Security Annex

Introductie
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.

De Security Annex is van toepassing op de (informatie)beveiliging van aan [Leverancier] [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 versie van deze Security Annex die van toepassing is, betreft de versie die op het moment van aanvaarding van de AIV, dan wel het tot stand komen van de Overeenkomst, online beschikbaar is. Alle eerdere versies blijven digitaal toegankelijk teneinde vast te kunnen stellen 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 ingevulde en ondertekende zelfcertificering (CYRA) 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 hierover te rapporteren aan SNBV.
   3.2. 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.
   3.3. 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.

3.4. 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.

3.5. 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.

3.6. 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.

3.7 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.

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 vooromschreven 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**

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.

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. De Leverancier dient gebruik te maken van cryptografische bewerkingen om de gegevens die hij verwerkt te beveiligen. Hij 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). 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 heel sterk zijn, en ten minste 16 karakters lang zijn met karakters uit ten minste drie categorieën zoals hoofdletters, kleine

letters, nummers en speciale karakters. Deze wachtwoorden moeten na maximaal 180 dagen vervangen worden of bij een vermoeden van inbreuk of een beveiligingsincident. 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 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**

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.

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 Bill of Materials. Indien gevraagd door SNBV kan aangegeven worden of er gebruik gemaakt wordt van specifieke componenten.

15. **Beveiligingsincidenten**

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.

16. **ECAC Common Evaluation Practice goedgekeurde middelen**

Securitycomponenten goedgekeurd door de European Civil Aviation Conference (ECAC) en gebaseerd op het ‘Common Evaluation Process’ 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.