Bijlage 4C-1 – Toepasselijkheidsmatrix ICT-eisen E1 t/m E86
behorende bij Bijlage 4C – ICT-randvoorwaarden gebouwbeheersysteem en koppelingen

## Oplegblad en toepasselijkheidsmatrix Bijlage 4C – ICT-randvoorwaarden gebouwbeheersysteem en koppelingen

Dit document vormt een aanvulling op en nadere afbakening van Bijlage 4C – ICT-randvoorwaarden gebouwbeheersysteem en koppelingen.

Bijlage 4C bevat een generiek gemeentelijk ICT-eisenkader. Niet alle daarin opgenomen eisen zijn onverkort van toepassing op het gebouwbeheersysteem en de bijbehorende beheer-/Cloudomgeving binnen deze opdracht.

De in dit oplegblad opgenomen toepasselijkheid en nadere afbakening zijn leidend voor de toepassing van de eisen E1 tot en met E86.

Indien de inhoud van dit oplegblad afwijkt van de oorspronkelijke tekst van Bijlage 4C, prevaleert de in dit oplegblad opgenomen bepaling.

Voor eisen die als niet van toepassing zijn aangemerkt, behoeft Inschrijver binnen deze opdracht niet aan de betreffende eis te voldoen.

Voor eisen die uitsluitend voor zover relevant of met nadere afbakening van toepassing zijn, geldt uitsluitend de hieronder opgenomen afbakening.

De verplichting tot het beschikbaar stellen en gebruiken van afzonderlijke ACCPT- en PROD-omgevingen vervalt.

De eisen in Bijlage 4C zijn mede opgesteld vanuit de mogelijkheid dat de aangeboden GBS-oplossing gebruikmaakt van een SaaS-/webportal. Voor zover de aangeboden GBS-oplossing geen gebruikmaakt van een dergelijke SaaS-/webomgeving, zijn eisen die uitsluitend betrekking hebben op een dergelijke omgeving niet van toepassing.

| Onderdeel | Van toepassing |
|---|---|
| Architectuur | E1 t/m E10 |
| Informatiebeheer | E11, E13, E15, E17, E18, E22, E24 |
| Koppelingen | E27, E28, E29, E30, E32, E34 |
| Zaakgericht werken / archivering | E36 |
| SLA/DAP | E39, E41, E43, E44, E45, E46 |
| Autorisatie | E47, E48, E50, E51 |
| Toegankelijkheid | E52, E53, E56, E57 |
| Authenticatie | E60, E61 |
| Privacy | E62, E63, E64, E65, E66, E68, E69 |
| Compliancy | E70, E71, E72, E73, E74, E76, E78, E80 |
| Logging | E82, E83, E84, E85, E86 |

### Niet van toepassing / vervallen:

Uitsluitend de hierboven onder “Van toepassing” genoemde eisen zijn binnen deze opdracht van toepassing. Alle overige eisen uit Bijlage 4C zijn niet van toepassing en vervallen voor deze opdracht.

Dit betreft: E12, E14, E16, E19, E20, E21, E23, E25, E26, E31, E33, E35, E37, E38, E40, E42, E49, E54, E55, E58, E59, E67, E75, E77, E79 en E81.

## E8 – nadere afbakening

E8 geldt uitsluitend voor zover een SaaS-/webportal onderdeel uitmaakt van de aangeboden GBS-oplossing. E8 houdt geen verplichting in om het volledige gebouwbeheersysteem als native SaaS-/Cloudoplossing uit te voeren.

## E15 – gewijzigde toepassing

De verplichting om de gemeente minimaal twee weken vooraf over relevante functionele wijzigingen te informeren via release notes blijft van toepassing. De verplichting om grotere releases eerst op een afzonderlijke ACCPT-omgeving te testen vóór uitrol op PROD vervalt.

## E17 – nadere afbakening

E17 is van toepassing. Voor zover E17 verwijst naar het kunnen aanpassen van workflows, geldt dit onderdeel uitsluitend indien workflowfunctionaliteit onderdeel uitmaakt van de aangeboden GBS-oplossing.

## E22 – nadere afbakening

E22 geldt uitsluitend voor zover workflowfunctionaliteit onderdeel uitmaakt van of relevant is voor het aangeboden gebouwbeheersysteem.

## E39 – gewijzigde toepassing

De verplichting om releasemomenten minimaal twee weken vooraf vast te stellen en release notes actief aan beheerders beschikbaar te stellen blijft van toepassing. De verplichting om een nieuwe release in een afzonderlijke testomgeving beschikbaar te stellen vervalt.

## E45 – nadere afbakening

De in E45 opgenomen mogelijkheid voor opdrachtgever om wijzigingen te testen blijft van toepassing. Deze bepaling houdt geen verplichting in tot het beschikbaar stellen van een afzonderlijke ACCPT-omgeving.

E27, E28, E29, E30, E32 en E34 gelden uitsluitend voor zover de betreffende functionaliteit of het betreffende koppelvlak relevant is voor het gebouwbeheersysteem en de binnen deze opdracht te realiseren koppelingen.

E47, E48, E50 en E51 gelden voor zover deze relevant zijn voor de gebruikers- en beheerinterface van het aangeboden gebouwbeheersysteem.

# Programma van eisen

# Niet functionele eisen

## PVE ICT

09-03-2026

# Inhoud

## Architectuur en integraties

| Nummer | Omschrijving |
|---|---|
| **E1.** | Een modulaire software opbouw kunnen leveren, zodanig dat functionele componenten logisch gescheiden zijn en afzonderlijk te autoriseren. |
| **E2.** | Voldoen aan de aanbevolen standaarden van Forum standaardisatie: https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen |
| **E3.** | Indien binnen de looptijd van het contract een relevante standaard wordt uitgebracht dient u deze binnen 1 jaar na vaststelling te ondersteunen. |
| **E4.** | Voldoen aan de architectuur-principes van GEMMA: https://www.gemmaonline.nl/wiki/Wat_is_de_basisarchitectuur |
| **E5.** | Een actuele architectuurplaat als onderdeel van het implementatieplan aanleveren waarop de componenten en onderlinge relaties en afhankelijkheden en verantwoordelijkheden die daarbij horen duidelijk zijn beschreven. |
| **E6.** | Output- , export- of gecreëerde bestanden via de user interface van de ICT prestatie benaderbaar kunnen maken. Tevens moet deze output compatible zijn met MS Office 365. |
| **E7.** | De architectuur desgevraagd aantoonbaar logisch kunnen scheiden tussen:<br>• gebruikersschermen, technische interfaces en web services,<br>• proceslogica en informatieverwerking en<br>• gegevensopslag en databases. |
| **E8.** | De ICT prestatie wordt als SaaS aangeboden en is web-based: een native Cloud applicatie. De oplossing moet volledig functioneren in de actuele en voorgaande (n-1) versies van Microsoft Edge, Google Chrome, Mozilla Firefox en Apple Safari. Zonder aanvullende plug-ins en extensies tenzij met vooraf akkoord van opdrachtgever. |
| **E9.** | De ICT prestatie is schaalbaar en kan op- en afschalen op basis van gebruikersbelasting. De ICT prestatie dient minimaal 20 gelijktijdige gebruikers met behoud van performance te kunnen ondersteunen. |
| **E10.** | De ontwikkelagenda (Roadmap) voor de ICT prestatie is beschikbaar en er is inzicht in de geplande ontwikkelingen. |

## Informatiebeheer

| Nummer | Omschrijving |
|---|---|
| **E11.** | Bij een back-up recovery kunnen garanderen dat geen gegevens terug in productie worden gezet die formeel al vernietigd zijn (al dan niet via het opnieuw inzetten/opstarten van de vernietigingsprocedure). |
| **E12.** | Een acceptatie-omgeving (ACCPT) beschikbaar stellen gedurende de project en gebruiksfase waar beheerders van de gemeente beheertaken kunnen uitvoeren en opleidingen kunnen verzorgen. |
| **E13.** | Onderbreking van beschikbaarheid en onderhoud vindt alleen plaats op vooraf overeengekomen dagen en tijdstippen én zoveel mogelijk buiten werktijd. De werkafspraken hierover leggen we vast in de SLA. |
| **E14.** | De acceptatie- en productieomgeving periodiek (semi)geautomatiseerd synchroniseren, tenminste twee maal per jaar. Waarbij rekening wordt gehouden met de eis rondom de privacy van gegevens onder E70. |
| **E15.** | Bij elke functionele wijziging van de ICT prestatie de gemeente vooraf -met voldoende tijd voor impactverwerking(minimaal 2 weken)- informeren via release notes. Grotere releases worden eerst op ACCPT getest voor uitrol op PROD |

| | |
|---|---|
| **E16.** | Mogelijkheid bieden om minimaal de inrichtingsdata in de acceptatieomgeving op aanvraag te synchroniseren met de productieomgeving. |
| **E17.** | Voor functioneel beheer:<br>- is geen programmeerkennis nodig:<br>- moet de functioneel beheerder zelf de autorisaties en stamtabellen kunnen inrichten en beheren.<br>- kan snel en flexibel inspelen op wijzigingen in processen en kan die workflows aanpassen. |
| **E18.** | Beheertaken kunnen uitvoeren terwijl gebruikers zijn ingelogd zonder dat dit consequenties heeft voor deze gebruikers of voor de performance van de ICT prestatie. |
| **E19.** | De oplossing kan voldoen aan de gemeentelijke huisstijl (logo, kleur en lettertype) door middel van configuratie. |
| **E20.** | De ICT prestatie biedt de mogelijkheid om documenten (sjablonen) op te maken volgens de huisstijl van de gemeente Lansingerland. Dit kan in de applicatie zelf of via integratie met c, de standaard voor tekstproductie van de gemeente Lansingerland. Deze integratie dient gestandaardiseerd te zijn. |
| **E21.** | Mogelijkheid bieden om zelf documentsjablonen te ontwikkelen met gebruik van voor ingevulde velden (prefill), opgehaald vanuit de casus of persoon. Voor de prefill zijn relevante in de ICT prestatie geregistreerde gegevens beschikbaar. |
| **E22.** | Mogelijkheid bieden om workflows flexibel in te richten en te configureren, waarbij termijnen tussen bepaalde stappen in te bouwen zijn in de workflow. |
| **E23.** | De oplossing moet het mogelijk maken om de werkvoorraad van gebruikers zowel individueel als in bulk te herverdelen, waarbij alle bijbehorende dossieronderdelen automatisch meeverhuizen. |
| **E24.** | Onderscheid kunnen maken tussen actieve en historische data. Dit om vervuiling van data in de ICT prestatie tegen te gaan. |
| **E25.** | Een geautomatiseerd administratief proces in kunnen richten voor het afhandelen van de standaard taken. |
| **E26.** | Consistentiecontrole uit kunnen voeren op de persoonsgegevens. Het gaat hierbij om een confrontatie tussen de persoonsgegevens in de ICT prestatie en de actuele persoonsgegevens in de BRP. In ieder geval bij het ophalen van lopende zaken, opstellen correspondentie en afsluiten en heropenen van zaken. Daarnaast indien er een wijziging aan de kant van de BRP plaatsvind zoals verhuizing buiten Lansingerland. |

## Koppelingen

| Nummer | Omschrijving |
|---|---|
| **E27.** | Gegevensuitwisseling kunnen ondersteunen via api's of standaard koppelvlakken (StUF) met andere systemen. De api's kunnen standaardiseren. Gestandaardiseerde gegevensmodellen kunnen gebruiken waar deze beschikbaar zijn. |
| **E28.** | De ICT prestatie voldoet aantoonbaar aan de volgende ICT-richtlijnen voor Koppelvlakken:<br>1. Het koppelvlak volledig kunnen ontkoppelen en onafhankelijk van elkaar kunnen laten functioneren;<br>2. Het koppelvlak volledig stateless kunnen maken ten opzichte van de ICT prestatie;<br>3. Het gekozen protocol dat via het koppelvlak loopt duidelijk kunnen vastleggen en |

| | |
|---|---|
| | volledig kunnen ondersteunen;<br>5. Het koppelvlak kunnen testen van en naar de ICT prestatie. |
| **E29.** | De inkomende en uitgaande data via koppelingen kunnen controleren op malafide code/Virussen/Trojans/Spam.<br>Het doel is dat alle data en documenten virusvrij zijn als ze worden aangeboden. Dus niet alleen bij de endpoint van de gebruiker scannen maar ook bij binnenkomst in de applicatie scannen. Alle bestanden dienen gescand te worden. Daarnaast kan via de GUI bepaalde bestandtypes worden toestaan/uitgesloten. |
| **E30.** | De leverancier zorgt voor de implementatie (technisch en functioneel) van koppelingen met andere (SaaS)applicaties als verantwoordelijke voor de integratie van de eigen applicatie. Van de leverancier wordt medewerking verwacht in projecten voor koppelingen onder leiding van een derde partij. De gemeente Lansingerland stelt daarbij de informatiebeveiligingskaders vast. Het gaat hier om bestaande en in de toekomst nog aan te leggen koppelingen met andere (SaaS) leveranciers. |
| **E31.** | Maximale data ontsluiting kunnen bieden; geregistreerde functionele data is via api's of ETL te ontsluiten. Gemeente Lansingerland heeft de mogelijkheid aan te geven welke gegevens ontsloten moeten worden. |
| **E32.** | De communicatie met de infrastructuur van gemeente Lansingerland kunnen beperken tot de daarvoor bestemde koppelvlakken. |
| **E33.** | Is er nog een voorkeur voor de routing en verwerking van bijv. API of stuff? Denk aan inzetten van een API-gateway? Verschil tussen intern-extern versus extern-extern? |
| **E34.** | Printen dient veilig te gebeuren. Printen via het IPPS-protocol is de eis indien de printopdracht vanuit uw omgeving wordt geïnitieerd. Bij inzet van andere oplossingen dient de vergelijkbare veiligheid aangetoond te worden. |

## Zaakgericht werken en geautomatiseerde rechtmatige archivering

| Nummer | Omschrijving |
|---|---|
| **E35.** | Het is mogelijk om de ICT prestatie te koppelen met het zaaksysteem/DMS (Dimpact) van de gemeente middels StUF-ZKN of de zaak-DMS API. De Gemma standaard Regie- en Zaakservices en de Gemma standaard Zaak- en document Service kunnen worden gebruikt door de ICT prestatie. |
| **E36.** | Informatieobjecten en bijbehorende metadata onherstelbaar kunnen vernietigen, conform de bepalingen hierover in archiefwet. Vernietigen van informatie is het blijvend ontoegankelijk maken van die informatie, waardoor deze niet meer vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar is. Digitaal vernietigen betreft digitale overheidsinformatie, ongeacht de vorm en met behoud van metagegevens over de vernietiging. |
| **E37.** | Een rapportage van vernietiging kunnen opstellen (bewijs van vernietiging). |
| **E38.** | Aan elke zaak en document een uniek en persistent identificatiekenmerk kunnen toekennen:<br>Bij voorkeur/ uitgangspunt is automatisch gegenereerd op basis van een identificatiesysteem, waarbij gebruikers geen unieke kenmerken handmatig kunnen toevoegen en muteren. |

## SLA/DAP

| Nummer | Omschrijving |
|---|---|

| | |
|---|---|
| **E39.** | De releasemomenten worden minimaal 2 weken van tevoren vastgesteld. Hierbij worden ook de release notes vrijgegeven, actief bekend gemaakt aan beheerders en daarbij komt de nieuwe release beschikbaar voor gebruikers in een testomgeving. |
| **E40.** | Er vindt minimaal 2x per jaar periodiek overleg plaats met de Opdrachtnemer op strategisch, tactisch en operationeel niveau. Er vindt tenminste ieder kwartaal overleg plaats met de leverancier t.a.v. aangemelde meldingen en wijzigingsverzoeken. |
| **E41.** | De functionele beschikbaarheid van de productie omgeving wordt van maandag tot vrijdag tussen 09:00 en 17:00 voor minimaal 98,5% per maand gegarandeerd. Voor de overige uren van de werkweek en het weekend wordt voor de productie omgeving de beschikbaarheid voor minimaal 98,5% per maand gegarandeerd met uitzondering van aangekondigd onderhoud. De Inschrijver levert 1 keer per kwartaal een rapportage aan van de gerealiseerde beschikbaarheid zowel technisch als functioneel. |
| **E42.** | De beschikbaarheid op werkdagen voor de ACCPT omgeving wordt voor minimaal 95% per maand gegarandeerd. Voor de overige uren van de werkweek en het weekend wordt voor de test/acceptatie omgeving de beschikbaarheid voor minimaal 90% per maand gegarandeerd met uitzondering van aangekondigd onderhoud. De Inschrijver levert 1 keer per kwartaal een rapportage aan van de gerealiseerde beschikbaarheid zowel technisch als functioneel. |
| **E43.** | De inschrijver moet voor het beheer en gebruik, relevante en actuele beschikbare documentatie over de functionele en eventueel technische werking van de actuele ICT prestatie beschikbaar stellen aan de functioneel beheerders van de gemeenten, zodat deze aansluit bij de laatste en dus gebruikte release. |
| **E44.** | De opdrachtnemer levert tenminste eenmaal per kwartaal een gedetailleerde en digitale rapportage in de vorm van een spreadsheet (formaat: Microsoft Excel), waarbij tenminste wordt vermeld:<br>- aantal storingen gegroepeerd naar afgesproken afhandeltermijn;<br>- gemiddelde hersteltijd (tijd waarbinnen de storing is opgelost).<br>Een Dashboard mag als alternatief hiervoor dienen. |
| **E45.** | Aanpassingen in de genoemde standaarden worden door de leverancier verwerkt binnen 6 maanden na publicatie of eerder indien dat wettelijk is vereist waarbij opdrachtgever (minimaal) 6 weken tijd heeft om te testen. De vorige versie wordt nog minimaal 12 maanden ondersteund |
| **E46.** | Response en behandeltijden rondom helpdesk en ondersteuning zijn marktconform. |

## Autorisatie

| Nummer | Omschrijving |
|---|---|
| **E47.** | Via een autorisatiematrix de rechten kunnen vastleggen. Deze rechten worden aangegeven en beheerd door een beheerder bij de opdrachtgever (nader te bepalen op basis van rol, functie, active directory). Regulier worden rechten via IAM toegekend; het gaat hier om het geval dat dit niet mogelijk is. |
| **E48.** | Autorisaties kunnen door een beheerinterface worden geconfigureerd. Het hele rollen- en rechtenmodel van de ICT-prestatie kan op één plek geconfigureerd worden. Het is mogelijk om configuraties in rollen en rechten te stapelen, in groepen toe te kennen, te overerven, te kopiëren en te delegeren. |

| | |
|---|---|
| **E49.** | Elke Zaak, inclusief de daaraan gekoppelde deelzaken, toegankelijk kunnen maken voor de behandelaar en bij de Klant betrokken Professionals (o.b.v. autorisatie). Het gaat hier om het overnemen van autorisaties. |
| **E50.** | Mogelijkheid bieden om autorisaties aan te maken, muteren en verwijderen door een beheerder van de gemeente Lansingerland. |
| **E51.** | Mogelijkheid bieden om gebruikersgroepen met specifieke rechten aan te maken door een beheerder van de gemeente Lansingerland. |

## Toegankelijkheid

| Nummer | Omschrijving |
|---|---|
| **E52.** | Het opstartproces voor de professional van de ICT-oplossing (inclusief inloggen) binnen 10 seconden verwezenlijken.<br>Voor rapportagefuncties en documentproductie de opstarttijd binnen 60 seconden verwezenlijken.<br>Voor alle overige schermen en functies geldt dat deze maximaal 5 seconden na muisklik op het scherm getoond zijn.<br>Gevraagde performance is exclusief de systeemperformance gemeente Lansingerland. |
| **E53.** | De aangeboden functionaliteiten beschikbaar stellen voor (eind)gebruikers via mobiele apparaten (pc, laptop, tablet en mogelijk e-diensten op de smartphone). |
| **E54.** | Een gedetailleerde zoekfunctie kunnen aanbieden op documenten en alle ingevoerde en automatisch gegenereerde metadata en combinaties hiervan. |
| **E55.** | Via de zoekfunctie de gevonden resultaten op basis van de autorisatie van de gebruiker op de gegevens en documenten kunnen presenteren. |
| **E56.** | Voor de user interface voor externe dienstverlening voldoen aan de eisen uit de Web Content Accessibility Guidelines (WCAG) toegankelijkheidsnorm: WCAG , niveau A + AA. |
| **E57.** | Handleidingen voor beheerders zijn bij oplevering van de ICT prestatie beschikbaar. |

## Authenticatie

| Nummer | Omschrijving |
|---|---|
| **E58.** | Authenticatie van rechtspersonen via de DigiD van de Toegangsmakelaar van gemeente Lansingerland kunnen laten verlopen. |
| **E59.** | Authenticatie van bedrijven via e-Herkenning van de Toegangsmakelaar van gemeente Lansingerland kunnen laten verlopen. |
| **E60.** | Verplichtbare twee-factor authenticatie (sms, smartphone, token, etc.) kunnen toepassen binnen én buiten de digitale werkplek van Lansingerland. En flexibel kunnen aanpassen aan nieuwe inzichten met betrekking tot Identity & Access Management. |
| **E61.** | Gebruik kunnen maken van Single of Same Sign On (SSO) op basis van het SAML2 protocol of het OAUTH2 protocol. De medewerker authentiseert zich hiermee conform de Identity & Access Management (IAM) oplossing van Opdrachtgever. De externe ketenpartner kan hiermee inloggen met de Lansingerlandse netwerk inlognaam en wachtwoord en token. |

## Privacy

| Nummer | Omschrijving |
|---|---|
| **E62.** | De naleving van geldende landelijke en Europese wet- en regelgeving over gegevensbescherming, informatiebeveiliging en informatiebeheer kunnen garanderen, onder meer de AVG, UAVG, WOO en de Archiefwet. De oplossing voldoet daarmee tevens aan de wetten waarop de Autoriteit Persoonsgegevens toezicht houdt (te weten de BRP, WPG, WJSG, Kieswet, AVG, UAVG), wanneer van toepassing. |
| **E63.** | Relevante wetswijzigingen kunnen opvolgen. Deze wijzigingen op functioneel, beveiligings- en/of technisch niveau per ingangsdatum kunnen activeren. |
| **E64.** | De conform VNG standaard Verwerkersovereenkomst die de opdrachtgever gaat voorleggen zal aanvullen en tekenen. Deze is bijgevoegd als bijlage bij de publicatie van deze aanbesteding. |
| **E65.** | De ICT prestatie ondersteunt opdrachtgever bij het voldoen aan algemene verplichtingen op het terrein van gegevensbescherming, onder meer door:<br>• Waarborgen voor de juistheid en kwaliteit (integriteit) van persoonsgegevens (toetsing aan authentieke brongegevens, afdwingbaarheid via invoer- en importmechanismes).<br>• Waarborgen in het kader van bewaar- en vernietigingstermijnen.<br>• Mogelijkheden voor tenuitvoerlegging van de verantwoordingsplicht. |
| **E66.** | Documentatie kunnen leveren die de door de leverancier genomen privacy maatregelen op een heldere manier beschrijft. Deze documentatie ook kunnen leveren als onderdeel van de verwerkersovereenkomst. |
| **E67.** | De ACCPT werkt geïsoleerd. Deze is niet gekoppeld aan de productieomgeving en werkt niet met productiedata maar werkt met geanonimiseerde gegevens. De ACCPT is een realistische afspiegeling van de productieomgeving, zonder daarbij inbreuk te maken op privacyregels. Bij synchronisatie wordt bij het 'meekopiëren' van relevante gegevens automatisch scrambling- of anonimiseringsregels toegepast. Hierdoor wordt zowel consistentie als compliance bereikt. |
| **E68.** | De oplossing wordt na een instelbaar aantal minuten ongebruikt te zijn automatisch vergrendeld, wat alleen door het invoeren van een wachtwoord opgeheven kan worden. Bewerkingen worden opgeslagen. Hiermee wordt bedoeld dat openstaand werk wel bewaard wordt en via een hersteloptie wordt aangeboden. |
| **E69.** | Gebruikersaccounts worden geblokkeerd na een instelbaar aantal achtereenvolgende foutieve authenticatiepogingen binnen een instelbare periode |

## Compliancy

| Nummer | Omschrijving |
|---|---|
| **E70.** | Voldoet aan Baseline Informatiebeveiliging Overheid (BIO)door middel van een ISO 27 001/2 certificering |
| **E71.** | Kan voldoen aan de eisen vanuit de NIS2/Cyberbeveiligingswet medio 2026 en beschrijft in het implementatieplan hoe hier aan voldaan gaat worden. |
| **E72.** | De leverancier voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties. |
| **E73.** | De ICT prestatie voldoet aan de meest actuele OWASP richtlijnen. |
| **E74.** | Bij nieuwe releases van de ICT-Prestatie bestaande gegevens onder beheer van toegankelijk kunnen laten blijven zonder verandering van inhoud en structuur of verlies van functionaliteit. |

| | |
|---|---|
| **E75.** | Er is functionaliteit aanwezig om informatieobjecten definitief te kunnen maken (niet meer wijzigbaar) en na het definitief maken van een informatieobject een waarschuwing geven dat wijzigen niet kan . Het moet minimaal mogelijk zijn om afgesloten zaak te kunnen bevriezen. |
| **E76.** | Manipulatie kunnen beperken door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt. |
| **E77.** | Binnen de productieomgeving beheer- en productieverkeer van elkaar kunnen afschermen. |
| **E78.** | Jaarlijks en op eerste verzoek een verklaring van een onafhankelijke derde, RSO (voorheen TPM) kunnen tonen waaruit blijkt dat de informatiebeveiliging van de organisatie conform de eisen van de opdrachtgever is. Dit ten bate van de Ensia (bijvoorbeeld Suwinet en DigiD) en WPG audits op basis van het normenkader van NOREA. |
| **E79.** | Data kunnen opslaan op minimaal twee fysiek gescheiden locaties. Volledig redundante data opslag infrastructuur. |
| **E80.** | Bij systeemkoppelingen (in- en uitgaand) wederzijds systeemauthenticatie laten plaatsvinden door middel van basic toegang authenticatie in combinatie met HTTPS of PKI (PKI) certificaten afgedwongen door de dataclassificatie. Wildcards certificaten zijn niet toegestaan. SAN certificaten zijn alleen binnen een omgeving toegestaan. |
| **E81.** | De oplossing ondersteunt alle middelen die binnen het WDO stelsel vallen zodra de WDO in werking treedt. |

## Logging

| Nummer | Omschrijving |
|---|---|
| **E82.** | In het systeem worden door technische logging gebeurtenissen opgenomen zoals het gebruik van technische- en functionele beheerfuncties, handelingen van beveiligingsbeheer, verstoringen in het productieproces en beveiligingsincidenten. Het doel van de controle van systeemgebruik is vaststellen of het informatiesysteem correct wordt gebruikt, goed wordt beheerd en functioneert conform de gestelde eisen. |
| **E83.** | Het systeem dient een volledige en niet-wijzigbare audit trail bij te houden van alle mutaties op gegevens, inclusief wie (gebruiker of systeem), wat (veld en oude/nieuwe waarde), wanneer (datum/tijd) en hoe (interface, handmatig, batch) de wijziging heeft plaatsgevonden.<br>Hierbij gelden de volgende specificaties:<br>• Logging moet real-time of near real-time plaatsvinden.<br>• Alleen bevoegde personen mogen de logs inzien (rol gebaseerde toegang).<br>• Logging dient ook plaats te vinden bij wijzigingen via API's of systeemkoppelingen. |
| **E84.** | Logging vanuit security en privacy (SIEM/SOC)<br>• De leverancier dient te beschikken over een operationele Security Operations Center (SOC) functie met ten minste 24/7 monitoringcapaciteit. De SOC moet in staat zijn om bij geconstateerde afwijkingen op basis van logging en monitoring onmiddellijk incident response in gang te zetten, conform een vastgestelde procedure (bijv. volgens NIS2 of ISO 27035).<br>• Beveiligingsincidenten moeten binnen 24 uur bij de gemeente gemeld worden (eis vanuit NIS2) |
| **E85.** | Bewaartermijnen, analyse en ontsluiting van logs |

| | |
|---|---|
| | • Logging dient minimaal een half jaar beschikbaar te zijn voor onderzoek. In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Bewaartermijnen van een log zijn beschreven in het BIO-OP product "Handreiking Dataclassificatie van de VNG"<br>• Logs moeten doorzoekbaar en exporteerbaar zijn (voor audits of onderzoeken).<br>• Verwijzen naar het loggingbeleid van de gemeente |
| **E86.** | De ingestelde logging dient de performance van de systemen niet in grote mate op een negatieve wijze te beïnvloeden. |