Overzicht van de standaard contracteisen die vanuit de Baseline Informatiebeveiliging 2 (BIO2) en ISO27001:2023 van toepassing zijn verklaard.

1	**Contractuele beveiligingsafspraken** *De informatiebeveiligingseisen zoals opgenomen in de offerte uitvraag, worden expliciet vastgelegd in het contract met de leverancier.*
2	***Contactpersoon informatiebeveiliging*** *De leverancier wijst binnen zijn organisatie een vaste contactpersoon aan voor communicatie betreffende informatiebeveiliging.*
3	***Meldplicht incidenten en kwetsbaarheden*** *In het contract wordt opgenomen dat de leverancier verplicht is om voor de dienst relevante beveiligingsincidenten en kwetsbaarheden inclusief datalekken te melden zodra deze ontdekt worden.*
4	***Jaarlijkse compliance-aantoning*** *In het contract wordt opgenomen dat de leverancier jaarlijks via een onafhankelijke partij aantoont dat aan de overeengekomen afspraken wordt voldaan.*
5	**Auditrecht** *In het contract wordt opgenomen dat de Provincie Noord-Brabant het recht heeft om aanvullend onderzoek of audits uit te laten voeren.*
6	**Exit-strategie** *Een uitgewerkte exit strategie met afspraken over beëindiging van de dienstverlening, inclusief overdracht en dataverwijdering is onderdeel van het contract.*
7	**Ketenbeveiliging doorleggen** *In het contract wordt opgenomen dat de leverancier bij gebruik van onderaannemers en sub-leveranciers de beveiligingseisen 1 op 1 doorgelegd binnen de gehele keten.*
8	**Veranderingen in de keten** *In het contract wordt vastgelegd dat de leverancier gedurende de looptijd van het contract wijzigingen in de toeleveringsketen van leveranciers vooraf afstemt met de opdrachtgever.*
9	**Basale beveiligingsconfiguratie** *Producten en diensten worden geleverd onder een beveiligde configuratie waarbij de toegepaste beveiligingsstandaarden actueel en niet kwetsbaar zijn.*
10	**Patchbeleid** *In het contract zijn vaste termijnen opgenomen voor het installeren van voor de dienst relevante updates en beveiligingspatches (kritieke patches (NCSC H/H) ≤7 dagen, Overige ≤30 dagen).*
11	**Meldplicht kwetsbaarheden** *In het contract is vastgelegd dat als er actief misbruikte kwetsbaarheden worden gedetecteerd deze tijdig gemeld worden aan opdrachtgever conform de CRA-verplichtingen.*
12	**CRA-conformiteit en CE-markering** *In het contract is vastgelegd dat de door de leverancier geleverde producten voldoen aan CRA-eisen en zijn voorzien van CE-markering daar waar verplicht. (per 11-12-2027)*

Overzicht van de standaard leverancierseisen die vanuit de Baseline Informatiebeveiliging 2 (BIO2) en ISO27001:2023 van toepassing zijn verklaard.

1	**Beoordeling ISMS-beleid leverancier** *De leverancier geeft inzicht in zijn informatiebeveiligingsbeleid, inclusief rollen, incidentmanagement, awareness en continuïteitsmaatregelen zodat dit kan worden beoordeeld.*
2	***ISO 27001-certificering*** *De leverancier beschikt over een geaccrediteerd ISO27001 certificaat met VvT, waarvan de scope de relevante dienst daadwerkelijk afdekt en overlegt dit jaarlijks aan de opdrachtgever.*
3	***Alternatieve Assurance (ISAE)*** *Als leverancier niet beschikt over een ISO27001-certificaat, kan in overleg worden bekeken om als alternatief een ISAE 3402 te accepteren (als scope dekkend voor gecontracteerde dienst).*
4	***Kwetsbaarhedenbeheerproces*** *De leverancier heeft een gedocumenteerd en aantoonbaar werkend proces voor het identificeren en oplossen van kwetsbaarheden. (ontdekking, registratie, beoordeling, herstel en termijnen).*
5	**Personeelsscreening** Medewerkers met toegang tot de systemen en/of data worden gescreend volgens passende normen. (minimaal VOG; VGB voor vertrouwensfuncties)
6	**Data-eigendom en vernietiging** *Er wordt formeel vastgelegd wie eigenaar is van de data na einde van het contract, en het afgeven van een bewijs van vernietiging na contracteinde door de leverancier.*
7	**SOC 2 Type II (optioneel)** *Indien wenselijk (op basis van de risicobepaling) kan er een aanvullende assurance-rapportage worden gevraagd, vooral van toepassing bij clouddiensten.*
8	**Inzicht in de toeleverancierskеten** *De leverancier geeft aantoonbaar inzicht in de keten van onderaannemers (sub-leveranciers), inclusief hun rol en beveiligingsniveau. Dit gaat verder dan alleen contractuele verklaringen.*
9	**Business Continuity Plan (BCP)** *De leverancier beschikt over een getest continuïteitsplan voor de geleverde dienst, inclusief vastgelegde hersteldoelstellingen (RTO/RPO) en test dit op reguliere basis.*
10	**Sub-verwerkersbeleid** *De leverancier maakt inzichtelijk welke derden provinciale data verwerken en informeert de organisatie tijdig over eventuele wijzigingen. (Dit is met name relevant bij cloud- en SaaS-diensten.)*
11	**Transparantie over wijzigingen** *De leverancier informeert de opdrachtgever vooraf over relevante wijzigingen in de dienst of het product en beschikt over een beheerst wijzigingsproces.*
12	**Gestandaardiseerde en beveiligde ontwikkelomgeving** *De leverancier toont aan dat hij bij maatwerkontwikkeling veilige ontwikkelmethoden toepast, zoals een secure SDLC, code reviews en beheer van afhankelijkheden.*
13	**Certificaat gebruik** *Indien er sprake is van openbaar webverkeer wordt er minimaal gebruik gemaakt van vertrouwde OV-certificaten welke geleverd worden door de organisatie.*

14	**Patchmanagement** *De leverancier moet een aantoonbaar patchbeleid hebben met vaste termijnen. Kritieke kwetsbaarheden worden binnen 7 dagen opgelost, hoge risico's binnen 30 dagen.*

Overzicht van de standaard SAAS eisen die vanuit de Baseline Informatiebeveiliging 2 (BIO2) en ISO27001:2023 van toepassing zijn verklaard.

1	**Uptime en beschikbaarheid (SLA)** *Er zijn afspraken over beschikbaarheid (SLA) met meetbare uptimepercentages en financiële consequenties bij niet-naleving. (laag en midden >=99,5%; hoog >=99,9%)*
2	**Auditlogs en toegangslogs** *De organisatie heeft toegang tot logs van gebruik en beheer. Deze zijn exporteerbaar en worden minimaal 12 maanden bewaard.*
3	**Monitoring en SIEM-integratie** *Beveiligingsmonitoring van de geleverde dienst is beschikbaar en kan worden gekoppeld aan het Security Information and Event Management systeem (SIEM) van de organisatie.*
4	**Data-locatie (EU/EER)** *De leverancier garandeert dat de provinciale data wordt opgeslagen binnen de EU/EER, inclusief gebruik van subverwerkers.*
5	**Dataportabiliteit** Data kan worden geëxporteerd in een open en gestandaardiseerd formaat, zodat vendor lock-in wordt voorkomen.
6	**MFA voor alle gebruikers** *MFA is verplicht en afdwingbaar voor zowel eindgebruikers als beheerders, inclusief toegang door de leverancier zelf.*
7	**Rolgebaseerd toegangsbeheer** *Toegang is gebaseerd op rollen en rechten zijn fijnmazig instelbaar volgens het least-privilege principe.*
8	**Encryptie tijdens transport** *Alle communicatie is versleuteld met TLS 1.3 of hoger en zwakke protocollen zijn uitgeschakeld.*
9	**Encryptie van opgeslagen data** *Gegevens die in het product worden opgeslagen, moeten versleuteld zijn om bescherming te bieden bij datalekken of diefstal van systemen.*
10	**DPIA-ondersteuning** *De leverancier levert alle benodigde informatie om een Data Protection Impact Assessment (DPIA) te kunnen uitvoeren.*
11	**Subverwerkersbeleid** *De leverancier geeft inzicht in subverwerkers en informeert vooraf over wijzigingen.*
12	**Pentest door opdrachtgever**

	De organisatie heeft het recht om zelf een onafhankelijke pentest uit te laten voeren op het product of dienst.
13	**Tenant-segmentatie** *Gegevens van verschillende klanten zijn logisch gescheiden. De leverancier toont periodiek bewijs van deze scheiding.*
14	**Scheiding beheeromgeving** *De beheeromgeving van de leverancier is gescheiden van de dienstomgeving. Toegang wordt beperkt en gelogd.*
15	**Incidentmanagement en escalatie** *Er is een formele procedure voor incidentafhandeling met duidelijke meldtermijnen richting de organisatie.*
16	**Wijzigingsbeheer (changemanagement)** *Belangrijke wijzigingen in de dienst worden vooraf aangekondigd (bijv. minimaal 30 dagen) en beheerst uitgevoerd.*