarden en eventuele toekomstige wijzigingen als dit de Common Evaluation Process goedkeuring in gevaar brengt. Leverancier dient SNBV hierover tijdig te informeren zodat partijen aanvullende maatregelen overeen kunnen komen.

17. Artificial Intelligence Security

17.1. De Leverancier stelt vast welke AI-systemen of -toepassingen worden ingezet bij de uitvoering van de Overeenkomst en legt deze vast in een AI-register dat op verzoek aan SNBV beschikbaar wordt gesteld.

17.2. De Leverancier past een AI-beveiligingskader toe dat minimaal de volgende onderwerpen omvat:

- Risicobeheersing van AI-gegenereerde uitvoer die invloed kan hebben op de vertrouwelijkheid, integriteit of beschikbaarheid van SNBV-informatie;
- Bescherming van trainingsdata en ML-modellen tegen ongeoorloofde toegang, manipulatie of datavergiftiging (data poisoning);
- Periodieke validatie van de nauwkeurigheid en betrouwbaarheid van AI-systemen die worden ingezet voor beveiligingsdoeleinden.

17.3. De Leverancier zorgt ervoor dat medewerkers die AI-hulpmiddelen gebruiken bij de verwerking van SNBV-informatie specifieke training ontvangen over de beveiligingsrisico's van generatieve AI, waaronder het risico van onbedoelde gegevensoverdracht naar externe modelleveranciers

17.4. De Leverancier informeert SNBV voorafgaand aan de inzet van nieuwe of gewijzigde AI-systemen die SNBV-data verwerken of daartoe toegang hebben.

18. Cryptografisch Sleutelbeheer en Post-Quantum Cryptografie

18.1. Cryptografische sleutels worden beschermd door middel van Hardware Security Modules (HSM) of een equivalent beveiligd sleutelopslagsysteem. Toegang tot sleutels is strikt beperkt tot geautoriseerde systemen en personen op basis van het least-privilege-principe.

18.2. De Leverancier bewaart een actueel overzicht van alle cryptografische algoritmen die worden ingezet voor de verwerking van SNBV-data en evalueert jaarlijks of deze voldoen aan de actuele normen (o.a. NIST, BSI, ENISA).

18.3. De Leverancier ontwikkelt en onderhoudt een transitiestrategie voor post-quantum cryptografie (PQC) conform de NIST PQC-standaarden. De Leverancier informeert SNBV op verzoek over de voortgang van de transitie en stelt de bijbehorende roadmap beschikbaar.

19. Forensisch Onderzoek en Digitale Bewijsborging

19.1. De Leverancier beschikt over een gedocumenteerde procedure voor het bewaren van digitaal bewijsmateriaal bij informatiebeveiligingsincidenten die SNBV raken. Deze procedure waarborgt de integriteit, aaneensluitende bewakingsketen (chain of custody) van het bewijsmateriaal.

19.2. De leverancier ondersteunt de organisatie in geval van juridische procedures waarbij informatie van de organisatie betrokken is (bijv. verzoeken om elektronische bewijsvergaring (e-discovery) of forensisch onderzoek).

19.3. Indien SNBV hierom verzoekt na een incident, draagt de Leverancier er zorg voor dat relevante logbestanden, systeemkopieën (forensische images), netwerkcapturedata en authenticatiegegevens worden veiliggesteld en voor de duur van ten minste 90 kalenderdagen – of langer indien juridische procedures dit vereisen – worden bewaard.

19.4. De Leverancier wijst een contactpersoon aan die verantwoordelijk is voor forensische onderzoeksactiviteiten en werkt samen met door SNBV ingeschakelde forensisch onderzoekers, mits dit niet in strijd is met toepasselijke wet- en regelgeving.

19.5. Bevindingen uit forensisch onderzoek worden vertrouwelijk behandeld en uitsluitend gedeeld met door SNBV aangewezen partijen.

20. Informatieclassificatie en -behandeling

20.1. De leverancier inventariseert alle informatiemiddelen van SNBV die hij ontvangt, verwerkt of opslaat in het kader van de Overeenkomst en classificeert deze overeenkomstig het door SNBV gehanteerde classificatieschema (of een aantoonbaar gelijkwaardig schema).

20.2. De Leverancier behandelt informatie in overeenstemming met het classificatieniveau en past passende maatregelen toe voor opslag, verzending, toegang, reproductie en vernietiging per classificatiecategorie.

20.3. Indien SNBV geen classificatieschema heeft medegedeeld, hanteert de Leverancier minimaal de volgende categorieën: Openbaar, Intern, Vertrouwelijk en Strikt Vertrouwelijk, en past hierop de beveiligingsmaatregelen toe die binnen zijn eigen organisatie voor dergelijke classificaties gelden.

20.4. Alle dragers (fysiek en digitaal) die SNBV-informatie bevatten op het niveau Vertrouwelijk of hoger, worden voorzien van een duidelijke markering en worden opgeslagen in beveiligde omgevingen.

21. Gegevensbescherming en Privacy

21.1. De Leverancier verwerkt persoonsgegevens die hij in het kader van de Overeenkomst ontvangt of genereert uitsluitend voor de doeleinden zoals overeengekomen in de Overeenkomst (of verwerkersovereenkomst) en in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en overige toepasselijke privacywetgeving.

21.2. De Leverancier past het beginsel van dataminimalisatie toe: er worden niet meer persoonsgegevens verwerkt dan strikt noodzakelijk voor de uitvoering van de Overeenkomst.

21.3. Indien de Leverancier een inbreuk in verband met persoonsgegevens (datalekmelding) constateert, meldt hij dit onverwijld – doch uiterlijk binnen 24 uur – aan SNBV conform artikel 15, zodat SNBV kan beoordelen of melding bij de Autoriteit Persoonsgegevens vereist is.

21.4. Op verzoek van SNBV verstrekt de Leverancier informatie ten behoeve van een gegevensbeschermingseffectbeoordeling (DPIA) en werkt hij mee aan het uitvoeren daarvan.

22. Fysieke Beveiliging

22.1. De Leverancier treft passende fysieke beveiligingsmaatregelen voor alle locaties waar SNBV-informatie, -systemen of -bedrijfsmiddelen aanwezig zijn of worden verwerkt. Passende maatregelen omvatten in ieder geval:
- Toegangscontrole op basis van geautoriseerde identiteitsverificatie (bijv. toegangspas, biometrie);
- Beveiliging van serverruimten en datacenters conform de IEC 62443- of ISO/IEC 27001-normen voor fysieke beveiligingszones;
- Camera- en alarminstallaties, alsmede inbraakdetectie bij kritieke faciliteiten.

22.2. Toegang van onbevoegde personen tot ruimten waarin SNBV-systemen of -data zijn opgeslagen, wordt gelogd en gemonitord. Bezoekers worden te allen tijde begeleid.

22.3. De Leverancier beschikt over maatregelen ter bescherming van kritieke utiliteitsvoorzieningen (stroom, koeling) om de continuïteit van de Levering(en) te waarborgen.

22.4. Op verzoek van SNBV verstrekt de Leverancier inzage in de relevante fysieke beveiligingsmaatregelen en de bijbehorende auditrapportages.

23. Security Event Logging en Monitoring

23.1. De Leverancier implementeert en onderhoudt een centrale logging- en monitoringoplossing met centrale tijdbron (NTP), die alle relevante beveiligingsgebeurtenissen registreert die betrekking hebben op de Levering(en) aan SNBV. Gelogde gebeurtenissen omvatten ten minste: inlogpogingen (geslaagd en mislukt), configuratiewijzigingen, toegang tot gevoelige data en systeemfouten.

23.2. De leverancier registreert indien van toepassing op de geleverde dienst activiteiten met ten minste de volgende gegevens: accountnaam, tijdstip, activiteit, systeemidentificatie en, indien van toepassing, netwerkadres. Activiteiten omvatten zowel aan- en afmeldingen bij de systemen als mislukte aanmeldpogingen. Het uitvoeren van transacties wordt in het systeem geregistreerd.

23.3. Logbestanden worden beschermd tegen ongeoorloofde wijziging of verwijdering en worden ten minste 12 maanden bewaard (of langer indien toepasselijke wet- en regelgeving dit voorschrijft).

23.4. Op verzoek van SNBV – in het bijzonder in het kader van een beveiligingsincident, risicoanalyse of audit als bedoeld in artikel 7 – stelt de Leverancier relevante logbestanden tijdig beschikbaar.

23.5. De Leverancier monitort beveiligingsgebeurtenissen actief en stelt escalatieprocedures in werking wanneer drempelwaarden voor verdachte activiteiten worden overschreden.

24. Veilige Softwareontwikkeling (SDLC)

24.1. Indien de Leverancier in het kader van de Overeenkomst software ontwikkelt, aanpast of levert, past de Leverancier een gedocumenteerde Secure Software Development Lifecycle (SSDLC) toe die minimaal omvat:
- Beveiligingsvereisten gebaseerd op risicoanalyse als integraal onderdeel van de specificatiefase;
- Statische code-analyse (SAST) en dynamische applicatietesting (DAST) vóór elke productierelease;
- Beoordeling van open-source- en derde-partijcomponenten op bekende kwetsbaarheden (SCA – Software Composition Analysis) met inachtneming van de SBOM-verplichting uit artikel 14.3.

24.2. Kritieke beveiligingsbevindingen uit code-reviews of testactiviteiten worden verholpen voorafgaand aan productierelease, tenzij SNBV een gedocumenteerde uitzondering schriftelijk accepteert.

24.3. De Leverancier maakt gebruik van veilige ontwikkelomgevingen die logisch of fysiek gescheiden zijn van productieomgevingen.

24.4. Productiedata wordt niet gebruikt in test- of ontwikkelomgevingen, tenzij geanonimiseerd of gepseudonimiseerd. Gevoelige informatie, zoals persoonsgegevens, wordt niet verwerkt in een ontwikkel-, test- en/of acceptatieomgeving.

25. Werken op Afstand

25.1. De Leverancier zorgt ervoor dat medewerkers en ingeschakelde derden die op afstand toegang hebben tot systemen of informatie van SNBV, dit uitsluitend doen via een versleutelde verbinding (minimaal TLS 1.2 of VPN met AES-256) en een door de Leverancier beheerd, gehardend eindpuntapparaat.

25.2. Toegang op afstand is onderworpen aan sterke authenticatie (MFA) conform artikel 9.4 en vindt standaard plaats via de door SNBV beheerde Privileged Access Management (PAM) oplossing.

25.3. De Leverancier beschikt over beleid voor veilig thuiswerken dat de omgeving van de medewerker beschermt tegen ongeoorloofde inzage van SNBV-informatie (bijv. schermvergrendeling, gebruik van privénetwerken, verbod op gebruik van niet-goedgekeurde cloudopslag).

26. N-party (Sub-leverancier) Risicobeheer

26.1. In aanvulling op ***artikel 3.2*** beschikt de Leverancier over een formeel programma voor het beheer van N-party risico's (risico's verbonden aan sub-leveranciers en toeleveranciers die een rol spelen bij de Levering(en) aan SNBV).

26.2. De Leverancier biedt voor aanvang van de samenwerking inzicht in hoe ze taken uitbesteden of onderaannemers inschakelen.

26.3. De Leverancier voert vóór aanvang van de samenwerking een beveiligingsbeoordeling uit van alle kritieke sub-leveranciers en herhaalt deze beoordeling jaarlijks of bij materiële wijzigingen in de dienstverlening.

26.4. De Leverancier stelt SNBV op verzoek in kennis van de namen van kritieke sub-leveranciers die toegang hebben tot SNBV-systemen of -data. SNBV heeft het recht om een sub-leverancier af te wijzen op grond van beveiligingsrisico's, na overleg met de Leverancier.

26.5. De Leverancier neemt contractuele verplichtingen op ten aanzien van informatiebeveiliging in overeenkomsten met kritieke sub-leveranciers die minimaal gelijkwaardig zijn aan de verplichtingen in deze Security Annex.

26.6. In lijn met artikel 21 lid 2 onder d van de NIS2-richtlijn en de EU Uitvoeringsverordening (C(2024)7151) beschikt de Leverancier over een gedocumenteerde beoordeling van de cybersecurityrisico's verbonden aan de componenten, software, hardware en diensten van zijn eigen toeleveranciers die worden ingezet bij de Levering(en) aan SNBV. De Leverancier stelt een samenvatting van deze beoordeling op verzoek beschikbaar aan SNBV.

26.7. De Leverancier neemt in zijn eigen contracten met kritieke toeleveranciers cybersecurityverplichtingen op die minimaal gelijkwaardig zijn aan de verplichtingen in deze Security Annex, en toont dit op verzoek aan SNBV aan. Dit vereiste geldt voor toeleveranciers die toegang hebben tot SNBV-data of -systemen, of wier producten of diensten integraal onderdeel uitmaken van de Levering(en) aan SNBV.

27. **Bestuurlijke Verantwoordelijkheid en Zorgplicht (NIS2 Art. 20)**

27.1. De Leverancier zorgt ervoor dat het bestuur of de directie van de Leverancier de Cyber Security Maatregelen die worden toegepast bij de uitvoering van de Overeenkomst, heeft goedgekeurd en actief toezicht houdt op de naleving en effectiviteit hiervan, conform artikel 20 van de NIS2-richtlijn en de daarmee corresponderende bepalingen van de Cyberbeveiligingswet.

27.2. De bestuurders en leidinggevenden van de Leverancier die betrokken zijn bij de Levering(en) hebben aantoonbaar een cyberbeveiligingsopleiding of -training gevolgd die hen in staat stelt de onder het vorige lid bedoelde goedkeuring weloverwogen te geven en de relevante cybersecurityrisico's te beoordelen. De Leverancier bewaart documentatie van deze trainingen.

27.3. Op verzoek van SNBV toont de Leverancier aan dat aan de verplichtingen in dit artikel is voldaan door overlegging van een verklaring van het bestuur, een trainingscertificaat of een gelijkwaardig bewijsmiddel.

27.4. Indien de Leverancier zelf een essentiële of belangrijke entiteit is in de zin van de Cyberbeveiligingswet, stelt de Leverancier SNBV hiervan op de hoogte en verstrekt hij op verzoek bewijs van zijn eigen registratie en naleving.

28. Threat Intelligence en Informatiedeling

28.1. De Leverancier beschikt over een proces voor het verzamelen, beoordelen en toepassen van threat intelligence dat relevant is voor de Levering(en) aan SNBV, teneinde dreigingen tijdig te onderkennen en risico-gebaseerde beveiligingsbeslissingen te ondersteunen.

28.2. De Leverancier deelt onverwijld met SNBV informatie over dreigingen, indicatoren van compromittering (IoC's) of aanvalspatronen die direct relevant kunnen zijn voor de Levering(en), de systemen of de data van SNBV. Deze verplichting bestaat naast de meldplicht uit artikel 15.

29. Kwetsbaarhedenbeheer

29.1. In aanvulling op artikel 10 (Patching & hardening) hanteert de Leverancier een gedocumenteerd proces voor kwetsbaarhedenbeheer dat ten minste voorziet in: (i) het periodiek en geautomatiseerd identificeren van technische kwetsbaarheden in de systemen, applicaties en componenten die worden ingezet voor de Levering(en); (ii) risico-gebaseerde prioritering op basis van CVSS-score en bedrijfsimpact; en (iii) tijdige remediation conform de hersteltijden uit artikel 10.1.

29.2. De Leverancier abonneert zich op relevante kwetsbaarheidsmeldingen, zoals CISA Known Exploited Vulnerabilities (KEV), NCSC-NL en leveranciersadviezen) en past dit toe op de eigen Bill of Materials (zie artikel 14.3) om bekend uitgebuite kwetsbaarheden in voor de Levering(en) gebruikte componenten met voorrang te verhelpen.

30. Cloudbeveiliging

30.1. Indien de Levering(en) clouddiensten (zoals SaaS, PaaS of IaaS) omvatten of daarop steunen, stelt de Leverancier SNBV op de hoogte van de identiteit van de onderliggende cloud service provider(s), de geografische locatie(s) waar SNBV-data wordt opgeslagen en verwerkt, en de toepasselijke verantwoordelijkheidsverdeling (shared responsibility model).

30.2. De Leverancier past beveiligingsmaatregelen toe die passend zijn voor het gebruikte Cloud model, waaronder ten minste: veilige configuratie conform CIS Benchmarks of een gelijkwaardige standaard, logische scheiding (tenant isolation) tussen SNBV-data en die van andere klanten, beheer van identiteiten en toegang conform artikel 6 en 9, en encryptie van data in rust en in transit conform artikel 8.4.

30.3. Op verzoek van SNBV toont de Leverancier aan dat de cloud-omgeving voldoet aan een erkend certificeringsschema (zoals ISO/IEC 27017, ISO/IEC 27018 of CSA STAR), aanvullend op de in artikel 2 vereiste certificeringen.

31. Wijzigingsbeheer (Change Management)

31.1. De Leverancier hanteert een gedocumenteerd wijzigingsbeheerproces dat borgt dat wijzigingen aan systemen, applicaties of infrastructuur die de Levering(en) ondersteunen, worden geautoriseerd, getest en gecontroleerd doorgevoerd zonder de beveiliging, beschikbaarheid of integriteit van de dienstverlening aan SNBV in gevaar te brengen.

31.2. De Leverancier informeert SNBV vooraf over geplande wijzigingen die een materiële invloed kunnen hebben op de wijze waarop de Levering(en) worden geleverd, waaronder wijzigingen in (sub)leveranciers, beveiligingsfunctionaliteit, authenticatiemechanismen, dataverwerkingslocaties of integraties met systemen van SNBV. Deze verplichting geldt onverminderd de meldplicht uit artikel 3.9.

31.3. Spoedwijzigingen (emergency changes) worden alleen doorgevoerd indien noodzakelijk en achteraf formeel beoordeeld en gedocumenteerd; SNBV wordt zo spoedig mogelijk geïnformeerd over spoedwijzigingen die de Levering(en) raken.

32. Contract beëindiging

32.1. Dit artikel is van toepassing op iedere beëindiging van de Overeenkomst, ongeacht de grondslag (afloop van rechtswege, opzegging, ontbinding of beëindiging op grond van artikel 2 of een andere bepaling van de Overeenkomst). De Leverancier hanteert een gedocumenteerd proces voor contractbeëindiging dat ten minste het volgende vereist: (a) tijdige en gestructureerde teruggave of migratie van alle SNBV-informatie en -gegevens conform artikel 12, in een door SNBV bruikbaar formaat; (b) aantoonbare en onomkeerbare vernietiging van resterende SNBV-informatie bij de Leverancier en diens N-parties conform artikel 12, met overlegging van een vernietigingsverklaring; (c) intrekking van alle toegangsrechten, accounts en authenticatiemiddelen die aan de Leverancier en diens medewerkers en N-parties zijn toegekend voor de Levering(en), conform artikel 6 en 11; (d) overdracht van voor de continuïteit van de dienstverlening relevante kennis, documentatie en operationele informatie aan SNBV of aan een door SNBV aan te wijzen opvolgende leverancier; (e) voortdurende naleving van licentieovereenkomsten en bescherming van intellectuele eigendomsrechten, waaronder geheimhouding, niet-gebruik en non-disclosure ten aanzien van SNBV-informatie, broncode, ontwerpen en andere beschermde materialen, ook na beëindiging van de Overeenkomst en voor de duur waarin de relevante rechten of verplichtingen voortbestaan; en (f) duidelijk vastgelegde bewaartermijnen per categorie gegevens die de Leverancier nog mag aanhouden vóór definitieve verwijdering, waarbij de bewaartermijn niet langer is dan strikt noodzakelijk voor het doel waarvoor deze geldt.

32.2. Ten behoeve van het bepaalde in lid 1 onder (f) legt de Leverancier per categorie gegevens (waaronder ten minste: persoonsgegevens, vertrouwelijke bedrijfsinformatie van SNBV, logbestanden, back-ups en gegevens die op grond van een wettelijke bewaarplicht moeten worden bewaard) de toegestane bewaartermijn vast, de juridische of operationele grondslag voor die termijn, en de wijze waarop verwijdering aantoonbaar plaatsvindt. Tenzij een langere termijn wettelijk verplicht of door partijen schriftelijk overeengekomen is, geldt voor SNBV-informatie een maximale bewaartermijn van negentig (90) dagen na de feitelijke beëindigingsdatum.

32.3. De Leverancier verstrekt SNBV op verzoek, doch in ieder geval binnen dertig (30) dagen na de feitelijke beëindigingsdatum, een schriftelijke bevestiging waarin per onderdeel (a) tot en met (f) van lid 1 wordt aangetoond dat aan de daar opgenomen verplichtingen is voldaan, met inbegrip van de vernietigingsverklaring bedoeld onder (b) en het overzicht van bewaartermijnen bedoeld in lid 2.