

Beveiliging van In Zicht

Infraprojecten raken kritieke infrastructuur. Daarom leggen wij hier open vast hoe wij uw data beschermen — zodat uw security-officer het kan toetsen.

Versie 1.1 — nog vast te stellen · Opgemaakt op 2026-10-29 · <https://hetinfraloket.nl/beveiliging>

Versie en contractuele status

Deze beveiligingsbijlage is een contractstuk. In artikel 7 van de [modelovereenkomst In Zicht](#) en in de [verwerkersovereenkomst](#) wordt naar de hieronder vermelde versie verwezen. Bij een contract geldt uitsluitend de versie die op het overeenkomstblad is aangekruist en gedateerd; latere versies gelden pas na schriftelijke bevestiging aan opdrachtgever.

De beveiligingsverplichtingen in deze bijlage rusten op Het infraloket (SaaS) B.V., in dit document verkort aangeduid als Het **infraloket**, als leverancier van In Zicht en de hosting. Waar deze bijlage “wij” of “ons” noemt, wordt deze vennootschap bedoeld.

Aanvaarding van deze bijlage verloopt via de modelovereenkomst In Zicht: op het overeenkomstblad bevestigt opdrachtgever dat deze beveiligingsbijlage is verstrekt, dat daarvan kennis kon worden genomen en dat zij wordt aanvaard. Een aparte handtekening onder deze bijlage is in de standaardflow niet nodig.

- Versienummer: **Versienummer** (bijv. 1.1)
- Vastgesteld op: **Vaststellingsdatum** (dd-mm-jjjj)
- Vervangt versie: **Vorige versie** (of: n.v.t.)
- Wijzigingen worden bijgehouden in het versieoverzicht: **Korte omschrijving laatste wijziging** (bijv. hostingpartij toegevoegd)

Hosting en datalocatie

- Hostingpartij: Scaleway.
- Productieserver: Amsterdam, Nederland.
- Back-up- en overige opslaglocaties: **Locatie(s) back-up en opslag** (te verifiëren)
- Locatie van overige datastromen (support, e-mail, AI-verwerking): **Locaties overige verwerkingen** (te verifiëren)
- Onafhankelijk van niet-Europese hyperscalers — uw data valt onder Nederlands en Europees recht.

Certificeringen en normen

- Eigen certificering: **ISO 27001 / NEN 7510 / geen** (alleen vermelden met certificaatnummer)
- Certificering hostingpartij: **Certificaten leverancier** . De vermelding “ISO 27001-infrastructuur” in de footer verwijst uitsluitend naar de certificering van onze hostingpartij, niet naar een eigen certificaat.
- Certificering AI-leverancier: **Naam en certificaat AI-leverancier** (alleen ISO 27001 of gelijkwaardig)
- Referentiekader: wij richten ons beveiligingsbeleid in langs de Baseline Informatiebeveiliging Overheid (BIO), omdat veel van onze opdrachtgevers daaraan gebonden zijn.

AI-functionnalité

De AI-module is optioneel. Neemt u die niet af, dan vindt geen enkele AI-verwerking van uw gegevens plaats. Neemt u die wel af, dan gelden de volgende uitgangspunten — dezelfde als in de [algemene voorwaarden](#) en de [verwerkersovereenkomst](#).

- Verwerking uitsluitend binnen de Europese Economische Ruimte.
- Invoer en output worden niet gebruikt voor het trainen of verbeteren van modellen.
- Uitsluitend ISO 27001-gecertificeerde AI-leveranciers, of leveranciers die een gelijkwaardige norm aantoonbaar naleven.
- Geen langdurige opslag bij de AI-leverancier; het resultaat komt in uw eigen projectomgeving te staan.
- Afrekening op verbruik, met waar overeengekomen een absoluut AI-kostenplafond om onverwachte kosten te begrenzen. Dat plafond staat los van het inbegrepen AI-volume en geldt alleen indien het afzonderlijk is overeengekomen.
- AI-output is ondersteunend en niet leidend — beoordeling en besluit blijven bij u.

Versleuteling

- In transit: al het verkeer verloopt over TLS **TLS-versie** (bv. 1.3)
- At rest: opslag versleuteld met **Encryptiestandaard** (bv. AES-256)
- Sleutelbeheer: **Wie beheert de sleutels en hoe**

Toegangsbeheer

- Rolgebaseerde autorisatie in In Zicht: gebruikers zien alleen de projecten en documenten die bij hun rol horen.
- Tweefactorauthenticatie: **Beschikbaar (optioneel)** (voor gebruikers en voor beheerders)
- Toegang door onze medewerkers gebeurt volgens het minste-rechten-principe en wordt vastgelegd in een auditlog.
- Single sign-on: **SSO ondersteund?** (bv. Entra ID, SAML)

Back-up en herstel

- Back-upfrequentie: één automatische back-up per werkdag (vijf per week), één aanvullende wekelijkse back-up en de mogelijkheid om direct handmatig een back-up te starten.
- Bewaartermijn back-ups: **Retentie** (bv. 30 dagen)
- Hersteltijd bij calamiteit: **RTO en RPO**
- Herstelprocedures worden periodiek getest — frequentie: **Testfrequentie** (bv. jaarlijks)
- U kunt daarnaast een eigen back-up laten wegschrijven naar uw eigen cloud of server, zodat u nooit afhankelijk bent van één partij.

Logging en monitoring

- Handelingen in het platform worden vastgelegd in een auditlog, zodat achteraf herleidbaar is wie wat wanneer heeft gedaan.
- Bewaartermijn logs: **Termijn** (bv. 12 maanden)
- Monitoring op beschikbaarheid en afwijkend gedrag: **Hoe en waarmee**

Veilige ontwikkeling

- Wijzigingen doorlopen code review en worden getest in een gescheiden omgeving voordat ze naar productie gaan.
- Ontwikkel-, test- en productieomgevingen zijn van elkaar gescheiden; in test wordt niet met echte klantdata gewerkt.
- Penetratietests: **Frequentie en uitvoerende partij** (of 'nog niet uitgevoerd')

Incidenten

Bij een beveiligingsincident schalen wij direct op, beperken wij de impact en informeren wij getroffen klanten. Betreft het een inbreuk in verband met persoonsgegevens, dan melden wij dat binnen de termijn uit de [verwerkersovereenkomst](#).

Contactpersoon beveiliging bij Het **infraloket**: **Naam en e-mailadres**

Kwetsbaarheid melden

Ontdekt u een kwetsbaarheid? Meld het bij ons via het formulier hieronder of direct per e-mail aan **E-mailadres responsible disclosure** (bv. security@hetinfraloket.nl) . Wij reageren binnen vijf werkdagen, houden u op de hoogte van de afhandeling en ondernemen geen juridische stappen tegen melders die zorgvuldig te werk gaan en de kwetsbaarheid niet misbruiken of openbaar maken voordat die is verholpen.

Laat dit veld leeg



Openstaande taken

Verzendafhandeling wordt lokaal ingeregeld — het formulier verstuurt nu nog niets.

- Eigen afzenderdomein instellen (bijv. notify.hetinfraloket.nl) zodat bevestigingsmails betrouwbaar aankomen
- Ontvangstadres voor meldingen instellen (bijv. security@hetinfraloket.nl)
- Automatische ontvangstbevestiging naar de melder, inclusief responsible-disclosure-afpraak en reactietermijn
- Interne afhandelprocedure en reactietermijn vastleggen
- Opslag van meldingen afstemmen op verwerkersovereenkomst

Naam

E-mailadres *

Type melding *

Geschatte ernst

Beschrijf wat u heeft gevonden, hoe het te reproduceren is, en eventuele URLs.

Beschrijving *

Geen bijlagen: dit formulier accepteert bewust geen bestandsuploads. Bewijsmateriaal, zoals schermafbeeldingen of logbestanden, deelt u uitsluitend via het platform nadat wij contact met u hebben opgenomen.

Mogelijke impact

☐ Ik ga zorgvuldig te werk, heb de kwetsbaarheid niet misbruikt of openbaar gemaakt, en geef u de tijd om deze te verhelpen.

Uw melding wordt vertrouwelijk behandeld. We ondernemen geen juridische stappen tegen melders die zich aan deze afspraak houden.