

Security Annex Informatiebeveiliging

Samen werken aan digitaal vertrouwen

Inwoners mogen erop vertrouwen dat hun gegevens veilig zijn. Dat geldt voor ons als gemeente, maar net zo goed voor de leveranciers waarmee wij samenwerken. Want digitale dienstverlening stopt niet bij de muren van het gemeentehuis.

Daarom werken wij met een Security Annex.

Niet om samenwerking ingewikkeld te maken, maar omdat de realiteit daarom vraagt. Vrijwel dagelijks verschijnen berichten over datalekken, ransomware of digitale verstoringen. De vraag is allang niet meer óf organisaties risico lopen, maar hoe serieus zij omgaan met het beschermen van gegevens en dienstverlening.

Wij geloven daarbij in openheid en samenwerking. Niet in gesloten deuren of een cultuur waarin risico's worden weggestopt. Sterke beveiliging begint juist met transparantie: eerlijk zijn over verbeterpunten, risico's bespreekbaar maken en samen kijken hoe we digitale weerbaarheid verhogen.

Van leveranciers verwachten wij daarom dat informatiebeveiliging een vast onderdeel is van de bedrijfsvoering. Niet alleen vanuit wet- en regelgeving, maar vanuit intrinsieke motivatie. De gegevens van inwoners verdienen die zorgvuldigheid.

Uiteindelijk werken we aan hetzelfde doel: betrouwbare en veilige dienstverlening waar inwoners op kunnen vertrouwen. Dat vraagt om partners die willen meedenken, willen verbeteren en samen met ons verantwoordelijkheid nemen voor een veilige digitale keten.

INHOUD

Security Annex Informatiebeveiliging	1
1. Toepasselijkheid en normenkader	3
2. Cloud governance en CSP-beleid	4
3. Cloudsoevereiniteit en Europese zeggenschap	4
4. Change-of-contract en wijzigingsclausule	6
5. Assurance, audits en toetsing	6
6. Continuïteit, RTO en RPO	8
7. Penetratietesten en red teaming	9
8. Leveranciersketen en subverwerkers	10
9. Incidentmelding en transparantie	10
10. Exit, datateruggave en vernietiging	11
11. Prevalentie van deze Security Annex	12
12. Sancties, boetes en ontbinding	12
Verdiepende maatregelen	14
13. Contact, communicatie en beveiligingskanalen	14
14. Authenticatie en accounts	15
15. Werkplekken en toegangsvoorzieningen	15
16. Toekenning en gebruik van administratieve rechten	16
17. Tenant-brede en hoogste beheerdersrechten	16
18. Secure Software Development Lifecycle (SSDLC)	16
19. Kunstmatige intelligentie (AI)	19
20. Technisch beveiligingsbeheer	20

1. Toepasselijkheid en normenkader

(BIO2: 5.01.01, 5.02.01, 5.19.01, 5.20.01 en ISO/IEC 27001)

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), 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 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);
- de Europese AI Act (2024/1689);
- 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. Cloudsoevereiniteit en Europese zeggenschap

(BIO2: 5.19, 5.20, 5.21.02, 5.21.03, 5.21.05 en 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 cloudomgeving binnen de Europese Unie, waarbij geldt dat:

- alle primaire, secundaire en back-uplocaties zich binnen de EU bevinden;
- beheer-, onderhouds- en ondersteuningsactiviteiten uitsluitend vanuit de EU worden uitgevoerd;
- cryptografische sleutels uitsluitend binnen de EU worden beheerd;
- geen structurele afhankelijkheid bestaat van niet-EU beheersorganisaties voor de uitvoering van de dienstverlening.

3.3 Leverancier waarborgt dat de dienstverlening wordt uitgevoerd door rechtspersonen gevestigd binnen de EU of EER en dat gegevens uitsluitend worden verwerkt onder toepasselijk Europees recht.

3.4 Leverancier treft passende technische, organisatorische en juridische maatregelen om ongeautoriseerde toegang door derde landen tot gegevens van Opdrachtgever te voorkomen.

3.5 Leverancier verklaart dat:

- de dienstverlenende rechtspersoon is gevestigd binnen de EU of EER;
- de uiteindelijke moedermaatschappij is gevestigd binnen de EU of EER;
- de uiteindelijke zeggenschap over Leverancier uitsluitend berust bij natuurlijke personen, rechtspersonen of publieke organisaties gevestigd binnen de EU of EER;
- geen directe of indirecte zeggenschap wordt uitgeoefend door een entiteit gevestigd buiten de EU of EER.

3.6 Onder zeggenschap als bedoeld in artikel 3.5 wordt verstaan iedere vorm van directe of indirecte beslissende invloed, waaronder:

- het direct of indirect beschikken over 25% of meer van de aandelen;
- het direct of indirect beschikken over 25% of meer van de stemrechten;
- het recht om bestuurders, commissarissen of toezichthouders te benoemen of te ontslaan;
- iedere andere vorm van feitelijke beslissende invloed op de bedrijfsvoering, strategie of governance van Leverancier.

3.7 Leverancier waarborgt dat de dienstverlening niet direct of indirect onderworpen is aan wet- of regelgeving van derde landen die toegang tot gegevens van Opdrachtgever kunnen afdwingen buiten het Europese rechtstelsel om.

3.8 De strategische besluitvorming, governance, financiering en operationele aansturing van de dienstverlening vinden plaats binnen de EU of EER. Leverancier maakt daarbij geen gebruik van een concernstructuur waarbij een niet-EU/EER-entiteit directe of indirecte invloed kan uitoefenen op de dienstverlening, gegevensverwerking of beveiligingsmaatregelen.

3.9 Leverancier meldt iedere voorgenomen of gerealiseerde wijziging in eigendom, zeggenschap, governance, financiering, fusie, overname of investering die leidt of kan leiden tot directe of indirecte invloed van een niet-EU/EER-entiteit onverwijld schriftelijk aan Opdrachtgever.

3.10 Opdrachtgever heeft in geval van een wijziging als bedoeld in artikel 3.9 het recht aanvullende maatregelen te verlangen, een herbeoordeling uit te voeren of de overeenkomst geheel of gedeeltelijk te beëindigen overeenkomstig de bepalingen van deze Overeenkomst.

3.11 Leverancier maakt uitsluitend gebruik van subverwerkers gevestigd binnen de EU of EER, tenzij Opdrachtgever hiervoor voorafgaand schriftelijk toestemming heeft verleend.

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:

- het overeengekomen beveiligingsniveau van de dienstverlening, waaronder het verminderen, uitschakelen of optioneel maken van bestaande beveiligingsmaatregelen;
- datalocatie;
- subverwerkers;
- jurisdictie;
- eigendomsstructuur;
- kritieke beveiligingsmaatregelen.

ten minste negentig (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, 5.22.01, 6.01.01, 6.02.01, 6.03.01 en 6.03.02)

5.1 Leverancier levert jaarlijks een passende combinatie van onafhankelijke assurance-informatie aan waarvan de scope de gecontracteerde dienstverlening dekt. Afhankelijk van aard en risicoprofiel kan dit bestaan uit:

- ISO 27001-certificaat inclusief de relevante Verklaring van Toepasselijkheid (VvT) en een samenvatting of verklaring waaruit blijkt dat de directiebeoordeling is uitgevoerd;
- (wens, geen eis) SOC 2 Type II, ISAE 3402 of ISAE 3000, voor zover passend bij de aard van de dienstverlening;
- ISO/IEC 27017, wanneer clouddienstverlening binnen de scope valt.

5.2 Eisen uit deze Security Annex en relevante beveiligingsmaatregelen uit de BIO 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 BIO 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.

5.4a Leverancier werkt jaarlijks mee aan een risicogerichte leveranciersreview door Opdrachtgever. De review beperkt zich in beginsel tot reeds beschikbare en passende bewijsstukken, openstaande relevante bevindingen, incidenten, ketenwijzigingen en de voortgang van overeengekomen verbetermaatregelen. Aanvullend onderzoek wordt alleen verlangd bij verhoogd risico, een incident of gerede twijfel over naleving.

5.5 Opdrachtgever behoudt het recht:

- aanvullende audits uit te voeren;
- third-party audits te laten uitvoeren;
- gerichte audits uit te (laten) 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 op verzoek 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;
- De minimale beschikbaarheid bedraagt minimaal 99,9%;
- De beschikbaarheid wordt gemeten over een kalendermaand, exclusief vooraf aangekondigd onderhoud dat schriftelijk is afgesteld 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. Penetratietesten en red teaming

(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 penetratietest wordt uitgevoerd door een onafhankelijke, CCV Keurmerk pentesten gekwalificeerde partij.

7.3 Het volledige penetratietestrapport en opvolging van bevindingen worden met de Opdrachtgever gedeeld.

7.4 Leverancier voert minimaal eens per twee jaar een red teaming-oefening uit op de eigen organisatie en de geleverde cloud- en hostingomgeving of relevante delen daarvan.

7.5 De scope van de red teaming-oefening omvat minimaal (wens, geen eis):

- aanvalspaden richting kernsysteemomgevingen en klantomgevingen, waaronder begrepen de omgevingen waarin de kritieke infrastructuur, beheersystemen en overige kroonjuwelen van Leverancier en Opdrachtgever zijn ondergebracht;
- misbruik van identiteiten en beheeraccounts;
- laterale beweging binnen de organisatie, beheerdomeinen en cloud- en hostingomgevingen.

7.6 De bevindingen worden gedeeld met de Opdrachtgever en zijn beoordeeld op ernst, impact en risico voor de dienstverlening.

7.7 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.

7.8 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, 5.21.02, 5.21.03, 5.21.04, 5.21.05 en 5.22.01)

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

8.2 Leverancier verstrekt vooraf inzicht in:

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

8.3 Wijzigingen of structurele niet nalevingen in de keten worden onverwijld gemeld, inclusief impactanalyse.

8.4 Leverancier legt de relevante eisen uit deze Security Annex onverkort op aan subleveranciers en subverwerkers, tenzij een eis aantoonbaar niet relevant is voor hun aandeel in de dienstverlening. Uitsluitingen worden onderbouwd en op verzoek aan Opdrachtgever verstrekt.

8.5 Leverancier beoordeelt minimaal jaarlijks de beveiligingsprestaties en relevante risico's van kritieke subleveranciers en betreft de uitkomsten bij de assurance-informatie en de leveranciersreview.

9. Incidentmelding en transparantie

(BIO2: 5.20.05, 5.24.01, 5.24.02, 5.24.07, 5.26.02, 5.27.01, 5.28.01, 8.15.01 t/m 8.15.06 en 8.16.01 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 NIS2 en/of 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.

9.7 Leverancier bewaart het incidentdossier, inclusief relevante logging, analyse, besluitvorming, herstelmaatregelen en communicatie, minimaal drie (3) jaar na afsluiting van het incident, tenzij een langere wettelijke bewaartermijn geldt.

9.8 Leverancier beschikt over passende detectie- en responsevoorzieningen voor de omgevingen die de dienstverlening ondersteunen. Manipulatie of verwijdering van beveiligingsloggegevens wordt gedetecteerd en als beveiligingsincident behandeld.

10. Exit, datateruggave en vernietiging

(BIO2: 5.20.06, 8.13.01, 8.13.03)

10.1 Op de beëindiging van de overeenkomst en de uitvoering van exit-werkzaamheden is artikel 29 van de GIBIT 2025 onverkort van toepassing.

10.2 In aanvulling op artikel 29 GIBIT geldt dat:

- gegevens worden aangeleverd in open, gangbare en machineleesbare formaten;
- Leverancier schriftelijk verklaart dat alle gegevens, restkopieën en back-ups van Opdrachtgever zijn verwijderd overeenkomstig overeengekomen bewaartermijnen;
- Leverancier op verzoek een vernietigingsverklaring of vernietigingscertificaat verstrekt conform een internationaal erkende norm voor gegevensvernietiging.

11. Prevalentie van deze Security 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 Security 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 Niet-naleving van de verplichtingen uit deze Security Annex en/of de in de Overeenkomst opgenomen informatiebeveiligingsverplichtingen wordt aangemerkt als een tekortkoming in de nakoming van de Overeenkomst.

12.2 Indien Leverancier tekortschiet in de naleving van de verplichtingen uit deze Security Annex, is Opdrachtgever gerechtigd Leverancier te verplichten passende corrigerende maatregelen te treffen binnen een redelijke, door Opdrachtgever gestelde termijn.

12.3 Indien Leverancier nalaat de vereiste maatregelen tijdig of volledig uit te voeren, dan wel sprake is van een ernstige of voortdurende tekortkoming, zijn de rechtsmiddelen, sancties, aansprakelijkheids- en ontbindingsmogelijkheden van toepassing zoals opgenomen in artikel 27 van de GIBIT 2025, onverminderd eventuele overige rechten die Opdrachtgever op grond van de Overeenkomst of toepasselijke wet- en regelgeving toekomen.

12.4 Voor zover deze Security Annex aanvullende informatiebeveiligingsverplichtingen bevat ten opzichte van de Overeenkomst, worden deze verplichtingen voor de

toepassing van artikel 27 van de GIBIT 2025 geacht integraal onderdeel uit te maken van de contractuele verplichtingen van Leverancier.

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.
[leverancier vult hier de contactgegevens in]

(CRA)

13.3 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 (seamless) 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 met Opdrachtgever.

De oplossing ondersteunt het afdwingen van phishing-resistente authenticatiesterkte en maakt gebruik van moderne authenticatiemechanismen die integreren met het 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 en afgedwongen 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)

(BIO2: 8.27.01, 8.28, 8.29.01, 8.30.01, 8.31.01, 8.31.02, 8.32.01 en 8.32.02)

18.1 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 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 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 Leverancier voert aantoonbaar beveiligingstests uit gedurende de gehele softwareontwikkelcyclus, waaronder minimaal:

- statische codeanalyse (SAST);
- dynamische analyse (DAST);
- dependency- en kwetsbaarheidsscans.

SAST, DAST en overige geautomatiseerde beveiligingscontroles zijn geïntegreerd in de ontwikkel- en releasepipeline en worden uitgevoerd voorafgaand aan iedere productie-uitrol.

Daarnaast voert Leverancier penetratietests uit die voldoen aan het CCV-keurmerk Pentesten, mede gebaseerd op de OWASP Top 10. Deze penetratietests worden uitgevoerd:

- voorafgaand aan majeure releases;
- bij significante functionele wijzigingen met een hoger risico.

Kritieke en hoge bevindingen worden hersteld vóór productiegang.

18.5 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 voldoet aan artikel 25 van de GIBIT 2025 inzake Software Bill of Materials (SBOM). De actuele SBOM wordt op verzoek onverwijld aan Opdrachtgever verstrekt.

Leverancier beschikt over een ingericht proces om op basis van de SBOM kwetsbaarheden tijdig te identificeren, de impact daarvan te beoordelen en passende mitigerende maatregelen te treffen.

Indien kritieke kwetsbaarheden worden vastgesteld in gebruikte componenten informeert Leverancier Opdrachtgever onverwijld, inclusief impactanalyse, herstelmaatregelen en hersteltermijn.

18.7 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, op voorwaarde dat deze vooraf schriftelijk zijn vastgelegd (CRA).

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

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

19. Kunstmatige intelligentie (AI)

(AI Act)

19.1 Toepasselijkheid

Leverancier meldt voorafgaand schriftelijk indien binnen de dienstverlening gebruik wordt gemaakt van kunstmatige intelligentie (AI) of andere algoritmes, waaronder begrepen maar niet beperkt tot:

- generatieve AI;
- large language models (LLM's);
- machine learning;
- AI-functionaliteiten van derden;
- AI-functionaliteiten die inhoud genereren, analyseren, classificeren, voorspellen of geautomatiseerde besluitvorming ondersteunen.

19.2 Leverancier beschikt over aantoonbaar ingerichte governance voor het beheersen van risico's die voortvloeien uit het gebruik van AI binnen de dienstverlening.

Deze governance omvat ten minste:

- verantwoordelijkheden en eigenaarschap;
- risicobeoordeling;
- wijzigingsbeheer;
- toezicht op AI-functionaliteiten;
- periodieke evaluatie van risico's en beheersmaatregelen.

Leverancier verstrekt op verzoek inzicht in de inrichting van deze governance.

19.3 Gegevens van Opdrachtgever worden niet gebruikt voor:

- training;
- hertraining;
- fine-tuning;
- validatie;
- evaluatie.

van AI-modellen, tenzij Opdrachtgever hiervoor vooraf expliciet schriftelijk toestemming heeft verleend.

19.4 Leverancier verstrekt op verzoek inzicht in:

- toegepaste AI-functionaliteiten;
- de doeleinden waarvoor AI wordt ingezet;
- betrokken AI-leveranciers;

- verwerkte gegevenscategorieën;
- locaties waar gegevens worden verwerkt;
- getroffen beveiligingsmaatregelen.

19.5 Leverancier meldt voorgenomen wijzigingen in AI-functionaliteiten ten minste negentig (90) dagen voorafgaand schriftelijk aan Opdrachtgever indien deze wijzigingen invloed kunnen hebben op:

- de verwerking van gegevens;
- de beveiliging van de dienstverlening;
- de functionaliteit van de oplossing;
- de toepasselijke risico's.

Opdrachtgever behoudt het recht om naar aanleiding van dergelijke wijzigingen een aanvullende risicobeoordeling uit te voeren.

19.6 Indien AI-functionaliteiten worden ingezet voor het ondersteunen van processen of besluitvorming, borgt Leverancier dat uitkomsten controleerbaar, navolgbaar en door een mens worden beoordeeld en kunnen worden gecorrigeerd.

20. Technisch beveiligingsbeheer

(BIO2: 5.14.01, 8.07.01, 8.07.03, 8.07.04, 8.08.01 t/m 8.08.03, 8.19.01, 8.20.02, 8.21.01, 8.21.02, 8.21.04 en 8.24.01 t/m 8.24.04)

20.1 Leverancier beschikt over een aantoonbaar proces voor kwetsbaarheden- en patchmanagement voor alle componenten die de dienstverlening ondersteunen. Bij kwetsbaarheden met een hoge kans op misbruik en hoge potentiële schade worden passende maatregelen zo snel mogelijk, maar uiterlijk binnen één week getroffen. Als structureel herstel niet binnen deze termijn mogelijk is, worden direct tijdelijke mitigerende maatregelen getroffen en wordt Opdrachtgever geïnformeerd over risico, maatregel en herstelplanning.

20.2 De omgevingen en beheerde werkplekken die de dienstverlening ondersteunen zijn voorzien van actuele bescherming tegen malware en ongeautoriseerde software. Ontvangen en gedownloade bestanden worden vóór uitvoering of opslag passend gecontroleerd.

20.3 Beheerinterfaces en beheersegmenten zijn logisch gescheiden van gebruikersnetwerken. Verkeer tussen vertrouwde en externe of onvertrouwde zones wordt bewaakt op verdacht verkeer en beschermd tegen aanvallen die beschikbaarheid, integriteit of vertrouwelijkheid kunnen aantasten.

20.4 Gegevens van Opdrachtgever worden tijdens transport en opslag versleuteld met actuele, algemeen aanvaarde cryptografische standaarden. Leverancier heeft

verantwoordelijkheden voor sleutelbeheer vastgelegd, houdt een actueel overzicht van toegepaste cryptografie bij en volgt voor algoritmen en sleutelsterktes de actuele adviezen van het NCSC en, waar relevant, het NBV van de AIVD.

20.5 Internetgerichte systemen en e-mailvoorzieningen die onderdeel zijn van de dienstverlening voldoen aan de toepasselijke verplichte standaarden van het Forum Standaardisatie. Leverancier kan de actuele toepassing daarvan op verzoek toelichten.