Inkoopeisen Cybersecurity Overheid (ICO)

# ICO informatiebeveiligingseisen

Voor de verwerving van een
Subsidiebeheersysteem voor de Gemeente Dordrecht



versie 1.0 voor clouddiensten

# Inhoud

# Digitale veiligheid: Inkoopeisen Cybersecurity Overheid

Digitale veiligheid is een essentiële randvoorwaarde voor vertrouwen in onze digitale economie en samenleving. De Rijksoverheid heeft ervoor gekozen een samenhangend niveau van veiligheid na te streven. Dit doet ze door in alle geledingen de op ISO27002 gebaseerde 'Baseline Informatiebeveiliging Overheid' (de BIO) te hanteren. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Om invulling te geven aan de BIO bij aanbestedingen en (systeem)verwerving bieden de zogenaamde Inkoopeisen Cybersecurity Overheid (ICO) een gestandaardiseerde basis.

De BIO is leidend voor de gemeente Dordrecht en daarmee zijn de ICO inkoopeisen dat ook. Door de ICO cybersecurity criteria op te nemen bij aanbestedingen stimuleren we de vraag naar digitaal veilige ICT-producten en diensten, de veiligheid van onze organisaties in de Drechtsteden verhogen en een goed voorbeeld geven.

Voor meer informatie, kijk op www.bio-overheid.nl , of specifiek voor ICO op de pagina https://www.bio-overheid.nl/category/ico-producten/ .

## Doel van deze toelichting voor het gevraagde Subsidiebeheersysteem

Voor het subsidiebeheersysteem is de gemeente Dordrecht expliciet op zoek naar een Cloud-gebaseerde oplossing. Daarom vragen wij u specifiek naar de clouddienst-gerelateerde onderwerpen uit de ICO, voor zowel het product zelf, als voor de processen die u als leverancier heeft ingericht en de maatregelen op het gebied van toegangsbeveiliging en huisvesting. Uit het onderdeel 'softwarepakketten' is een beknopte selectie opgenomen, als aanvulling op de eisen voor producteigenschappen.

### Relevante Inkoopeisen Subsidiebeheersysteem

Dit document omvat de ICO eisen uit de ICO wizard ( https://www.bio-overheid.nl/ico-wizard/ ):

Onderdeel **Clouddiensten** (zowel proces- als producteisen):

- Minimale producteigenschappen (PE 1 t/m 17)
- Minimale procesinrichting dienstverlening (PI 1 t/m 17)

Onderdeel **Softwarepakketten** (selectie):

- Minimale toetsing product (TP 1 t/m 11)

Onderdeel **Toegangsbeveiliging**:

- Toegangsbeveiligingseisen fysiek en digitaal (TB 1 t/m 19)

- Alleen eisen van **normaal** en **hoog** belang zijn geselecteerd. Eisen die **alleen** gericht zijn op schaalgrootte zijn **niet** meegenomen.
- De beschrijvingen vanuit de ICO wizard zijn in dit overzicht deels anders geformuleerd voor de leesbaarheid. Enkele eisen die de ICO wizard aanlevert zijn in dit document niet meegenomen omdat de relevantie in deze context laag is.
- Indien u voor de ICO op bovenstaande onderdelen 'clouddiensten, softwarepakketten en toegangsbeveiliging' al een passende standaardbeantwoording heeft, dan kunt u deze beantwoording gemakkelijk gebruiken voor uw reactie op dit document.

### Beantwoordingsbijlage

U kunt uw antwoorden met eventuele verwijzingen naar documenten en bijlagen vastleggen in de bijgevoegde Excel bijlage " Bijlage Invultabel ICO eisen Subsidiebeheersysteem Gemeente Dordrecht v 1.0".

# Clouddiensten: Minimale eisen producteigenschappen (PE 1 t/m 17)

Toon met bewijsstukken en/of verklaringen aan dat de door u aangeboden oplossing minimaal onderstaande methodieken, functionaliteiten en beveiligingseisen borgt.

**PE 1. Transparantie**
- Geef een systeembeschrijving met specifiek aandacht voor jurisdictie (zoals de locatie van uw dienst en de geldende wet- en regelgeving), onderzoeksmogelijkheden (zoals de mogelijkheid de locatie te (laten) inspecteren) en relevante certificaten (zoals ISO27002 / ISO27017 / ISO27018).

**PE 2. IT-functionaliteiten**
- Beschrijf de keten en de borging van relevante BIV-aspecten hierin.

**PE 3. Data en Privacy**
- Beschrijf de maatregelen die u treft vanuit de verschillende dimensies (beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie).

**PE 4. Clouddienstenarchitectuur**
- Beschrijf de architectuur van uw oplossing, specifiek vanuit beveiliging, privacy maar ook koppelbaarheid en bruikbaarheid (denk hierbij aan platformonafhankelijkheid). Zie ook PI 11.

**PE 5. Bedrijfscontinuïteitsservices**
- Beschrijf hoe uw oplossing de geboden beschikbaarheid biedt

**PE 6. Herstelfunctie voor data en clouddiensten**
- Beschrijf de herstelfunctie, onder meer in termen als MTBF en MTTR (hier bedoeld als Mean time to Recovery)

**PE 7. Dataprotectie**
- Beschrijf hoe gegevens binnen uw oplossing worden beschermd, in transport en in rust

**PE 8. Dataretentie en gegevensvernietiging**
- Beschrijf hoe uw oplossing voorziet in zowel dataretentie als gegevensvernietiging

**PE 9. Datascheiding**
- Beschrijf hoe gegevens van de afnemer zijn afgescheiden van andere afnemers en uw eigen (beheer-)organisatie.

**PE 10. Scheiding dienstverlening**
- Beschrijf hoe u uw dienstverlening scheidt voor verschillende afnemers (aanvullend op PE 9 (datascheiding)

**PE 11. Malware-protectie**
- Beschrijf de maatregelen die u treft om malware (e.d.) te detecteren en de gevolgen ervan te mitigeren.

**PE 12. Toegang IT-diensten en data**
- Beschrijf hoe u garandeert dat diensten en data alleen toegankelijk zijn voor bevoegden, in het bijzonder alleen door de juiste afnemer van uw oplossing.

**PE 13. Cryptoservices**
- Beschrijf, aanvullend op PE 7, op welke wijze uw oplossing gegevens versleuteld, in transport en in rust.

**PE 14. Koppelvlakken**
- Beschrijf hoe u datalekken in de keten voorkomt, detecteert en mitigeert

**PE 15. Interoperabiliteit en portabiliteit**
- Beschrijf de interoperabiliteit en portabiliteit van uw oplossing, in termen standaarden, uniformiteit en platformonafhankelijkheid

**PE 16. Logging en monitoring**
- Beschrijf de logging en monitoring die u oplossing biedt en de wijze waarop de verwerkte gegevens beschikbaar zijn (voor de afnemer), ontoegankelijk zijn (voor onbevoegden). Verwijs hierbij (en vul aan op) PE 8.

**PE 17. Multi-tenantarchitectuur**
- Beschrijf de scheiding van verschillende omgevingen voor afnemers, aanvullend op PE 9, PE 10 en PE 12.

# Clouddiensten: Minimale eisen procesinrichting (PI 1 t/m 17)

Toon met bewijsstukken en/of verklaringen aan dat voor de levering van de door u aangeboden oplossing minimaal onderstaande structuren, processen en beveiligingseisen zijn geborgd.

**PI 1. Wet en Regelgeving**
- Beschrijf hoe u borgt dat uw oplossing voldoet aan relevante wet- en regelgeving.

**PI 2. Cloudbeveiligingsstrategie**
- Beschrijf de beveiligingsstrategie voor uw cloudoplossing(en)

**PI 3. Exit-strategie**
- Beschrijf hoe uw oplossing en bijbehorende dienstovereenkomst voorziet in een geborgde en gegarandeerde exit-strategie.

**PI 4. Clouddienstenbeleid**
- Vul waar nodig PI 2 aan met de wijze waarop u uw diensten expliciet heeft afgestemd voor gebruik als clouddienst.

**PI 5. Risicomanagement**
- Beschrijf hoe risicomanagement zowel procedureel als organisatorisch is belegd binnen uw organisatie, gericht op de door u geboden oplossing.

**PI 6. Bedrijfscontinuïteitsmanagement**
- Beschrijf uw BCM proces en hoe dit deel uitmaakt van uw dienstverlening en de bijbehorende dienstovereenkomst.

**PI 7. Beveiligingsorganisatie**
- Beschrijf de wijze waarop u binnen uw dienstverlening beveiliging heeft georganiseerd, waar nodig verwijzend naar PI 4, PI 5 en PI 6.

**PI 8. Standaarden voor clouddiensten**
- Licht toe hoe u standaardisatie ondersteund en integraal borgt binnen uw oplossing.

**PI 9. Risico-assessment**
- Voor uw oplossing voert u een risico-assessment (risico-analyse en risico-evaluatie) uit, op basis van de criteria en de doelstellingen van uw Cloudbeveiligingsstrategie en Clouddienstenbeleid.

**PI 10. Service-orkestratie**
- Voor de servicecomponenten van uw clouddiensten die u samengesteld, geaggregeerd of op een andere wijze gecoördineerd aanbiedt, doet u dit op basis van service-orkestratie.

**PI 11. Clouddienstenarchitectuur**
- Uw oplossing is gebaseerd op een gedocumenteerd en geïmplementeerde clouddienstenarchitectuur waarin de samenhang tussen, de beveiliging van en de verbinding(en) voor het leveren van uit cloudiensten zijn vastgelegd. Zie ook PE 4.

**PI 12. Servicemanagementbeleid en evaluatierichtlijnen**
- Overleg uw servicebeleid, met daarin de door u gehanteerde beheersingsprocessen, controleactiviteiten en beschikbare rapportages

**PI 13. Risico-control**
- Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.

**PI 14. Compliance en assurance**
- Beschrijf hoe u compliancy borgt en hierover verantwoording aflegt.

**PI 15. Technische kwetsbaarhedenbeheer**
- Beschrijf hoe u (technische) kwetsbaarheden registreert en actief inventariseert, alsmede hoe u deze mitigeert en op een verantwoorde wijze deelt met belanghebbenden. Relevante Standaarden : STIX en TAXII (uitwisseling van cyberdreigingsinformatie)

**PI 16. Security-monitoring**
- Beschrijf hoe u regulier en waar nodig ad hoc rapporteert over de wijze waarop uw informatiebeveiligingsmaatregelen effectief zijn.

**PI 17. Beheerorganisatie clouddiensten**
- Beschrijf uw beheerorganisatie, inclusief t.b.v.'s van betrokken functionarissen, waar nodig verwijzend naar PI 5, PI 6 en PI 7.

# Clouddiensten: Minimale toetsing product (TP 1 t/m 11)

Voor uw oplossing dient (de inrichting van) uw oplossing minimaal de volgende maatregelen en functionaliteiten te bieden om de veilige werking van uw oplossing te ondersteunen. Toon met bewijsstukken, verklaringen en/of testresultaten aan dat binnen de door u aangeboden oplossing minimaal onderstaande zaken zijn geborgd.

**TP 1. Bedrijfscontinuïteit**
- Om de bedrijfscontinuïteit te borgen heeft uw organisatie processen, procedures en beheersmaatregelen gedocumenteerd, geïmplementeerd en handhaaft deze.

**TP 2. Input-/output-validatie**
- Uw oplossing heeft functionaliteiten voor het normaliseren en valideren van invoer en voor het schonen van uitvoer

**TP 3. Sessiebeheer**
- Sessies zijn authentiek zijn voor elke gebruiker en worden ongeldig gemaakt na een time-out of perioden van inactiviteit. Relevante standaard: SAML (authenticatie)

**TP 4. Gegevensopslag**
- Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Alleen noodzakelijke gegevens worden opgeslagen (minimale dataset).

**TP 5. Communicatie**
- Uw oplossing past versleuteling, passend bij het classificatieniveau van gegevens, toe op de communicatie van deze gegevens en controleert hierop. Relevante standaarden: TLS, HTTPS en HSTS (beveiligde verbinding) en DNSSEC (ondertekende domeinnaam)

**TP 6. Authenticatie**
- Uw oplossing heeft functionaliteiten voor identificatie en authenticatie van alle typen gebruikers.

**TP 7. Toegangsautorisatie**
- Uw oplossing heeft functionaliteiten voor het toekennen, inzien, aanpassen en verwijderen van autorisaties.

**TP 8. Autorisatiebeheer**
- De rechten die gebruikers (inclusief beheerders) hebben binnen uw oplossing zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies (zgn. Role Based Access, RBAC) zodanig dat scheiding van niet-verenigbare autorisaties mogelijk is.

**TP 9. Applicatielogging**
- Uw oplossing biedt beveiligde signaleringsfunctionaliteiten voor registratie en detectie, zodanig dat de juiste werking van uw oplossing kan worden gecontroleerd en mogelijk problemen tijdig (preventief) worden opgemerkt.

**TP 10. Application Programming Interface (API)**
- Uw oplossing gebruikt uitsluitend veilige API's voor import en export van gegevens.

**TP 11. Gegevensimport**
- Uw oplossing heeft functionaliteiten om niet-vertrouwde (bestands)gegevens uit niet-vertrouwde omgevingen veilig te importeren en deze vervolgens veilig te verwerken en op te slaan.

# Clouddiensten: Toegangsbeveiligingseisen (TB 1 t/m 19)

Om gebruik te kunnen maken van SaaS diensten is het van groot belang dat de toegang tot deze diensten en de systemen die hieraan ondersteunend adequaat zijn beveiligd, zodanig dat zowel **fysieke** als **digitale** toegang alleen mogelijk is voor bevoegden en uitsluitend tot de toegewezen diensten en systemen, conform het toegangsbeveiligingsbeleid en de inrichting daarvan. De onderstaande items zijn geclusterd, zo kunt u ze makkelijker integraal beantwoorden.

## Beleid en organisatie toegangsbeveiliging

Om professioneel invulling te geven aan toegangsbeveiliging:

**TB 1.** Hoe heeft u toegangsbeveiligingsbeleid ingericht

**TB 2.** Hoe heeft u het eigenaarschap van elk toegangsbeveiligingssysteem belegd en geborgd

**TB 3.** Is toegangsbeveiliging functioneel belegd binnen uw organisatie ('Beveiligingsfunctie')

**TB 4.** Is toegangsbeveiliging organisatorisch belegd met duidelijke t.b.v.'s (taken, bevoegdheden en verantwoordelijkheden.) en rapportagelijnen ('Beveiligingsorganisatie')

**TB 5.** Alle medewerkers van de organisatie zijn op de hoogte van het toegangsbeleid, volgen dit en krijgen regelmatig functiegerichte bijscholing van de beleidsregels en procedures van de organisatie

*Toon het bovenstaande aan met bewijsstukken en/of verklaringen (items TB1 t/m TB5).*

## Procedures toegangsbeveiliging

Voor toegangsbeveiliging heeft u minimaal de volgende procedures ingericht en geborgd:

**TB 6.** Toegangsverleningsprocedure, om toegangsrechten toe te wijzen, aan te passen en in te trekken

**TB 7.** Registratieprocedure, om het aanvragen en intrekken van toegangsrechten vast te leggen

**TB 8.** Inlogprocedure, om toegang tot systemen en toepassingen te beheersen en te beveiligingen.

*Toon het bovenstaande aan met bewijsstukken en/of testen (items TB6 t/m TB8).*

## Fysieke toegangsbeveiliging

U heeft specifiek voor de fysieke toegang tot systemen en gegevensopslag maatregelen getroffen om toegang te reguleren, te monitoren en vast te leggen. Daartoe heeft u minimaal beleid, procedures en systemen ingericht om aan de onderstaande eisen invulling te geven:

**TB 9.** Fysieke toegangsbeveiliging, waardoor beveiligde gebieden alleen voor bevoegd personeel toegankelijk zijn, conform het beleid

**TB 10.** Fysieke bescherming tegen natuurrampen, stroomuitval, kwaadwillende aanvallen of ongelukken en andere verstoringen wordt conform ontwerp toegepast;

**TB 11.** Gebeurtenissen rond fysieke toegang worden geregistreerd (logging en monitoring), waaronder gebruikersactiviteiten, incidenten en uitzonderingen. Deze gebeurtenissen worden bewaard en conform beleid regelmatig beoordeeld en verwerkt.

*Toon het bovenstaande aan met bewijsstukken, verklaringen en/of testen (items TB9 t/m TB11).*

## Digitale toegangsbeveiliging

Voor de logische, digitale toegang tot systemen en gegevens heeft u de volgende maatregelen getroffen en/of ingericht:

**TB 12.** Autorisatieproces, een formeel proces voor het beheren en beheersen van toegangsrechten

**TB 13.** Autorisaties worden uitsluitend toegekend conform het toegangsbeveiligingsbeleid

**TB 14.** Wachtwoordbeheer, conform beleid en passend binnen de specifieke context

**TB 15.** Speciale toegangsrechtenbeheer, waarbij bijzondere autorisaties zeer beperkt en afgeschermd zijn

**TB 16.** Functiescheiding, zodanig dat de kans misbruik en onbevoegd gebruik wordt geminimaliseerd

**TB 17.** Geheime authenticatie-informatie, alleen toewijsbaar via een formeel proces

**TB 18.** Gebeurtenissen rond digitale toegang worden geregistreerd (logging en monitoring), waaronder gebruikersactiviteiten, incidenten en uitzonderingen. Deze gebeurtenissen worden bewaard en conform beleid regelmatig beoordeeld en verwerkt

**TB 19.** Beleid voor het gebruik van cryptografische beheersmaatregelen is opgesteld en geïmplementeerd voor de bescherming van de authenticatie-informatie.

*Toon het bovenstaande aan met bewijsstukken, verklaringen en/of testen (items TB12 t/m TB19).*