



Security Annex

uitgave 1-10-2022

Security Annex

Betrouwbare informatievoorziening en digitale oplossingen zijn cruciaal om de *purpose* van Eindhoven Airport waar te maken; daarnaast moeten we ons houden aan de zich voortdurend ontwikkelende wet- en regelgeving en standaarden die gelden in ons werkveld. In deze situatie kan een onzorgvuldige omgang met gegevens – aldan niet bewust – onze bedrijfsvoering, reputatie of financiële positie bedreigen, en zijn informatie- en cyberdreigingen niet alleen IT-risico's, maar ook ondernemingsrisico's.

Met deze Security Annex geven we cyber security formeel een actieve en zichtbare plek binnen onze organisatie en committeren we ons aan een hoog niveau van cyber security naar al onze stakeholders.

Colofon

Security Annex

Uitgave 1-10-2022

Versie 2.0

Auteur Bas Kluijtmans

Classificatie Intern

Eindhoven Airport N.V.

Office Luchthavenweg 13

Telefoon +31 (0) 40 2919 9829

Terminal Luchthavenweg 25,

5657 EA Eindhoven

Security Annex

Inhoudsopgave

Hoofdstuk 1

Over dit Document	4
-------------------	---

Hoofdstuk 2

Het beheersen van informatiebeveiligingsrisico's	4
Eisen aan de opdrachtnemer's medewerkers en ingeschakelde derden	5
Toegangsbeheer	5
Penetratietesten, audits, technische risk assessments	6
Netwerk-, Communicatie- en Endpoint beveiliging	6
Wachtwoorden	7
Multi-factor authenticatie	7
Patching & hardening	7
Accountbeheer	8
Vernietigen van gegevens	8
Bedrijfsmiddelen	8
Beveiligingsincidenten	8
Meldingen onder de Security Annex	9



Hoofdstuk 1

Over dit Document

Deze Security Annex bevat de key security controls die we van onze opdrachtnemers/ leveranciers eisen bij de levering van producten en/of diensten, en wordt als bijlage bij de hoofdovereenkomst opgenomen. Alleen als er géén hoofdovereenkomst maar wél een Verwerkersovereenkomst wordt gesloten, wordt de Security Annex als bijlage bij de Verwerkersovereenkomst opgenomen. Verwijder in dat geval punt 12 omdat dit al in de hoofdtekst van de Verwerkersovereenkomst staat.

Let op: Alle tekst in **rood** dient ingevuld, aangepast of verwijderd te worden alvorens dit document te delen met de opdrachtnemer/ leverancier. Eventuele wijzigingen aan de security eisen dienen altijd goedgekeurd te worden door de Information Security Officer (ISO) van EANV, neem daarvoor contact op via: cyber@eindhovenairport.nl. In het voortraject hoeft de ISO niet betrokken te worden tenzij er vragen of onduidelijkheden zijn.

Voorbehoud: *de opdrachtnemer is alleen verantwoordelijk voor hetgeen binnen zijn invloedssfeer valt.*

- A. De opdrachtnemer is gehouden alle met de uitvoering van de Opdracht verband houdende cyber security maatregelen te treffen en implementeren die redelijkerwijs van hem kunnen worden verwacht en die voldoen aan de op dat moment geldende industry good practices. Onder 'opdrachtnemer' worden tevens verstaan: zijn medewerkers en eventuele door hem ingeschakelde derden, waaronder onderaannemers, onderopdrachtnemers, toeleveranciers, adviseurs en financiers. De opdrachtnemer treft voorgenoemde maatregelen voor eigen rekening en risico.
- B. Meer specifiek, de opdrachtnemer's cyber security maatregelen omvatten ten minste:



Hoofdstuk 2

Het beheersen van informatiebeveiligingsrisico's

- 1.1. De opdrachtnemer is verantwoordelijk voor het beheersen van alle cyber security risico's die zich (kunnen) voordoen in het kader van de uitvoering van de Opdracht door de opdrachtnemer. In dit kader zal de opdrachtnemer proactief alle informatiebeveiligingsrisico's identificeren, beperkende c.q. mitigerende cyber security maatregelen treffen en evalueren.
- 1.2. De opdrachtnemer controleert ten minste eens per jaar of de in het kader van de Opdracht door hem verstrekte dienstverlening voldoet aan de bepalingen zoals in deze Security Annex uiteengezet en rapporteert op verzoek aan EANV over de mate waarin zijn organisatie voldoet aan de bepalingen van deze Annex.
- 1.3. Indien de opdrachtnemer een risico constateert ten aanzien van (het bewaken van) de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, bedrijfsmiddelen, systemen van en dienstverlening aan EANV, dient de opdrachtnemer EANV hierover zo spoedig mogelijk maar uiterlijk binnen 7 dagen schriftelijk te informeren. Een dergelijke mededeling bevat minimaal het volgende:

- a. het risico dat EANV loopt.
 - b. de voorgestelde beheersmaatregelen om het risico te verminderen, te vermijden of over te dragen en datum/tijdstip waarop deze uiterlijk worden getroffen.
- 1.4. De opdrachtnemer zorgt ervoor dat de (hosting) dienst gedurende de uitvoering van de Opdracht c.q. duur van de Overeenkomst gecertificeerd is volgens [naam certificering] (bijv. ISO 27001 of PCI DSS).

Eisen aan de opdrachtnemer's medewerkers en ingeschakelde derden

- 2.1 De opdrachtnemer draagt er zorg voor dat ieder van de bij de uitvoering van de Opdracht betrokken medewerkers en door hem ingeschakelde derden de juiste training op het gebied van informatiebeveiliging hebben ontvangen in het kader van hun functie en gelet op de verantwoordelijkheden bij het verrichten van de werkzaamheden in het kader van de Opdracht. Om aan deze verplichting te kunnen voldoen, verzorgt de opdrachtnemer in ieder geval een security awareness programma, opleidingen en trainingsactiviteiten op basis van geldende good practices. Daarnaast informeert de opdrachtnemer de bij de dienstverlening betrokken medewerkers en ingeschakelde derden over de vereisten door EANV gesteld in deze Security Annex.
- 2.2 De opdrachtnemer draagt er zorg voor dat vóór aanvang van de Opdracht een anteceden-tenonderzoek is uitgevoerd bij de bij de uitvoering van de Opdracht betrokken medewerkers en/of ingeschakelde derden. Slechts in geval van een positieve uitkomst krijgen deze personen/instanties toegang tot (de voor de Opdracht relevante) informatie, bedrijfsmiddelen, systemen en dienstverlening van EANV. 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 EANV. In het bijzonder is een Verklaring van Geen Bezwaar voor Burgerluchtvaart (VGB) vereist voor medewerkers en/of ingeschakelde derden die in het kader van de Opdracht toegang zullen krijgen tot beveiligd gebied, accounts met verhoogde rechten, kritieke informatiesystemen en/of bedrijfsgevoelige informatie van EANV.
- 2.3 De opdrachtnemer dient te beschikken over een formele disciplinaire procedure voor medewerkers en ingeschakelde derden die een veiligheidsinbreuk hebben gepleegd of niet voldoen aan informatiebeveiligingsvereisten van EANV (zoals vastgelegd in deze Security Annex), volgens de geldende good practice. In ernstige gevallen van wangedrag dient deze procedure te voorzien in onmiddellijke schorsing en intrekking van toegangsrechten en privileges met betrekking tot de informatie en systemen van EANV. De opdrachtnemer dient dergelijke gevallen per omgaande schriftelijk te rapporteren aan EANV.

Toegangsbeheer

- 3.1 De bij de dienstverlening betrokken medewerkers en ingeschakelde derden hebben slechts toegang tot die onderdelen van de informatie, bedrijfsmiddelen en systemen van EANV alsmede van de locaties van de dienstverlening die benodigd zijn voor de uitvoering van hun werkzaamheden binnen hun functie en in het kader van de Opdracht (het zogenoemde *least privilege*-principe).
- 3.2 De opdrachtnemer 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 zijn niet toegestaan.

- 3.3 De opdrachtnemer dient een lijst bij te houden van alle bij de dienstverlening betrokken medewerkers en ingeschakelde derden die toegang hebben tot informatie, bedrijfsmiddelen, en systemen van EANV. Gedurende de dienstverlening dient de opdrachtnemer deze lijst ten minste elke 90 dagen te controleren om te garanderen dat het *least privilege*-principe gehandhaafd blijft en dat eventuele achtergebleven/overtollige accounts worden verwijderd.

Penetratietesten, audits, technische risk assessments

- 4.1 In overleg met de opdrachtnemer en voor zover de kosten en de planning het toelaten, kan EANV risicoanalyses (b.v. penetratietests), technische risk assessments, security scans (b.v. PCI compliance scans) en audits op de opdrachtnemer's dienstverlening – inclusief informatiesystemen waarop EANV data worden verwerkt – uitvoeren of laten uitvoeren door onafhankelijke derde partijen. De opdrachtnemer stelt voor deze activiteiten relevante informatiebeveiligingsbeleidsstukken, standaarden, procesomschrijvingen, documentatie en informatie beschikbaar. De opdrachtnemer voert binnen de afgesproken tijdlijn correctieve acties uit op bevindingen die geïdentificeerd worden tijdens door EANV uitgevoerde audits/technische risk assessments.

Netwerk-, Communicatie- en Endpoint beveiliging

- 5.1 De opdrachtnemer dient beheersmaatregelen te nemen om de vertrouwelijkheid en integriteit van gegevens die via openbare netwerken of draadloze netwerken worden verstuurd te beschermen conform de laatste stand van techniek en tevens om de aangesloten systemen en applicaties te beschermen. Geschikte maatregelen betreffen onder andere Firewalls, Proxys, IDS/IPS, netwerk segmentatie en monitoring oplossingen.
- 5.2 De opdrachtnemer dient beheersmaatregelen te nemen om alle voor de dienstverlening gebruikte endpoints (b.v. servers, werkstations en laptops) te beschermen tegen malware, door deze te voorzien van anti-malware management software, waarvan de signatures minimaal één maal per dag automatisch worden bijgewerkt, en het netwerk te monitoren op verdachte activiteiten.
- 5.3 De opdrachtnemer dient gebruik te maken van cryptografische bewerkingen om de (persoons)gegevens die hij verwerkt te beveiligen. Hij past encryptie (versleuteling) toe bij verzending van (persoons)gegevens via netwerken, bij de opslag van (persoons)gegevens op (draagbare) apparatuur en op verwijderbare media, zoals usb-sticks en in andere situaties waar (persoons)gegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld (persoons)gegevens die via het internet kunnen worden benaderd). Voorbeelden van toegestane technologie zijn VPN's, SSH of HTTPS of een vergelijkbare technologie voor netwerkbeveiliging.
- 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 ongeautoriseerde en/of misbruikt worden.
 - Voor websites, -applicaties en -services zal de opdrachtnemer gebruik maken van beveiligde verbindingen zoals HTTPS, om het netwerkverkeer tussen de cliënt en de webserver te beschermen tegen inzagte of wijziging door derden.
 - De opdrachtnemer draagt er zorg voor dat zijn websites, -applicaties en -services gebruik maken van TLS certificaten die zijn uitgegeven door een erkende publieke Certificate Authority (CA) zoals Digicert en VeriSign. Het certificaat zal voldoen 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.

Wachtwoorden

- 6.1 De opdrachtnemer zorgt ervoor dat wachtwoorden van alle accounts, zowel van beheerders als gebruikers, worden opgeslagen met een veilig one-way-hash mechanisme zoals SHA-2 of SHA-3 met een "salt" toevoeging.
- 6.2 De opdrachtnemer zorgt ervoor dat wachtwoorden voor user accounts met toegang tot EANV data en systemen sterk zijn, dat wil zeggen ten minste 12 karakters lang en geen repeterend patroon. Deze wachtwoorden moeten na maximaal 180 dagen vervangen worden, waarbij de laatste 10 wachtwoorden niet hergebruikt mogen worden.
- 6.3 Wachtwoorden voor beheeraccounts die door de opdrachtnemer gebruikt worden moeten heel sterk zijn, dat wil zeggen ten minste 15 karakters lang en geen repeterend patroon. Deze wachtwoorden moeten na maximaal 180 dagen vervangen worden, waarbij de laatste 10 wachtwoorden niet hergebruikt mogen worden.
- 6.4 Wachtwoorden voor serviceaccounts – waarmee niet wordt ingelogd door een menselijke gebruiker maar door een ander informatiesysteem/applicatie, bijvoorbeeld voor data-uitwisseling of automatische taken – die door de opdrachtnemer gebruikt worden moeten heel sterk zijn, dat wil zeggen ten minste 24 karakters lang en geen repeterend patroon. Deze wachtwoorden moeten na maximaal 5 jaar vervangen worden, waarbij de laatste 10 wachtwoorden niet hergebruikt mogen worden.

Multi-factor authenticatie

- 7.1 Multi-factor-authenticatie dient gebruikt te worden voor accounts met verhoogde rechten van de opdrachtnemer, voor toegang tot systemen die gevoelige (persoons)gegevens verwerken, en voor toegang op afstand via het internet.

Patching & hardening

- 8.1 De software die door de opdrachtnemer wordt ingezet of geleverd (OS, database, middleware en applicatiesoftware) is voorzien van alle bekende security patches zoals de opdrachtnemer, ontwikkelaar of programmeur heeft 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

- 8.2 De opdrachtnemer verzorgt hardening van de systemen en software in lijn met de CIS standaarden (dan wel de security richtlijnen van de leverancier) om een veilige configuratie te borgen.

Accountbeheer

- 9.1 De opdrachtnemer draagt er zorg voor dat hij formele procedures heeft en in stand houdt voor het tijdig aanmaken, muteren en verwijderen van (beheer)accounts. Een account dat 90 dagen niet gebruikt is dient gedeactiveerd of gewist worden.

Vernietigen van gegevens

- 10.1 De opdrachtnemer draagt er zorg voor dat gegevens tijdig en conform de (wettelijke) bewaartermijn worden vernietigd.

Bedrijfsmiddelen

- 11.1 Alle apparatuur van de opdrachtnemer die opslagmedia bevat, zoals laptops of smartphones, wordt door de opdrachtnemer ontdaan van de nog eventueel aanwezige (persoons)gegevens, alvorens het apparaat te verwijderen of hergebruiken. De (persoons)gegevens moeten onherstelbaar worden gewist of, als de media niet onherstelbaar gewist kan worden, dan moet de media onherstelbaar worden vernietigd.
- 11.2 De opdrachtnemer zorgt ervoor dat de gevoelige (persoons)gegevens niet bekend worden gemaakt aan onbevoegde partijen.

Beveiligingsincidenten

- 12.1 Indien de opdrachtnemer eventuele feitelijke of veronderstelde beveiligingsincidenten met betrekking tot informatie, bedrijfsmiddelen, systemen of dienstverlening heeft geïdentificeerd, dient de opdrachtnemer dit exclusief en onmiddellijk, maar in ieder geval binnen 24 uur nadat de opdrachtnemer daarmee bekend is geraakt, aan EANV te melden.
- 12.2 Een melding aan de IT Servicedesk dient ten minste de volgende informatie te bevatten:
- de begin-, en eindtijd, de begin-, en einddatum en de locatie van de gebeurtenis;
 - de 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 (persoons)gegevens;
 - soort en (inschatting van) aantal getroffen Betrokkenen
 - de te verwachten gevolgen, met inbegrip van de gevolgen voor Betrokkenen 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 andere contactpersoon, waar additionele informatie betreffende het incident kan worden verkregen.
- 12.3 Indien EANV hierom verzoekt, dient de opdrachtnemer een onderzoek naar het informatiebeveiligingsincident toe te staan en te ondersteunen.

Meldingen onder de Security Annex

- 13.1 Meldingen die worden gedaan onder deze Security Annex dienen te worden gericht aan de IT Servicedesk van EANV:

IT Servicedesk

Tel: +31 (0) 40 – 2919847

e-mail: IT@eindhovenairport.nl

De ICT Servicedesk is 24 uur per dag, 7 dagen per week telefonisch bereikbaar.

- 13.2 Indien een melding onder deze Security Annex wordt gedaan, dient de opdrachtnemer daarnaast ook de contactpersoon zoals opgenomen in de Overeenkomst daarvan op de hoogte te stellen.