

Programma van Eisen

ten behoeve van de aanbesteding

Softwarebroker

Referentienummer: IBMN-2026-MOL-MK-001

Datum: 10 juli 2026

Versie: 1.0 - Definitief

Inhoud

Programma van Eisen	3
1: Algemene eisen	3
2. Dienstverlening	4
3. Portaal & automatisering	5
4. Eisen aan uitvoering van de werkzaamheden	5
5. Facturen en prijzen	6
6. Communicatie, managementrapportage en evaluatie	7
7. Privacy & Informatiebeveiliging	8
8. Einde overeenkomst en exit.....	9
Appendix A — Eisenprofiel per risicoklasse (Laag/Midden/Hoog).....	11

Programma van Eisen

1: Algemene eisen

1.1 Naleving wet- en regelgeving

De opdrachtnemer draagt er zorg voor dat de uitvoering van de dienstverlening te allen tijde voldoet aan de geldende wet- en regelgeving.

De opdrachtnemer is gedurende de looptijd van de overeenkomst volledig verantwoordelijk voor het blijven voldoen aan deze wet- en regelgeving.

1.2 Vertrouwelijkheid en gegevensbescherming

De opdrachtnemer behandelt alle informatie die in het kader van de opdracht wordt verkregen als vertrouwelijk en verstrekt deze uitsluitend aan derden na voorafgaande schriftelijke toestemming van opdrachtgever, tenzij een wettelijke verplichting tot verstrekking bestaat.

De opdrachtnemer voldoet aantoonbaar aan alle relevante wet- en regelgeving op het gebied van gegevensbescherming en informatiebeveiliging.

1.3 Conformiteit met opdracht en inschrijving

De opdrachtnemer garandeert dat de dienstverlening volledig wordt uitgevoerd conform:

- de offerteaanvraag;
- de bijbehorende bijlagen;
- en de eigen inschrijving.

Afwijkingen zijn uitsluitend toegestaan na voorafgaande schriftelijke instemming van opdrachtgever.

1.4 Integriteit en onafhankelijkheid

De opdrachtnemer handelt gedurende de looptijd van de overeenkomst integer en zorgvuldig, en voorkomt (de schijn van) belangenverstrengeling.

Indien sprake is van mogelijke conflicterende belangen met andere opdrachtgevers of activiteiten, meldt de opdrachtnemer dit onverwijld aan de opdrachtgever en treft passende maatregelen.

1.5 Aansprakelijkheid voor uitvoering

De opdrachtnemer is integraal verantwoordelijk voor de kwaliteit en continuïteit van de dienstverlening, inclusief de inzet van eventuele onderaannemers binnen de providerboog.

De opdrachtnemer blijft te allen tijde aanspreekpunt en eindverantwoordelijk richting opdrachtgever.

1.6 Eigendom en toegankelijkheid van data

De opdrachtgever blijft te allen tijde eigenaar van alle data die door opdrachtgever beschikbaar wordt gesteld dan wel door opdrachtnemer wordt verzameld of gegenereerd in het kader van de uitvoering van de opdracht.

De opdrachtnemer waarborgt dat de opdrachtgever te allen tijde volledige, directe en onbelemmerde toegang heeft tot deze data.

De opdrachtnemer verleent op eerste verzoek en zonder aanvullende kosten

medewerking aan het beschikbaar stellen, ontsluiten en, indien van toepassing, overdragen van deze data in een open, gangbaar en machine leesbaar formaat.

2. Dienstverlening

2.1 Doel van de opdracht

Opdrachtnemer levert standaardsoftwarelicenties en abonnementen en verzorgt de administratieve afhandeling (offerte, bestelling, licentiebewijs, facturatie) via een portal.

2.2 Reikwijdte van de dienstverlening

Opdrachtnemer garandeert dat de gemeente te allen tijde over rechtmatige gebruiksrechten beschikt en registreert licenties (waar mogelijk) op naam van de gemeente

2.3 Assortiment en leveringsplicht

Opdrachtnemer levert licenties/abonnementen op software binnen de scope van de opdracht zonder beperking, tenzij producenten levering via resellers uitsluiten.:

2.4 Microsoft-specifiek (1)

- A. Opdrachtnemer beschikt over een geldige Microsoft LSP-status. De Microsoft-licenties worden conform de geldende voorwaarden van het VNG GT-Microsoft Framework aangeboden.
- B. Opdrachtnemer kan Microsoft-constructies (EA, SCE, CSP en Azure) leveren/verlengen/beheren op expliciete opdracht van de gemeente

2.5 Offerteproces en levertijden

- A. Ontvangstbevestiging van een offerteaanvraag binnen 24 uur; offerte binnen 5 werkdagen; spoed binnen 1 werkdag.
- B. Offertes zijn transparant en bevatten minimaal: looptijd, aantallen, prijsopbouw (producentprijs/listprijs waar beschikbaar, inkoopprijs, mark-up, eindprijs).
- C. Licenties worden geleverd binnen 5 werkdagen na opdracht, tenzij producent aantoonbaar anders levert. Met uitzondering van spoedaanvragen.
- D. Spoedlicenties worden geleverd binnen 1 werkdag na opdrachtverlening, tenzij aantoonbaar is dat de producent deze termijn niet kan realiseren.

2.6 Verlengingen

Verlengingen vinden uitsluitend plaats op expliciete opdracht van de gemeente. Opdrachtnemer signaleert uiterlijk 3 maanden vóór de verlenging cq opzegtermijn van de betreffende licentie-, onderhouds- of contractperiode dat verlenging mogelijk aan de orde is. Stilzwijgende verlenging door opdrachtnemer of derden is niet toegestaan.

2.7 Licentiebeheer (administratief)

Opdrachtnemer houdt een actuele en gestructureerde administratie bij van via opdrachtnemer geleverde licenties en abonnementen.

2.8 Servicedesk

Opdrachtnemer biedt een Servicedesk voor spoedprocedures, administratieve vragen, portaalgebruik en vragen over bestellingen, licenties, contracten en facturatie. De

servicedesk is bereikbaar via e-mail en telefonisch op doordeweekse werkdagen van 08:30 tot 17:00 uur. De voertaal van de Servicedesk is Nederlands.

3. Portaal & automatisering

3.1 Beschikbaarheid en toegang

Opdrachtnemer stelt uiterlijk per ingangsdatum van de raamovereenkomst een via internet bereikbaar portaal beschikbaar aan de gemeente. De portal heeft het kenmerk van een webportaal.

3.2 Autorisatieniveau's

Het portaal ondersteunt verschillende autorisatieniveaus (rollen/rechten), waaronder ten minste: raadplegen en bestellen.

3.3 Functionaliteit

Het portaal biedt minimaal: productcatalogus, rapportages, offerteaanvragen, ontvangen offertes, bestellingen plaatsen, ontvangen licentiebewijs/proof-of-license (en key waar van toepassing), statusoverzicht offertes/leveringen en facturatieoverzicht.

3.4 Export

Het portaal maakt (realtime) export van licentiegegevens mogelijk in gangbare formaten (.CSV of .XLS).

4. Eisen aan uitvoering van de werkzaamheden

4.1 Algemeen

De opdrachtnemer voert de werkzaamheden zodanig uit dat deze aantoonbaar bijdragen aan het behalen van de doelstellingen van de opdracht.

De opdrachtnemer draagt zorg voor een ordelijke, consistente en kwalitatief hoogwaardige uitvoering van de dienstverlening, waarbij de belangen van de medewerker en opdrachtgever centraal staan.

4.2 Kwaliteit van uitvoering

De opdrachtnemer:

- Zorgt voor een consistente kwaliteit van uitvoering, ongeacht de inzet van medewerkers;
- borgt dat werkzaamheden uitsluitend worden uitgevoerd door voldoende gekwalificeerde en geïnstrueerde personen;
- is verantwoordelijk voor de kwaliteit van alle uitgevoerde werkzaamheden.

4.3 Continuïteit van dienstverlening

De opdrachtnemer:

- waarborgt de continuïteit van de dienstverlening gedurende de looptijd van de overeenkomst;
- draagt zorg voor adequate vervanging bij afwezigheid van medewerkers;
- voorkomt dat verstoringen in de personele inzet leiden tot vertraging of kwaliteitsverlies in de uitvoering.

De kosten voor vervanging of kennisoverdracht komen voor rekening van de opdrachtnemer.

4.4 **Uitvoering en resultaat**

De opdrachtnemer:

- zorgt voor een tijdige en correcte realisatie van de dienstverlening zoals beschreven in de offerteaanvraag;
- bewaakt actief de voortgang van de werkzaamheden en stuurt bij waar nodig;
- signaleert risico's en knelpunten in de uitvoering en neemt passende maatregelen;
- stemt de uitvoering af met betrokken partijen en waarborgt een efficiënte samenwerking in de keten.

4.5 **Transparantie en navolgbaarheid**

De opdrachtnemer:

- maakt keuzes en besluitvorming in de uitvoering inzichtelijk en navolgbaar voor de opdrachtgever;
- legt relevante acties en beslissingen vast;
- is in staat om desgevraagd verantwoording af te leggen over de uitvoering van de werkzaamheden.

5. Facturen en prijzen

5.1 **Mark-up en transparantie**

Opdrachtnemer hanteert één transparant, vast opslagpercentage (all-in) gedurende de gehele contractduur incl. verlengingen.

5.2 **All-in opslagpercentage**

Opdrachtnemer hanteert geen additionele kosten/toeslagen buiten inkooprijzen en opslag.

5.3 **Betaling**

Betaling van correcte en volledig gespecificeerde facturen vindt plaats binnen 30 dagen na ontvangst.

De opdrachtnemer richt zijn administratieve organisatie zodanig in dat deze aansluit op de facturatie- en verantwoordingsvereisten zoals opgenomen in de overeenkomst en bijbehorende documentatie.

5.4 **Rapportages en aanvullende werkzaamheden**

Rapportages en overige werkzaamheden die noodzakelijk zijn voor de uitvoering, monitoring en verantwoording van de dienstverlening, worden uitgevoerd zonder aanvullende kosten voor de opdrachtgever, tenzij uitdrukkelijk anders overeengekomen

5.5 **Indexering**

Indexatie van de onderliggende licentieprijzen vindt plaats conform artikel 11 van de GIBIT 2025. Het opslagpercentage is gedurende de overeenkomst niet aan indexatie en/of andere veranderingen onderhevig.

5.6 **Facturering**

Facturen worden digitaal aangeleverd (PDF en/of UBL), bij voorkeur via PEPPOL, en zijn helder gespecificeerd per licentie/product met aantallen en looptijd (begin- en

einddatum). Facturen zijn in ieder geval voorzien van het inkoopnummer zoals per nadere opdracht aangedragen door opdrachtgever.

6. Communicatie, managementrapportage en evaluatie

6.1 Contractmanagement en aanspreekpunten

De opdrachtnemer wijst voor het contractmanagement één vast aanspreekpunt aan (single point of contact) dat bevoegd is om namens opdrachtnemer afspraken te maken en besluiten voor te bereiden.

Daarnaast wijst opdrachtnemer ten minste één operationeel aanspreekpunt aan voor de (dagelijkse) afstemming.

De opdrachtnemer borgt dat beide contactpersonen gedurende werkdagen bereikbaar zijn via e-mail en telefonisch tussen 09:00 en 17:00 uur (uitgezonderd wettelijke feestdagen).

6.2 Vervanging contactpersonen en kennisborging

De opdrachtnemer meldt voorgenomen vervanging van vaste contactpersonen zo vroeg mogelijk en uiterlijk twee weken vooraf.

Vervanging vindt zodanig plaats dat continuïteit en kwaliteit van de dienstverlening niet worden beïnvloed. Opdrachtgever behoudt het recht om gemotiveerd bezwaar te maken tegen een vervanger indien deze aantoonbaar niet passend is voor de rol.

6.3 Overlegstructuur (governance)

De opdrachtnemer neemt deel aan de overlegstructuur zoals hieronder beschreven en levert de benodigde input tijdig aan.

Implementatie overleg

Partijen maken bij de start van de implementatie afspraken over de aard en frequentie van het implementatieoverleg. Uitgangspunt is dat dit ten minste tweewekelijks plaatsvindt.

Tactisch overleg (minimaal per kwartaal)

Doel: sturen op voortgang, kwaliteit, knelpunten, risico's, verbetermaatregelen en planning.

De opdrachtnemer bereidt het overleg voor (conceptagenda en input) en verzorgt de vastlegging van besluiten en acties.

Strategisch overleg (minimaal jaarlijks)

Doel: evaluatie samenwerking, ontwikkelingen (wetgeving/markt/beleid), doorontwikkeling van dienstverlening en mogelijke bijstellingen van werkwijze.

Indien de situatie daarom vraagt, kan opdrachtgever de overlegfrequentie van het tactisch en/of strategisch overleg tijdelijk verhogen.

6.4 Rapportages (inhoud en kwaliteit)

Opdrachtnemer levert minimaal elk kwartaal een overzicht van actuele licenties/abonnementen (aantallen, einddata en omschrijvingen) of maakt

dit realtime oproepbaar via het portal. Indien wordt gekozen voor een realtime overzicht, dient dit overzicht exporteerbaar te zijn.

6.5 **Wijzigingen en doorontwikkeling rapportage**

Opdrachtgever kan gedurende de looptijd wijzigingen aanbrengen in de rapportageformaten of rapportage-inhoud indien dit noodzakelijk is voor sturing of verantwoording. De opdrachtnemer werkt hieraan mee en implementeert wijzigingen binnen een redelijke termijn.

6.6 **Evaluatie en verbetercyclus**

De opdrachtnemer neemt deel aan evaluatiemomenten en borgt een continue verbetercyclus. In evaluaties worden minimaal besproken:

- prestaties en kwaliteit (incl. klachten, afwijkingen en verbeterpunten);
- samenwerking en communicatie;
- naleving afspraken en doorlooptijden;
- ontwikkelingen in markt/wetgeving/beleid met impact op uitvoering;
- verbetervoorstellen en innovatie die aantoonbaar bijdragen aan doelmatigheid/doeltreffendheid.

Opdrachtnemer legt verbeteracties vast, inclusief eigenaar en opvolging, en rapporteert de voortgang daarvan in de reguliere rapportage.

7. Privacy & Informatiebeveiliging

7.1 **Verwerkingsverantwoordelijkheid (AVG)**

De opdrachtnemer wordt aangemerkt als (zelfstandig) verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming (AVG) ten aanzien van de eigen verwerkingen van persoonsgegevens.

7.2 **Verwerking buiten de EER**

De opdrachtnemer zal geen persoonsgegevens (laten) verwerken buiten de Europese Economische Ruimte (EER).

7.3 **Eisen ten aanzien van informatiebeveiliging.**

Op deze opdracht zijn de eisen van Appendix A integraal van toepassing. De opdracht valt onder risicoklasse Midden (M), waarbij de verplichte eisen volgen uit Appendix A (LMH-eisenprofiel). Afwijkingen zijn uitsluitend toegestaan via het in Bijlage A beschreven afwijkingsproces.

Leverancier motiveert expliciet wanneer een generieke eis niet van toepassing is en beschrijft (waar relevant) gelijkwaardige alternatieven en compensatoire maatregelen conform Bijlage A.

8. Einde overeenkomst en exit

8.1 Algemene verplichting bij beëindiging

Bij beëindiging van de overeenkomst, om welke reden dan ook, werkt de opdrachtnemer actief en zonder aanvullende kosten mee aan een zorgvuldige overdracht van de dienstverlening aan:

- een opvolgende opdrachtnemer; of
- de opdrachtgever, indien geen opvolgende opdrachtnemer wordt aangewezen.

De opdrachtnemer waarborgt dat de continuïteit van de dienstverlening aan woningeigenaren tijdens de overdracht niet wordt onderbroken.

8.2 Specifieke exit verplichtingen Microsoft-licenties

Opdrachtnemer is verplicht om volledige en onmiddellijke medewerking te verlenen aan een versnelde CSP partner-to-partner transfer van Microsoft-licenties, op eerste verzoek van opdrachtgever.

8.3 Overdracht van werkzaamheden en dossiers

De opdrachtnemer:

- draagt zorg voor een volledige, tijdige en gestructureerde overdracht van alle lopende werkzaamheden;
- levert een actueel en compleet overdrachtsdocument aan met daarin ten minste:
 - lopende dossiers,
 - contactpersonen;
 - geplande activiteiten;
 - openstaande acties en verplichtingen.
- verleent medewerking aan kennisoverdracht aan de opdrachtgever of opvolgende opdrachtnemer.

8.4 Overdracht van data

De opdrachtnemer:

- draagt zorg voor een volledige en tijdige overdracht van alle relevante en toegestane data die in het kader van de opdracht is verzameld of gegenereerd;
- stelt deze data beschikbaar in open, gangbare en duurzame bestandsformaten;
- garandeert dat de overgedragen data volledig, juist en bruikbaar zijn;
- levert de data binnen een met de opdrachtgever afgestemde termijn.

Indien van toepassing werkt de opdrachtnemer actief mee aan de migratie van data naar systemen van de opdrachtgever of een opvolgende opdrachtnemer.

8.5 Continuïteit en afronding

De opdrachtnemer:

- rondt lopende werkzaamheden ordelijk af, tenzij anders overeengekomen;
- voorkomt dat beëindiging leidt tot onduidelijkheid of vertraging in lopende trajecten met woningeigenaren;
- stemt actief af met opdrachtgever over prioriteiten in de afrondingsfase.

8.6 Bewaring en vernietiging van data

Na overdracht van de data:

- bewaart de opdrachtnemer gegevens uitsluitend voor zover dit noodzakelijk is op grond van geldende wet- en regelgeving;
- draagt zorg voor tijdige en aantoonbare vernietiging van data van de opdrachtgever na afloop van de toepasselijke bewaartermijnen;

- waarborgt dat persoonsgegevens worden verwerkt en vernietigd conform de geldende privacywetgeving.
-

Appendix A — Eisenprofiel per risicoklasse (Laag/Midden/Hoog)

Deze appendix hoort bij Generieke eisen Gemeente Molenlanden.

A.1 Gebruik en reikwijdte

Deze Appendix A is van toepassing op opdrachten **boven de drempel** (gegevensverwerking, cloud, SaaS en vergelijkbare digitale diensten).

Voor **overige ICT-inkopen** kan deze set als kader worden gebruikt, waarbij eisen worden “getailord” op basis van risicoklasse en leveringsmodel (zie §0.1).

Waar een eis als **verplicht** is aangemerkt voor een risicoklasse, is dit een **contractuele eis**. Afwijkingen alleen via het formele afwijkingsproces (zie §0.3).

A.2 Legenda

V = Verplicht

A = Aanvullend verplicht (bovenop de minimale vloer)

O = Optioneel / alleen indien relevant voor het leveringsmodel of de oplossing

— = Niet van toepassing / niet vereist

A.3 Overzicht: minimale eisen per risicoklasse

Let op: “V” bij Laag betekent dat het *altijd* geldt voor L/M/H, maar bij M/H kunnen aanvullende eisen gelden.

1) Basiskader (scope, risicoklasse, architectuur)

Onderwerp	Laag	Midden	Hoog	Verwijzing
Toepassingskader & drempel + tailoring	V	V	V	§0.1
Risicoklassen (L/M/H) leidend	V	V	V	§0.2
Architectuur leidend + afwijkingsproces	V	V	V	§0.3
Geen “leverancier voldoet aan BIO2” (correcte duiding)	V	V	V	§1

2) Domein 2 — Organisatie-eisen leverancier (Cbb art. 10–11)

Onderwerp	Laag	Midden	Hoog	Verwijzing
Transparantie risicomanagement & keten (subleveranciers)	V	V	V	§3.1
Minimale vloer: leveranciersregisterinformatie (op verzoek)	V	V	V	§3.2.1
Minimale vloer: schriftelijke beveiligingsafspraken	V	V	V	§3.2.2
Minimale vloer: incidentmeldplicht	V	V	V	§3.2.3
Minimale vloer: kwetsbaarheidsmanagement & patchproces	V	V	V	§3.2.4
Minimale vloer: personeel/toegang/geheimhouding (JML/least privilege)	V	V	V	§3.2.5
Onafhankelijke assurance (opzet/bestaan/werking) met dienst-scope	—	A	A	§3.3.1
Aanvullend onderzoek/auditrecht Molenlanden	—	—	A	§3.3.2
Subleveranciers vooraf melden + wijzigingsbeheer	—	A	A	§3.3.3
Screening + training personeel (passend bij risico)	—	A	A	§3.3.4
Continuïteit & herstel (BC/DR), testen + RTO/RPO	—	A	A	§3.3.5

3) Domein 3 — Product-/diensteisen (SaaS/Cloud + CRA waar relevant)

Onderwerp	Laag	Midden	Hoog	Verwijzing
Leveringsmodel-differentiatie (SaaS vs product/CRA)	V	V	V	§4.1
Security-by-default + hardeningopties	V	V	V	§4.2.1
Encryptie in transit + at rest (tenzij n.v.t.)	V	V	V	§4.2.2
Logging/audittrail (auth, admin, mutaties)	V	V	V	§4.2.3
Scheiding omgevingen (prod + test/acceptatie passend)	V	V	V	§4.2.4
Pentest/security test op specifieke dienst/omgeving	—	—	A	§4.3.1
SBOM / inzicht componenten en dependencies	—	A	A	§4.3.2
Patch-SLA / concrete termijnen kwetsbaarheden	—	A	A	§4.3.3

Beheersing configuratie- en integratierisico's	—	A	A	\$4.3.4
CRA-conformiteit (alleen indien CRA van toepassing)	O	O	O	\$4.4

4) Cloud, data en soevereiniteit (incl. DICTU)

Onderwerp	Laag	Midden	Hoog	Verwijzing
Azure-tenant compatibiliteit / cloudstrategie passend	V	V	V	\$5.1
Azure-integratie (Azure AD / logging/monitoring)	—	A	A	\$5.1
EU-dataverwerking (data residency EU)	V	V	V	\$5.2.1
Transparantie datatoegang/jurisdictie + mitigaties	V	V	V	\$5.2.2
Sleutelbeheeropties / (waar mogelijk) CMK of compensaties	—	A	A	\$5.2.3
Exit-/dataportabiliteitstest	—	—	O/A*	\$5.2.4

*Bij Hoog risico: **verplicht meewerken** als Molenlanden dit verlangt; opname als expliciete contracteis aanbevolen in de aanbestedingstekst.

5) Open standaarden & interoperabiliteit

Onderwerp	Laag	Midden	Hoog	Verwijzing
Open standaarden (Forum Standaardisatie)	V	V	V	\$6.1
Gemeentelijke koppelingen (GEMMA/Digikoppeling/StUF) waar van toepassing	O	A/O	A/O	\$6.2
API & export in open formaten (lock-in preventie)	—	A	A	\$6.3

6) IAM (Azure AD, lifecycle, privileged access)

Onderwerp	Laag	Midden	Hoog	Verwijzing
SSO via Azure AD (SAML/OIDC), geen lokale accounts tenzij afwijking	—	A	A	\$7.1
Provisioning/lifecycle (SCIM of gelijkwaardig)	—	A	A	\$7.2

Privileged access eisen (least privilege, traceerbaar, JIT waar relevant)	—	—	A	\$7.3
---	---	---	---	-------

7) Technische & functionele eisen

Onderwerp	Laag	Midden	Hoog	Verwijzing
Browser/device-onafhankelijk (Edge/Chrome/Firefox/Safari/Brave)	V	V	V	\$8.1
Geen lokale componenten op locaties (tenzij expliciet)	—	A	A	\$8.2
Plug-ins alleen generiek/browservergelijk, gedocumenteerd	V	V	V	\$8.3
Test/acceptatievoorziening passend bij dienst	V	V	V	\$8.4
Performance aantoonbaar passend (evt. 200 users/3 sec)	—	A	A	\$8.5
Beschikbaarheid/SLA/onderhoud & escalatie	—	A	A	\$8.6
Toegankelijkheid (WCAG) indien UI voor medewerkers/burgers	O	A/O	A/O	\$8.7

8) Privacy & gegevensbescherming

Onderwerp	Laag	Midden	Hoog	Verwijzing
AVG + verwerkersovereenkomst + transparantie subverwerkers/datastromen (indien persoonsgegevens)	O	A/O	A/O	\$9.1
DPIA-ondersteuning (documentatie, TOMs, datastromen, bewaartermijnen)	—	A	A	\$9.2
Bewaartermijnen & aantoonbare vernietiging bij einde contract	—	A	A	\$9.3

9) Exit & lock-in preventie

Onderwerp	Laag	Midden	Hoog	Verwijzing
Data-export voor exit in open formaten	V	V	V	\$10.1

Exit-plan (stappen, termijnen, overdracht config/documentatie)	—	A	A	§10.2
Beëindiging: intrekken toegang + veilige overdracht/vernietiging	—	A	A	§10.3

A.4 Minimale set “altijd opnemen” in aanbestedingstekst (boven drempel)

Om het praktisch te maken: bij alle opdrachten boven de drempel wordt aangeraden om in de aanbesteding expliciet ten minste deze elementen op te nemen:

Risicoklasse (L/M/H) en leveringsmodel (SaaS/laaS/PaaS/COTS/maatwerk)

Architectuurleidend + afwijkingsproces (§0.3)

Domein 2 minimale vloer (§3.2)

Domein 3 basiseisen (§4.2)

EU-dataverwerking + transparantie (§5.2.1–§5.2.2)

Open standaarden (§6.1)

Exit/export (§10.1)

(Bij M/H) assurance met dienst-scope (§3.3.1) en DPIA-ondersteuning (§9.2)

A.5 Notitie over “waar van toepassing”

Voor eisen met markering **O** (“waar van toepassing”) geldt:

Molenlanden bepaalt in de aanbesteding of een eis van toepassing is, gebaseerd op leveringsmodel, gegevenssoorten, integraties en impact.

De leverancier motiveert expliciet wanneer hij meent dat een “O”-eis niet van toepassing is.

A.6 — Korte eisenprofiel-samenvatting per risicoklasse (zonder tabellen)

Risicoklasse LAAG (L) — “Basisvloer + passend, lichtgewicht bewijs”

Bij **laag risico** gelden de **basis- en hygiëne-eisen** voor digitale diensten boven de drempel. De oplossing/dienst:

Past binnen de architectuur van Mollenlanden; afwijkingen uitsluitend via formeel afwijkingsproces met compensaties.

Hanteert **transparantie** over risicomanagement en (indien aanwezig) relevante subleveranciers.

Heeft contractueel geborgd: **incidentmelding, kwetsbaarheidsproces/patchproces, schriftelijke beveiligingsafspraken**, en **toegangsbeheer** (least privilege, geheimhouding, joiner/mover/leaver).

Voldoet aan **product/dienst basis-security**: security-by-default, encryptie in transit/at rest (tenzij aantoonbaar n.v.t.), logging/audittrail, en een passende test/acceptatievoorziening.

Voldoet aan **EU-dataverwerking** en **transparantie over datatoegang/jurisdictie** (minimumeisen soevereiniteit).

Ondersteunt **open standaarden** waar relevant en levert **exitbaarheid**: export in open formaten zonder onredelijke belemmeringen.

Functioneert device- en browseronafhankelijk; plug-ins alleen generiek en gedocumenteerd.

Kenmerk L: geen zware assurance-eisen als ISO27001 “moet”; bewijs is “passend en proportioneel”.

Risicoklasse MIDDEN (M) — “Basisvloer + aantoonbaarheid + Azure/IAM en assurance met scope”

Bij **midden risico** geldt alles van **Laag (L)**, plus extra eisen gericht op aantoonbaarheid en beheersing van keten en integraties. De leverancier:

Levert **onafhankelijke assurance** (bijv. ISO27001/SOC2/ISAE) die **expliciet de gecontracteerde dienst/omgeving in scope** heeft (dus niet alleen “hoofdkantoor-certificaat”).

Meldt en beheerst **subleveranciers/subverwerkers** (vooraf inzicht + wijzigingsbeheer) en borgt gelijkwaardige beveiligingsafspraken in de keten.

Ondersteunt **Azure AD SSO** (SAML/OIDC) en waar passend **lifecycle/provisioning** (bijv. SCIM of gelijkwaardig).

Levert **aanvullende product/dienst eisen**: concrete patchtermijnen, aanvullende logging, mitigatie van integratie-/configuratie-risico's, en waar relevant SBOM of component-inzicht.

Levert **SLA's** voor beschikbaarheid, onderhoud en escalatie passend bij de dienst.

Werkt mee aan **DPIA-ondersteuning** indien persoonsgegevens worden verwerkt (datastromen, TOMs, bewaartermijnen, subverwerkers).

Kenmerk M: aantoonbaarheid via third-party assurance **met dienst-scope** + verplichte Azure/IAM-integratie waar relevant.

Risicoklasse HOOG (H) — “Streng regime: assurance + aanvullend onderzoek + pentest + CMK/exit-test”

Bij **hoog risico** geldt alles van **Midden (M)**, met extra eisen voor kritieke processen, gevoelige/grootschalige persoonsgegevens en sterke afhankelijkheden. De leverancier:

Levert jaarlijks **onafhankelijke assurance** met dekkende scope én accepteert **aanvullend onderzoek/auditrecht** door of namens Molenlanden (proportioneel, vooraf afgestemd).

Borgt strikte **ketenbeveiliging**: subverwerkers vooraf melden/goed beheer, aantoonbare keteneisen, en passende screening/training van personeel met privileged access of toegang tot gevoelige data.

Levert **BC/DR-maatregelen** met aantoonbare testen en contractuele **RTO/RPO** waar passend.

Levert **product/dienst-zekerheden** op hoog niveau: periodieke **pentest/security test op de specifieke omgeving/configuratie**, harde patch-SLA's, SBOM/component-inzicht, en aantoonbare beheersing van integratie-risico's in de Molenlanden-tenant.

Voldoet aan verzwaarde **soevereiniteit/cryptografie-eisen**: EU-dataverwerking, transparantie datatoegang, en waar mogelijk **customer-managed keys** of gelijkwaardige compensaties.

Ondersteunt **privileged access controls** (least privilege, traceerbaar, geen shared admin; waar relevant tijdelijke elevatie/JIT).

Ondersteunt **exit-plan** én (indien gevraagd) **exit-/dataportabiliteitstest**, plus aantoonbare data-vernietiging/overdracht bij einde contract.

Kenmerk H: “bewijs + verificatie” (assurance én aanvullend onderzoek), plus technische diepgang (pentest, CMK waar mogelijk, streng IAM, continuïteit).