

Security Annex Informatiebeveiliging

INHOUD

Security Annex Informatiebeveiliging	1
1. Toepasselijkheid en normenkader	2
2. Cloud governance en CSP-beleid	3
3. Cloud soevereiniteit en datalokalisatie	3
4. Change-of-contract en wijzigingsclausule	4
5. Assurance, audits en toetsing	4
6. Continuïteit, RTO en RPO	6
7. Pentesten (alleen van toepassing bij software ontwikkeling)	7
8. Leveranciersketen en subverwerkers	7
9. Incidentmelding en transparantie	8
10. Exit, datateruggave en vernietiging	9
11. Prevalentie van deze annex	9
12. Sancties, boetes en ontbinding	9
Verdiepende maatregelen	11
13. Contact, communicatie en beveiligingskanalen	11
14. Authenticatie en accounts	12
15. Werkplekken en toegangsvoorzieningen	12
16. Toekenning en gebruik van administratieve rechten	12
17. Tenant-brede en hoogste beheerdersrechten	13
18. Secure Software Development Lifecycle (SSDLC) (alleen van toepassing bij software ontwikkeling)	13

1. Toepasselijkheid en normenkader

(BIO2: 5.01.01, 5.02.01, 5.35.01)

1.1 Leverancier verklaart dat de dienstverlening gedurende de gehele looptijd van de overeenkomst, tot en met overdracht, afwikkeling en aantoonbare vernietiging van data, voldoet aan de eisen uit deze Security Annex en aantoonbaar in lijn is met de voor de dienstverlening relevante beveiligingsmaatregelen uit de geldende versie van de Baseline Informatiebeveiliging Overheid (BIO), thans BIO2, dan wel opvolgende versies, of dat aantoonbaar gelijkwaardige maatregelen zijn getroffen, passend bij de aard van de dienstverlening, de verwerkte gegevens en het risicoprofiel.

1.2 Leverancier beschikt over een werkend en gecertificeerd Information Security Management System (ISMS) conform de laatst geldende en actuele versie van NEN-EN-ISO/IEC 27001 of een opvolgende norm, waarbij expliciet is geborgd dat de relevante BIO-maatregelen onderdeel vormen van scope, risicoanalyse, beheersmaatregelen en audits.

1.3 Leverancier verklaart te voldoen aan alle op de dienstverlening toepasselijke geldende en toekomstige wet- en regelgeving op het gebied van informatiebeveiliging, cybersecurity, gegevensbescherming en archivering, waaronder begrepen maar niet beperkt tot:

- de Baseline Informatiebeveiliging Overheid (BIO) in de geldende versie;
- de Cyberbeveiligingswet (NIS2) en het Cyberbeveiligingsbesluit, alsmede opvolgende wetgeving;
- de bijbehorende uitvoeringsregelgeving, waaronder Uitvoeringsverordening (EU) 2024/2690 en opvolgende verordeningen;
- de Algemene Verordening Gegevensbescherming (AVG);
- de Archiefwet en onderliggende regelgeving;
- de Cyber Resilience Act (CRA) ;
- overige toepasselijke nationale en Europese wet- en regelgeving, zoals deze van tijd tot tijd wordt gewijzigd of aangevuld.

1.4 Leverancier verplicht zich de dienstverlening gedurende de looptijd van de overeenkomst in te richten en aangepast te houden conform:

- de van toepassing zijnde BIO-overheidsmaatregelen in de geldende versie;
- de geldende bepalingen uit de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit;
- toepasselijke privacy- en archiefwetgeving, alsmede opvolgende of gewijzigde regelgeving.

1.5 Wijzigingen in wet- en regelgeving of normenkaders die gedurende de looptijd van de overeenkomst van toepassing worden, worden door Leverancier onverwijld geïmplementeerd, zonder dat hiervoor een wijziging van deze overeenkomst noodzakelijk is.

2. Cloud governance en CSP-beleid

(BIO2: 5.23.01, 5.20.06)

2.1 Leverancier hanteert een aantoonbaar vastgesteld en geïmplementeerd beleid voor:

- selectie en inrichting van cloudomgevingen
- beheer van datalocaties
- beëindiging en exit van clouddiensten

2.2 In het contract worden expliciet situaties benoemd die aanleiding vormen tot ontbinding, waaronder:

- structurele niet-naleving van beveiligingseisen
- wezenlijke wijzigingen in eigendom, zeggenschap of jurisdictie
- verlies van relevante certificeringen

3. Cloud soevereiniteit en datalokalisatie

(BIO2: 5.19, 5.20, 5.21.01, 5.21.02, 5.23.01)

3.1 Gegevens van Opdrachtgever worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER), tenzij voorafgaand schriftelijk anders overeengekomen.

3.2 Leverancier levert de dienstverlening uitsluitend vanuit een soevereine cloud-omgeving binnen de Europese Unie, waarbij geldt dat:

- alle primaire en secundaire datalocaties zich binnen de EU bevinden
- beheerhandelingen uitsluitend plaatsvinden onder EU-jurisdictie (WENS)
- geen structurele afhankelijkheid bestaat van niet-EU beheersentiteiten (WENS)

3.3 Leverancier verklaart te voldoen aan het EU Cloud Sovereignty Framework en borgt dat:

- gegevens niet toegankelijk zijn voor derde landen zonder rechtsgeldige EU-grondslag
- sleutelbeheer uitsluitend plaatsvindt binnen de EU en onder controle van Leverancier
- subverwerkers uitsluitend binnen de EU zijn gevestigd, tenzij vooraf schriftelijk toegestaan

3.4 Leverancier verstrekt jaarlijks een schriftelijke verklaring inzake:

- datalocaties
- betrokken subverwerkers
- toepasselijke jurisdicties en wetgeving

3.5 Tenant-isolatie en scheiding van klantomgevingen

- Indien de dienstverlening plaatsvindt in een multi-tenant omgeving, borgt Leverancier dat gegevens, processen en omgevingen van Opdrachtgever logisch en technisch zijn gescheiden van die van andere afnemers.
- Leverancier kan deze scheiding aantoonbaar maken door middel van:
 - architectuur- en ontwerpdocumentatie;
 - assurance-rapportages;
 - of andere verifieerbare bewijsmiddelen.
- Opdrachtgever heeft het recht periodiek bewijs op te vragen waaruit blijkt dat tenant-isolatie effectief is ingericht en gehandhaafd.

4. Change-of-contract en wijzigingsclausule

(BIO2: 5.20.04, 5.23.01, 5.21.04)

4.1 Leverancier meldt voorgenomen wijzigingen die impact hebben op:

- beveiligingsarchitectuur
- datalocatie
- subverwerkers
- jurisdictie
- eigendomsstructuur
- kritieke beveiligingsmaatregelen

ten minste 90 dagen voorafgaand schriftelijk aan Opdrachtgever.

4.2 Opdrachtgever heeft het recht:

- aanvullende risicobeoordelingen uit te voeren
- aanvullende eisen te stellen
- de overeenkomst kosteloos te ontbinden indien het restrisico door de gemeente als onacceptabel wordt bevonden

5. Assurance, audits en toetsing

(BIO2: 5.20.01, 5.20.03, 5.20.04, 5.35.02, 6.01, 6.02 en 6.03)

5.1 Leverancier levert jaarlijks onafhankelijke assurance-rapportages aan met dekkende scope:

- ISO 27001 certificaat inclusief Statement of Applicability en verslag jaarlijkse directiebeoordeling

5.2 Eisen uit deze Security Annex en relevante beveiligingsmaatregelen uit de BIO2 maken aantoonbaar onderdeel uit van:

- audit-scope
- beheersmaatregelen
- managementverklaring

5.3 Gedurende minimaal de volledige contractduur blijven de Security Annex en relevante beveiligingsmaatregelen uit de BIO2 onderdeel van de assurance-audits.

5.4 Leverancier past de ingezette assurance-vormen aan indien wijziging van normenkaders, wet- en regelgeving of toezichtpraktijk daartoe aanleiding geeft, zodat de verstrekte assurance blijvend aansluit bij de geldende eisen en risico's.

5.5 Opdrachtgever behoudt het recht:

- aanvullende audits uit te voeren;
- third-party audits te laten uitvoeren;
- gerichte audits te voeren bij incidenten of verhoogd risico.

5.6 Indien uit audits, onderzoeken of assessments blijkt dat Leverancier niet voldoet aan de overeengekomen beveiligingseisen, wettelijke verplichtingen of deze Security Annex, komen alle kosten die voortvloeien uit het herstellen van deze bevindingen volledig voor rekening van Leverancier.

5.7 Onder deze kosten worden mede begrepen:

- kosten voor herstelmaatregelen en verbeteracties;
- kosten voor aanvullende audits of hertoetsingen;
- kosten voor externe deskundigen die noodzakelijk zijn voor verificatie van herstel.

5.8 Leverancier bespreekt de voorgenomen herstelmaatregelen, planning en prioritering vooraf met Opdrachtgever. Herstel vindt plaats na instemming van Opdrachtgever.

5.9 Indien herstelmaatregelen naar het oordeel van Opdrachtgever een zodanige doorlooptijd hebben dat een vastgesteld risico te lang open blijft staan en dit risico niet acceptabel is voor Opdrachtgever, kan de opdrachtgever besluiten om de overeenkomst kosteloos en zonder schadevergoeding te ontbinden.

5.10 Personele screening en betrouwbaarheid

- Leverancier borgt dat alle medewerkers en ingehuurde derden die toegang hebben tot systemen, gegevens of omgevingen van Opdrachtgever, voorafgaand aan die toegang aantoonbaar zijn gescreend.
- Deze screening omvat minimaal een geldige Verklaring Omtrent het Gedrag (VOG) of een aantoonbaar gelijkwaardige screeningmaatregel.

- Voor functies met verhoogde bevoegdheden of toegang tot gevoelige gegevens past Leverancier aanvullende, risicogebaseerde screening toe, indien wettelijk vereist of voortvloeiend uit de risicoanalyse.
- Leverancier herhaalt de screening periodiek en bij functiewijzigingen die leiden tot uitgebreidere of gewijzigde toegangsrechten.
- Opdrachtgever heeft het recht om op verzoek inzage te krijgen in het beleid en de procedures voor personele screening, zonder dat daarbij privacygevoelige persoonsgegevens worden verstrekt.

6. Continuïteit, RTO en RPO

(BIO2: 5.30.01, 8.13.02, 8.13.04)

6.1 Leverancier borgt contractueel vastgelegde hersteldoelstellingen voor alle kritieke diensten.

6.2 Voor deze dienst worden de volgende hersteldoelstellingen vastgelegd:

- Recovery Time Objective (RTO) conform GIBIT 2025
- Recovery Point Objective (RPO) conform GIBIT 2025

6.3 Leverancier test deze hersteldoelstellingen minimaal jaarlijks en verstrekt de testresultaten aan Opdrachtgever.

6.4 Niet-naleving van afgesproken RTO- en RPO-waarden geldt als toerekenbare tekortkoming.

6.5 Leverancier is volledig verantwoordelijk voor:

- het maken van tijdige, in lijn met de RPO eisen, volledige en consistente back-ups van alle relevante gegevens;
- de technische en functionele juistheid van deze back-ups;
- de beveiliging, beschikbaarheid en integriteit van de back-upvoorzieningen.

6.6 Leverancier controleert periodiek, maar minimaal 1 keer per jaar, en aantoonbaar de bruikbaarheid en volledigheid van back-ups door middel van:

- steekproefsgewijze verificatie;
- periodieke hersteltesten.

6.7 Leverancier draagt zelf de volledige verantwoordelijkheid voor de juistheid, volledigheid en herstelbaarheid van back-ups. Deze verantwoordelijkheid kan nimmer bij Opdrachtgever worden gelegd.

6.8 Het ontbreken van juiste, volledige of herstelbare back-ups geldt als een toerekenbare tekortkoming van Leverancier.

6.9 Opdrachtgever behoudt het recht audits uit te voeren op de back-upvoorzieningen en herstelprocedures met betrekking tot zijn gegevens.

6.10 Beschikbaarheid en uptime

- Leverancier borgt de beschikbaarheid van de dienstverlening conform de GIBIT 2025
- De minimale beschikbaarheid bedraagt minimaal 98%
- De beschikbaarheid wordt gemeten over een kalendermaand, exclusief vooraf aangekondigd onderhoud dat schriftelijk is afgestemd met Opdrachtgever.
- Niet-naleving van de afgesproken uptime-percentages geldt als een toerekenbare tekortkoming in de zin van hoofdstuk 12 van deze Security Annex.

7. Pentesten (alleen van toepassing bij software ontwikkeling)

(BIO2: 8.08.04, 8.08.05)

7.1 Leverancier laat minimaal jaarlijks een whitebox penetratietest uitvoeren op:

- volledige applicatie en onderliggende omgeving

7.2 De pentest wordt uitgevoerd door een onafhankelijke, CCV Keurmerk pentesten gekwalificeerde partij.

7.3 Het volledige rapport en opvolging van bevindingen worden aan Opdrachtgever verstrekt.

7.4 De bevindingen worden gezamenlijk door Leverancier en Opdrachtgever beoordeeld op ernst, impact en risico voor de dienstverlening.

7.5 Indien bevindingen door Opdrachtgever als onacceptabel risico worden aangemerkt, worden deze vastgelegd in het verbeterplan met bijbehorende herstelmaatregelen en tijdslijnen. Zolang deze bevindingen niet zijn hersteld, mag de betreffende functionaliteit of omgeving niet productief worden ingezet, tenzij Opdrachtgever hiervoor expliciet en schriftelijk toestemming verleent.

7.6 Indien herstelmaatregelen naar het oordeel van Opdrachtgever een zodanige doorlooptijd hebben dat een vastgesteld risico te lang open blijft staan en dit risico niet acceptabel is voor Opdrachtgever, kan de opdrachtgever besluiten om de overeenkomst kosteloos en zonder schadevergoeding te ontbinden.

8. Leveranciersketen en subverwerkers

(BIO2: 5.20.03, 5.21.01, 5.21.02, 5.21.03, 5.21.04)

8.1 Leverancier blijft volledig verantwoordelijk voor naleving van deze annex door alle subverwerkers.

8.2 Leverancier verstrekt vooraf inzicht in:

- ketenstructuur
- betrokken subverwerkers
- datalocaties
- relevante risico's

8.3 Wijzigingen in de keten worden onverwijld gemeld, inclusief impactanalyse.

9. Incidentmelding en transparantie

(BIO2: 5.20.05, 5.24.01 t/m 5.25.01 en 8.15.01 t/m 8.16.04)

9.1 Leverancier meldt beveiligingsincidenten die mogelijk impact hebben op de dienstverlening:

- onverwijld;
- door middel van een eerste early-warning melding uiterlijk binnen 4 uur na ontdekking, waarin minimaal de aard van het incident en de vermoedelijke impact worden aangegeven;
- en met een volledige incidentmelding uiterlijk binnen 24 uur na ontdekking.

9.2 Meldingen bevatten minimaal:

- aard en omvang
- getroffen systemen en gegevens
- genomen en geplande maatregelen
- impact op beschikbaarheid, integriteit en vertrouwelijkheid

9.3 Leverancier verleent volledige medewerking aan wettelijke meldplichten en toezichthouders.

9.4 Indien Leverancier op grond van toepasselijke wet- en regelgeving, waaronder de Cyberbeveiligingswet, zelf meldplichtig is, draagt Leverancier zorg voor tijdige en correcte melding aan de bevoegde toezichthouders en instanties.

9.5 Indien Opdrachtgever meldplichtig is, verstrekt Leverancier onverwijld alle informatie en ondersteuning die noodzakelijk is om Opdrachtgever in staat te stellen tijdig en volledig aan zijn meldverplichtingen te voldoen.

9.6 Beveiligingsmonitoring en log-export

- Leverancier borgt dat beveiligingsrelevante loggegevens, waaronder audit-, toegangs- en beheerderslogs, beschikbaar zijn voor Opdrachtgever.
- Deze loggegevens zijn:
 - exporteerbaar in een gangbaar en machineleesbaar formaat;
 - conform de eisen zoals gesteld in BIO2 8.15.01

- minimaal twaalf (12) maanden beschikbaar, tenzij wet- of regelgeving een langere termijn vereist.
- Loggegevens zijn beschermd tegen ongeautoriseerde wijziging en verwijdering en geschikt voor forensisch onderzoek.

10. Exit, datateruggave en vernietiging

(BIO2: 5.20.06, 8.13.01, 8.13.03)

10.1 Leverancier borgt een uitgewerkte exit-strategie inclusief:

- dataportabiliteit in open en gangbare formaten;
- veilige en volledige dataverwijdering;
- overdrachtsdocumentatie en technische ondersteuning bij migratie.

10.2 De uitvoering van de exit-strategie vindt plaats kosteloos en zonder enige aanvullende vergoeding, verborgen kosten of aanvullende voorwaarden.

10.3 Na beëindiging van de overeenkomst verklaart Leverancier schriftelijk dat:

- alle gegevens van Opdrachtgever zijn verwijderd;
- geen restkopieën of replicaties meer bestaan;
- back-ups conform vastgesteld beleid zijn vernietigd.

10.4 Leverancier verstrekt een officieel vernietigingscertificaat waaruit blijkt dat de vernietiging heeft plaatsgevonden conform NEN-EN-ISO/IEC 21964 (voorheen DIN 66399) of een gelijkwaardige internationaal erkende norm.

11. Prevalentie van deze annex

(BIO2: 5.20.01, 5.20.02)

11.1 Bij tegenstrijdigheden tussen deze Security Annex en andere contractdocumenten, algemene voorwaarden, SLA's of bijlagen, prevaleert deze Security Annex.

11.2 Afwijkingen van deze annex zijn uitsluitend geldig indien deze expliciet en schriftelijk door Opdrachtgever zijn goedgekeurd.

12. Sancties, boetes en ontbinding

(BIO2: 5.20.02, 5.23.01)

12.1 Structurele of ernstige niet-naleving door Leverancier van deze Security Annex en/of de overgenomen beveiligingsverplichtingen in de overeenkomst geldt als toerekenbare tekortkoming.

12.2 Onverminderde de bevoegdheid van Opdrachtgever op grond van deze Security Annex, heeft Opdrachtgever bij niet-naleving van de verplichtingen door Leverancier het recht op:

- opschorting van dienstverlening;
- Leverancier is verplicht om binnen een door de Gemeente te stellen redelijke termijn de door de Gemeente verlangde aanvullende maatregelen te treffen. Indien Leverancier nalaat deze maatregelen tijdig en volledig te implementeren, is de Gemeente gerechtigd deze maatregelen zelf (of door een derde) te laten uitvoeren, waarbij de daarmee gemoeide kosten volledig voor rekening van Leverancier komen.
- tussentijdse ontbinding van de overeenkomst zonder schadevergoeding aan Leverancier.

12.3 De boetebepalingen uit de Gemeente Alkmaar Inkoopvoorwaarden worden geacht integraal deel uit te maken van deze Security Annex en de hoofdovereenkomst, tenzij uitdrukkelijk anders is aangegeven en schriftelijk door Opdrachtgever is goedgekeurd.

<https://www.alkmaar.nl/inkoopvoorwaarden-gemeente-alkmaar/>

Verdiepende maatregelen

13. Contact, communicatie en beveiligingskanalen

(BIO2: 5.20.05, 5.24.01, 5.24.02, 8.08.06)

13.1 Bij alle communicatie met betrekking tot informatiebeveiliging, waaronder begrepen maar niet beperkt tot:

- incidentmeldingen en early warnings;
- audit- en assurance-rapportages;
- meldingen van kwetsbaarheden;
- wijzigingen met beveiligingsimpact;
- herstelplannen en verbetertrajecten;

neemt Leverancier altijd het adres **security@alkmaar.nl** op als vast contactpunt.

13.2 Leverancier wijst vaste contactpersonen aan voor informatiebeveiliging en incidentafhandeling en zorgt dat deze 24/7 bereikbaar zijn voor Opdrachtgever.

13.3 Coordinated Vulnerability Disclosure

(CRA)

Leverancier hanteert een *Coordinated Vulnerability Disclosure-beleid (CVD)* voor het ontvangen, beoordelen en verhelpen van gemelde beveiligingskwetsbaarheden.

Dit beleid beschrijft ten minste:

- hoe kwetsbaarheden op verantwoorde wijze kunnen worden gemeld;
- hoe meldingen worden beoordeeld en opgevolgd;
- hoe afstemming plaatsvindt met melders en betrokken partijen;
- op welke wijze en op welk moment communicatie over verholpen kwetsbaarheden plaatsvindt.

Leverancier stelt als onderdeel van dit beleid een duidelijk en openbaar toegankelijk contactpunt beschikbaar voor het melden van kwetsbaarheden.

Het CVD-beleid is openbaar toegankelijk en wordt op verzoek aan Opdrachtgever verstrekt.

14. Authenticatie en accounts

(BIO2: 5.17.01, 5.18.01, 8.18.01)

14.1 Alle beheer- en administratieve accounts worden uitsluitend gebruikt met wachtwoordloze, phishing-bestendige authenticatie op basis van de FIDO2-standaard of een gelijkwaardige non-phishable authenticatiemethode.

14.2 Het gebruik van wachtwoorden, sms-codes of app-gebaseerde push-notificaties voor accounts is niet toegestaan, tenzij Opdrachtgever hiervoor expliciet en schriftelijk toestemming verleent op basis van een risicoafweging.

14.3 De door Opdrachtnemer geleverde systemen, diensten en applicaties ondersteunen naadloos Single Sign-On (SSO) op basis van federatieve identity-standaarden (zoals SAML 2.0 of OpenID Connect) en zijn volledig compatibel met de door Opdrachtgever gebruikte identityprovider, zijnde Microsoft Entra ID.

Authenticatie dient wachtwoordloos en phishing-resistent plaats te vinden via FIDO2/passkeys, zonder fallback naar minder veilige methoden (zoals wachtwoorden of legacy MFA), tenzij expliciet en schriftelijk overeengekomen.

De oplossing ondersteunt het afdwingen van phishing-resistente authenticatiesterkte en maakt gebruik van moderne authenticatiemechanismen die integreren met Conditional Access-beleid van Opdrachtgever.

14.4 Voor overige accounts wordt bij voorkeur gebruikgemaakt van FIDO2-gebaseerde authenticatie of een gelijkwaardige phishing-bestendige methode. Leverancier zorgt ervoor dat deze methode uiterlijk binnen twaalf (12) maanden na ingangsdatum van de overeenkomst beschikbaar is en structureel wordt toegepast voor alle accounts.

15. Werkplekken en toegangsvoorzieningen

(BIO2: 5.15.01, 5.17.01, 8.01.01)

15.1 Leverancier werkt vanaf beheerde, beveiligde werkplekken, welke beperkt zijn in het installeren van ongeautoriseerde software, voorzien van actuele hardening, patching en endpoint-beveiliging.

15.2 Beheerhandelingen mogen niet worden uitgevoerd vanaf werkplekken waarop de gebruiker standaard beschikt over lokale administratorrechten.

16. Toekenning en gebruik van administratieve rechten

(BIO2: 5.18.01, 5.18.02, 8.02.01)

16.1 Administratieve rechten worden nooit standaard of permanent toegekend.

16.2 Alle verhoogde rechten worden uitsluitend verleend op basis van het just-in-time principe, waarbij:

- rechten tijdelijk en taakgericht worden toegekend;
- rechten automatisch vervallen na afloop van de taak;
- gebruik wordt gelogd en gemonitord.

16.3 Leverancier maakt hiervoor gebruik van een voorziening voor Privileged Identity Management (PIM) of een gelijkwaardige oplossing.

17. Tenant-brede en hoogste beheerdersrechten

(BIO2: 5.18.01, 8.18.01)

17.1 Tenant-brede administratieve rollen met volledige bevoegdheden, waaronder begrepen maar niet beperkt tot rollen zoals Global Administrator, Tenant Owner of gelijkwaardige hoogste beheerdersrollen, worden tot een minimum beperkt.

17.2 Deze rollen worden uitsluitend toegekend:

- op basis van het just-in-time principe;
- met verplichte FIDO2-authenticatie;
- met aanvullende logging en monitoring.

18. Secure Software Development Lifecycle (SSDLC) (alleen van toepassing bij software ontwikkeling)

(BIO2: 8.27.01, 8.28.02, 8.30.01, 8.31.01, 8.31.02, 8.32.01, 8.32.02)

18.1 Secure Software Development Lifecycle en Security by Design
Leverancier ontwikkelt software conform een Secure Software Development Lifecycle (SSDLC), waarbij beveiliging vanaf het ontwerp structureel is ingebed (Security by Design en Security by Default).

Voorafgaand aan iedere (door)ontwikkeling wordt een risicoanalyse uitgevoerd. De uitkomsten hiervan worden aantoonbaar verwerkt in het ontwerp en de implementatie. De risicoanalyse is op verzoek van Opdrachtgever opvraagbaar.

18.2 Omgevingsscheiding en toegangsbeperking

Alleen geautoriseerde personen hebben toegang tot ontwikkel-, test- en productieomgevingen.

De scheiding tussen ontwikkel-, test- en productieomgevingen is verplicht en aantoonbaar ingericht.

Ontwikkel- en testomgevingen bevatten geen productiegegevens en zijn niet gekoppeld aan productiesystemen.

18.3 Broncodebeheer en codebeoordeling

Leverancier beschikt over procedures voor:

- het beoordelen van broncode (bijvoorbeeld via peer reviews);
- het borgen van het vier-ogen-principe bij wijzigingen in kritieke code;
- het documenteren en opvolgen van bevindingen uit codebeoordelingen.

18.4 Beveiligingstests en validatie vóór livegang

Leverancier voert aantoonbaar beveiligingstests uit, waaronder minimaal:

- statische codeanalyse (SAST);
- dynamische analyse (DAST);
- penetratietests die voldoen aan het CCV-keurmerk Pentesten, mede gebaseerd op de OWASP Top 10.

Deze testen worden uitgevoerd:

- voorafgaand aan iedere livegang;
- bij majeure releases of significante functionele wijzigingen.

Kritieke en hoge bevindingen worden hersteld vóór livegang.

18.5 Dependency scanning en gebruik van externe componenten

Leverancier maakt uitsluitend gebruik van bekende en veilige softwarecomponenten, zoals libraries en frameworks.

Er is een ingericht proces voor:

- dependency scanning;
- het detecteren van kwetsbaarheden in externe componenten;
- het tijdig patchen of vervangen van kwetsbare afhankelijkheden.

Het gebruik van componenten met bekende kritieke kwetsbaarheden is niet toegestaan.

18.6 Software Bill of Materials (SBOM) **CRA**

Leverancier stelt voor de door hem geleverde software en componenten een actuele Software Bill of Materials (SBOM) op en onderhoudt deze gedurende de gehele looptijd van de overeenkomst.

De SBOM geeft volledig en actueel inzicht in alle gebruikte softwarecomponenten, waaronder in ieder geval begrepen:

- open source en commerciële componenten;

- libraries, frameworks en andere afhankelijkheden;
- versienummers;
- herkomst (leverancier / bron);
- licentie-informatie.

De SBOM wordt opgesteld in een gangbaar en machineleesbaar formaat en wordt op verzoek onverwijld aan Opdrachtgever verstrekt.

Leverancier beschikt over een ingericht proces om op basis van de SBOM:

- kwetsbaarheden in componenten tijdig te identificeren;
- de impact daarvan op de dienstverlening te beoordelen;
- passende mitigerende maatregelen te treffen, waaronder patching of vervanging.

Indien uit de SBOM blijkt dat de dienstverlening afhankelijk is van componenten met bekende kritieke kwetsbaarheden, meldt Leverancier dit onverwijld aan Opdrachtgever, inclusief:

- een impactanalyse;
- voorgestelde herstelmaatregelen;
- een realistische hersteltermijn.

Het ontbreken van een actuele, volledige of juiste SBOM geldt als een tekortkoming in de nakoming van deze Security Annex.

18.7 Patchbaarheid en updatevoorzieningen

Software is zodanig ontworpen dat deze eenvoudig en veilig kan worden geüpdatet.

Leverancier beschikt over procedures voor:

- het snel patchen van kwetsbaarheden;
- het gecontroleerd uitrollen van beveiligingsupdates; deze mogen niet worden uitgesteld door functionele wijzigingen. Ze kunnen wél apart worden uitgerold [CRA]
- het informeren van Opdrachtgever over kritieke kwetsbaarheden en patches.

Leverancier informeert, indien van toepassing, op transparante wijze over verholpen beveiligingskwetsbaarheden zodra een beveiligingsupdate beschikbaar is gesteld [CRA]

Beveiligingsupdates voor kritieke en hoge kwetsbaarheden worden onverwijld beschikbaar gesteld en uitgerold, zonder aanvullende kosten voor Opdrachtgever. Voor maatwerkproducten kunnen hierover afwijkende afspraken worden gemaakt, mits deze vooraf schriftelijk zijn vastgelegd [CRA].

18.8 Documentatie en overdraagbaarheid

Ontwikkelde software is adequaat en actueel gedocumenteerd, zodanig dat deze:

- overdraagbaar is aan andere ontwikkelaars of teams;
- onderhoudbaar is zonder afhankelijkheid van specifieke personen.