AXIOMATIC

ICT-dossier

Inora, voor de CISO en de ICT-manager

Versie 1.13, 11 november 2026

1. Wat dit dossier regelt

U bent CISO of ICT-manager van een zorgorganisatie, en een collega wil met Inora beginnen. Uw vraag: kost dit mijn team werk? Dit dossier beantwoordt die vraag zo volledig dat u in één gesprek ja kunt zeggen, en het is zo opgezet dat u het in uw eigen archief legt.

Inora is het kennissysteem van de organisatie: zorgmedewerkers krijgen antwoord uit de eigen protocollen en werkafspraken. Axiomatic bouwt Inora, voert het zelf in en beheert het. Inora is ingericht volgens NEN 7510 en ISO 27001.

In het kort:

- **Uw team doet niets om te starten.** Eén toestemming in uw identiteitsbeheer. Verder niets. Medewerkers loggen in met single sign-on; er is niets te installeren.
- **Uw gegevens verlaten de EU nooit.** Eén eigen omgeving per organisatie bij Amazon Web Services in Ierland, het taalmodel in EU-regio's, of alles op uw eigen servers.
- **Alleen de engineers die Inora bouwen, kunnen bij productie:** elk bij naam in de verwerkersovereenkomst. Persoonlijke accounts met MFA, elke toegang vastgelegd.
- **Elke maatregel staat op papier**, in de controlematrix in hoofdstuk 5.
- **Wat de Cyberbeveiligingswet van uw bestuur vraagt, ligt klaar**, per plicht met het document.

2. Waarom u gelijk hebt om het te vragen

- **Besluit elektronische gegevensverwerking door zorgaanbieders, artikel 3, lid 2.** De zorgaanbieder zorgt volgens NEN 7510 en NEN 7512 voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem. Bron: wetten.overheid.nl, BWBR0040238.
- **Inspectie Gezondheidszorg en Jeugd.** Wie zijn ICT uitbesteedt, blijft als zorgaanbieder zelf verantwoordelijk voor de informatiebeveiliging. Bron: igj.nl, Vragen over NEN 7510.

- **Cyberbeveiligingswet, sinds 15 augustus 2026.** Artikel 21, lid 3, onder d noemt de beveiliging van de toeleveringsketen als deel van de zorgplicht; artikel 24 legt de goedkeuring van de maatregelen en de kennis om ze te beoordelen bij het bestuur; artikel 26 vraagt een vroegtijdige waarschuwing binnen 24 uur. Bron: wetten.overheid.nl, BWBR0052872.

Een leverancier van AI is dus een risico dat u draagt. Dit dossier laat zien hoe klein Inora dat risico maakt, en waar het op papier staat.

3. Dag één: 0 uur ICT-werk, met single sign-on

Onderdeel	Wat uw team doet	Uren
Accounts	Niets. Medewerkers loggen in via uw eigen identiteitsbeheer, met SAML 2.0 of OpenID Connect; SCIM houdt de accounts bij. Met single sign-on bewaart Inora geen wachtwoorden; MFA en wachtwoordregels stelt u zelf in.	0
Netwerk	Niets te doen: geen VPN, geen firewallregel. De pilot vraagt geen koppeling; koppelingen komen daarna, en uw ICT zet ze aan. Dan geldt: Inora maakt de rapportage klaar; de zorgmedewerker leest en tekent, en pas op dat akkoord zet Inora haar in het dossier; Inora werkt namens die persoon, nooit met meer rechten dan die zelf heeft.	0
Installatie	Niets. Inora is een dienst in de browser en de app. Updates doen wij. Nieuwe functies melden wij een week vooraf, met de uitkomst van de toets; met uw schriftelijke opdracht, na instemming van de ondernemingsraad waar u er een heeft, toetsen wij ook op de vragen van uw eigen teams. Beveiliging-supdates gaan zonder week vooraf door, kritieke binnen 72 uur, na dezelfde toets; die melden wij achteraf.	0

De beheerder geeft Inora eenmalig toestemming in uw identiteitsbeheer en kiest welke groepen toegang krijgen; daarna houdt SCIM de accounts bij. Bij Entra ID, de meest gebruikte, geeft de toestemming in Entra ID geeft Inora alleen `openid`, `profile`, `email` en `User.Read`, gedelegeerd en alleen-lezen; uw groepen komen als claim in het inlogbewijs. Inora leest alleen de groepen die u aan de app toewijst, zodat de claim nooit overloopt. Geen toegang tot mail, bestanden, Teams of SharePoint.

Uw bronnen blijven in uw eigen documentsysteem staan; Inora werkt met een kopie die uw handboekbeheerder aanlevert en bijwerkt. U bepaalt daarna zelf welke groepen medewerkers toegang krijgen en wie documenten en instellingen beheert.

4. Waar het draait en wie erbij kan

4.1 Hosting en locatie

Onderdeel	Leverancier	Locatie
Toepassing, database, document-opslag, zoekindex	Amazon Web Services EMEA SARL, Luxemburg	Regio Europa (Ierland), eu-west-1
Back-ups	Amazon Web Services EMEA SARL	Regio Europa (Ierland), eu-west-1; verspreid over meerdere beschikbaarheidszones
Taalmodel en embeddingmodel	Amazon Bedrock, via het EU-inferentieprofiel	AWS-regio's in de EU

Op uw keuze draait Inora op uw eigen servers, binnen uw eigen netwerk; uw verwerkersovereenkomst noemt dan elke leverancier van die inrichting.

4.2 Het taalmodel

Het systeem kiest per taak een taalmodel dat in de EU draait: bij Amazon Web Services of bij Microsoft Azure in de EU-regio, met de aangepaste misbruikmonitoring van Microsoft. Beide staan op de lijst van subverwerkers. Op uw eigen servers draait het taalmodel binnen uw netwerk.

Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, in de EU. Geen mens leest mee, en het model bewaart niets. De indeling blijft in de omgeving en verdwijnt met het gesprek.

Geen model traint op uw gegevens: niet bij Axiomatic, niet bij de leverancier van het model. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model. Azure OpenAI draait Axiomatic met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring). Elk model, en elke wijziging in Inora, wordt getoetst voordat uw medewerkers ermee werken; met uw schriftelijke opdracht ook op uw eigen vragen.

4.3 Eén omgeving per organisatie

Elke organisatie heeft een eigen omgeving: een eigen database, eigen documentopslag en een eigen zoekindex. Een vraag die binnen de ene organisatie wordt gesteld, kan alleen de documenten van die organisatie bereiken. De scheiding zit in de infrastructuur, niet alleen in de software.

4.4 Wie bij productie kan

- Alleen de engineers die Inora bouwen en beheren, elk bij naam in de verwerkersovereenkomst (bijlage 2). De adviseurs van Axiomatic, en ieder ander bij Axiomatic, hebben geen toegang tot de productieomgeving en niet tot gegevens van organisaties.

- Alleen persoonlijke accounts, met multifactorauthenticatie. Geen gedeelde accounts.
- Elke toegang tot de omgeving van een organisatie wordt vastgelegd (4.7).
- Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend, en iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).
- Werklaptops hebben volledige schijfversleuteling en automatische beveiligingsupdates. Vertrekt iemand, dan vervalt de toegang dezelfde dag.

4.5 Inloggen en sessies

Inloggen loopt standaard via de single sign-on van uw eigen identiteitsbeheer, met elke identiteitsprovider: Entra ID, Okta, Google of elke andere via SAML of OpenID Connect. De beheerder stelt dit zelf in één stap in; SCIM maakt accounts aan en sluit ze af. Schakelt u daar een account uit, dan kan die persoon niet meer inloggen; een open sessie eindigt uiterlijk acht uur nadat zij begon.

Met single sign-on bewaart Inora geen wachtwoorden. Die accounts schakelt uw beheerder in Inora uit.

4.6 Versleuteling

- Tijdens transport: TLS 1.2 of hoger, voor al het verkeer van en naar Inora en tussen de onderdelen.
- Bij opslag: AES-256 voor databases, documentopslag, zoekindexen en back-ups. De sleutels staan in AWS Key Management Service, in de EU; elk gebruik wordt vastgelegd.
- Tijdens het beantwoorden van een vraag zijn de vraag en de passages alleen ontsleuteld zolang het antwoord wordt gemaakt; het model bewaart ze niet.

4.7 Back-ups, logging en updates

- Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland), verspreid over meerdere beschikbaarheidszones; hooguit 24 uur aan gegevens gaat verloren. Elk kwartaal zetten wij een back-up terug als test.
- Een herstel uit back-up duurt ten hoogste 8 uur.
- Beveiligingsupdates voor kritieke kwetsbaarheden binnen 72 uur, andere binnen 30 dagen.

Zonder koppeling leest Inora het dossier in een eigen microVM per gebruiker, met de login en rechten van die persoon: de zorgmedewerker logt zelf in, Inora bewaart geen wachtwoorden en houdt de sessie alleen vast zolang de taak loopt; werk op schema loopt op een sessie die de naamdrager vooraf goedkeurde. Alleen in de systemen die de organisatie aanwijst.

Inora legt inlogmomenten, beheerhandelingen en elke toegang door medewerkers van Axiomatic vast, 12 maanden lang. Zodra Inora het dossier leest, via een koppeling of de eigen login, houdt Inora ook een dossierlogboek bij, ingericht volgens NEN 7513: per stap wat Inora deed en namens wie, in te zien door de functie die de organisatie aanwijst. Op verzoek krijgt een organisatie de beveiligingslogging van haar omgeving, opgeteld per team van minstens vijf mensen en per dag, en elke toegang door Axiomatic; een

dag met minder dan vijf inlogs staat er als ‘<5’. Inlogmomenten en IP-adressen van één medewerker gaan nooit naar de organisatie. Bij een beveiligingsincident onderzoekt Axiomatic het logboek zelf en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen.

4.8 Beschikbaarheid

Ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht. Een storing meldt u aan support@axiomatic.digital, dag en nacht. Bij een storing krijgt de contactpersoon van uw organisatie bericht per e-mail, tot de storing is verholpen.

4.9 Wat de EU nooit verlaat

Uw gegevens, de back-ups en de logging. Voor een organisatie in de EU draait Inora in de EU en verwerkt het taalmodel gegevens alleen binnen de EU.

5. Elke maatregel, en hoe die is ingevuld

De controlematrix: alle beheersmaatregelen uit ISO 27001 en de maatregelen die NEN 7510 voor de zorg toevoegt, elk met hoe Inora die invult en met zijn status. De matrix is de basis voor uw verklaring van toepasselijkheid.

Organisatorisch (37)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.1	Beleidsregels voor informatiebeveiliging	Het beveiligingsbeleid en het beveiligingsoverzicht leggen vast hoe Inora is beveiligd, en beide zijn openbaar. Iedereen bij Axiomatic leest en tekent de beveiligingsregels bij de start en daarna elk jaar opnieuw. De directeur keurt het beleid goed en herziet het elk jaar en na elk ernstig beveiligingsincident.	▪ Ingericht
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	De directeur is verantwoordelijk voor beveiliging en privacy binnen Axiomatic. Het beveiligingsoverzicht noemt wie bij de productieomgeving kan en wie niet.	▪ Ingericht
5.3	Functiescheiding	Geen wijziging gaat in productie zonder beoordeling door een tweede engineer. Wie organisaties bij de implementatie begeleidt, heeft geen toegang tot de productieomgeving of tot hun gegevens.	▪ Ingericht
5.4	Managementverantwoordelijkheden	De directie eist van iedereen dat hij de beveiligingsregels bij de start en elk jaar tekent, en draagt de verantwoordelijkheid voor beveiliging en privacy zelf.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.5	Contact met overheidsinstanties	Bij een datalek helpen wij de organisatie met haar melding bij de Autoriteit Persoonsgegevens. Een overheidsverzoek beantwoorden wij alleen als het Unierecht of Nederlands recht ons verplicht, met niet meer dan nodig en, tenzij de wet het verbiedt, nadat de organisatie het weet.	▪ Ingericht
5.6	Contact met speciale belangengroepen	Wij volgen de beveiligingsadviezen van het NCSC en Z-CERT en de beveiligingsmeldingen van elk bouwblok waarop Inora draait.	▪ Ingericht
5.7	Informatie en analyses over dreigingen	Met de adviezen uit 5.6 beoordelen wij elke maand welke dreigingen Inora raken, en leggen dat vast. Bekende kwetsbaarheden in de bibliotheken worden automatisch gevolgd.	▪ Ingericht
5.8	Informatiebeveiliging in projectmanagement	Elke implementatie en elke nieuwe functie begint met de beveiligingsvragen schriftelijk beantwoord: welke gegevens, wie erbij kan, welke leverancier.	▪ Ingericht
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Een register noemt elk systeem, elke leverancier, elke gegevensopslag en elke laptop, met een eigenaar, en wordt elk kwartaal nagelopen.	▪ Ingericht
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	De beveiligingsregels die iedereen tekent, zeggen hoe informatie en laptops gebruikt mogen worden. Gegevens van organisaties staan nooit op een laptop.	▪ Ingericht
5.11	Retourneren van bedrijfsmiddelen	Vertrekt iemand, dan komt de laptop op de laatste werkdag terug en wordt hij gewist. De toegang vervalt dezelfde dag.	▪ Ingericht
5.12	Classificeren van informatie	Alles wat gebruikers in Inora typen, geldt als gezondheidsgegeven en wordt zo beschermd. De documenten van de organisatie gelden als intern.	▪ Ingericht
5.13	Labelen van informatie	Elke omgeving, opslag en zoekindex draagt in de infrastructuur het label van haar organisatie en haar gegevensklasse.	▪ Ingericht
5.14	Overdragen van informatie	Al het verkeer van en naar Inora, en tussen de onderdelen ervan, is versleuteld met TLS 1.2 of hoger. Wat wij met gegevens doen en met wie, staat in de verwerkersovereenkomst.	▪ Ingericht
5.15	Toegangsbeveiliging	De organisatie bepaalt welke groepen medewerkers toegang krijgen en wie beheerder is. Bij de productieomgeving kunnen alleen de engineers die Inora bouwen, elk bij naam.	▪ Ingericht
5.16	Identiteitsbeheer	Medewerkers loggen in met hun eigen account via het identiteitsbeheer van de organisatie, met SAML of OpenID Connect; SCIM maakt accounts aan en sluit ze af. Schakelt de organisatie een account daar uit, dan kan die persoon niet meer inloggen. Gedeelde accounts zijn er niet.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.17	Beheren van authenticatie-informatie	Met single sign-on bewaart Inora geen wachtwoorden. Beheertoegang tot de productieomgeving vraagt een fysieke beveiligingssleutel, en sleutels en certificaten van diensten staan in een sleutelkluis, nooit in de broncode.	▪ Ingericht
5.18	Toegangsrechten	Elk kwartaal controleren wij de toegangsrechten. Vertrekt iemand, dan vervalt de toegang dezelfde dag.	▪ Ingericht
5.19	Informatiebeveiliging in leveranciersrelaties	Wij werken met zo min mogelijk subverwerkers: voor Inora Amazon Web Services, en Microsoft (Azure OpenAI, EU). Wij blijven verantwoordelijk voor wat onze leveranciers doen.	▪ Ingericht
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Elke subverwerker heeft een overeenkomst getekend met verplichtingen die niet zwakker zijn dan die in onze verwerkersovereenkomst.	▪ Ingericht
5.21	Beheren van informatiebeveiliging in de ICT-keten	Inora draait op open bouwblokken en het taalmodel is uitwisselbaar, zodat Inora van geen enkele leverancier afhangt. De bibliotheken waarop het draait, worden gecontroleerd op bekende kwetsbaarheden.	▪ Ingericht
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Een nieuwe subverwerker melden wij 30 dagen vooraf. De organisatie kan bezwaar maken. Vinden wij samen geen oplossing, dan mag zij de overeenkomst beëindigen voor het deel dat zonder de nieuwe subverwerker niet kan worden geleverd, zonder kosten.	▪ Ingericht
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Inora draait bij Amazon Web Services EMEA SARL in de regio Europa (Ierland), het taalmodel via het EU-inferentieprofiel van Amazon Bedrock of via Azure OpenAI in de EU; het systeem kiest het model. Niemand traint modellen met deze gegevens. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model, en Azure OpenAI draait met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens, zodat Microsoft geen vragen of antwoorden bewaart en geen medewerker van Microsoft ze leest.	▪ Ingericht
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Een vastgelegde incidentprocedure in zeven stappen: ontdekken, indammen, beoordelen, melden, ondersteunen, verslag en leren.	▪ Ingericht
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Elke gebeurtenis wordt beoordeeld op welke organisaties, gegevens en mensen zij raakt, en ingedeeld in vier ernstklassen, van kritiek tot laag, zoals Kwetsbaarheid melden ze beschrijft.	▪ Ingericht
5.26	Reageren op informatiebeveiligingsincidenten	Een datalek of een vermoeden daarvan melden wij uiterlijk 24 uur na kennisname aan de organisatie, met wat bekend is. Binnen tien werkdagen volgt een schriftelijk verslag.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.27	Leren van informatiebeveiligingsincidenten	Elk incident onderzoeken wij zonder schuldvraag, met de oorzaak in het systeem, en wij passen het systeem of de procedure aan om herhaling te voorkomen.	▪ Ingericht
5.28	Verzamelen van bewijsmateriaal	Bij een incident leggen wij een momentopname van de getroffen omgeving vast voordat er iets verandert, met wie haar nam en wanneer. De logging is onveranderbaar (5.33).	▪ Ingericht
5.29	Informatiebeveiliging tijdens een verstoring	De herstelprocedure staat op papier, zodat elke engineer haar alleen kan uitvoeren. Na een herstel passen wij verwijderingen opnieuw toe.	▪ Ingericht
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Elke dag een back-up, elk kwartaal een hersteltest, ten hoogste 24 uur gegevensverlies. Een herstel uit back-up duurt ten hoogste 8 uur. Ingericht op 99,9% beschikbaarheid, met als doel 95% van de storingen binnen 4 uur opgelost en een reactie binnen een uur, dag en nacht.	▪ Ingericht
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	De AVG, de UAVG en de AI-verordening zijn in de gepubliceerde beleidsstukken op Inora betrokken. De verwerkersovereenkomst volgt artikel 28 AVG.	▪ Ingericht
5.32	Intellectuele-eigendomsrechten	De protocollen en het handboek blijven van de organisatie die ze schreef. Voor bronnen van anderen, zoals landelijke richtlijnen, geldt de licentie van hun uitgever.	▪ Ingericht
5.33	Beschermen van registraties	Logging wordt 12 maanden in de EU bewaard en kan door de applicatie niet worden gewijzigd. Facturen en de stukken erachter bewaren wij zeven jaar, zoals de fiscale wet vraagt.	▪ Ingericht
5.34	Privacy en bescherming van persoonsgegevens	De organisatie is verwerkingsverantwoordelijke, wij zijn verwerker. Niemand in de organisatie leest een gesprek van een medewerker, en geen model traint op de gegevens.	▪ Ingericht
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De organisatie of haar auditor controleert elke verplichting uit de verwerkersovereenkomst, in beginsel eenmaal per jaar.	▪ Ingericht
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Elk jaar toetsen wij deze matrix aan wat in productie draait; een afwijking wordt hersteld of vastgelegd.	▪ Ingericht
5.37	Gedocumenteerde bedieningsprocedures	De incidentprocedure en de herstelprocedure staan op papier, zodat elke engineer haar alleen kan uitvoeren.	▪ Ingericht

Mensgericht (8)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
6.1	Screening	Iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
6.2	Arbeidsovereenkomst	Iedereen tekent een geheimhoudingsverklaring die ook na vertrek blijft gelden, en de beveiligingsregels, bij de start en daarna elk jaar.	▪ Ingericht
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Twee keer per jaar oefent het team met phishing en met het omgaan met zorggegevens. Iedereen tekent de beveiligingsregels bij de start en elk jaar.	▪ Ingericht
6.4	Disciplinaire procedure	De beveiligingsregels noemen wat er gebeurt bij een overtreding, van een gesprek tot het intrekken van toegang en ontslag.	▪ Ingericht
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	De geheimhouding blijft na vertrek gelden, en de toegang vervalt dezelfde dag.	▪ Ingericht
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend, zoals artikel 30, lid 4 UAVG vraagt van wie gezondheidsgegevens verwerkt zonder eigen beroepsgeheim.	▪ Ingericht
6.7	Werken op afstand	Werklaptops hebben volledige schijfversleuteling, een firewall en automatische beveiligingsupdates, en vergrendelen na enkele minuten. Gegevens van organisaties staan nooit op een laptop.	▪ Ingericht
6.8	Melden van informatiebeveiligingsgebeurtenissen	Een verloren of gestolen laptop melden wij dezelfde dag. Onderzoekers melden een kwetsbaarheid per mail en krijgen binnen drie werkdagen een ontvangstbevestiging.	▪ Ingericht

Fysiek (14)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
7.1	Fysieke beveiligingszones	Inora draait alleen in datacenters van Amazon Web Services in de EU; hun fysieke beveiliging ligt bij AWS, volgens zijn eigen ISO/IEC 27001- en SOC 2-rapporten. Op het kantoor van Axiomatic staan geen gegevens van organisaties.	▣ Ingericht bij AWS
7.2	Fysieke toegangsbeveiliging	Axiomatic heeft geen eigen serverruimte; niemand van Axiomatic komt in een datacenter. Wij bereiken Inora alleen op afstand, met een persoonlijk account en een fysieke beveiligingssleutel (de datacenters zelf: 7.1).	▪ Ingericht
7.3	Beveiligen van kantoren, ruimten en faciliteiten	De ruimten waar gegevens van organisaties staan, zijn die van AWS. Een kantoor van Axiomatic bevat geen gegevens van organisaties.	▣ Ingericht bij AWS
7.4	Monitoren van de fysieke beveiliging	De datacenters worden door AWS bewaakt, zoals zijn eigen auditrapporten beschrijven.	▣ Ingericht bij AWS

Nr.	Beheersmaatregel	Zo is het ingericht	Status
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Brand, water, stroom en klimaat in de datacenters zijn de verantwoordelijkheid van AWS. Back-ups staan apart van de productie, versleuteld, in de EU.	▣ Ingericht bij AWS
7.6	Werken in beveiligde zones	Het werk in de beveiligde zones van de datacenters doet AWS; Axiomatic werkt er niet.	▣ Ingericht bij AWS
7.7	‘Clear desk’ en ‘clear screen’	Laptops vergrendelen na enkele minuten zonder gebruik. Gegevens van organisaties staan nooit op een laptop, en dus ook nooit op een bureau.	▪ Ingericht
7.8	Plaatsen en beschermen van apparatuur	De servers van Inora zijn die van AWS, door AWS geplaatst en beschermd.	▣ Ingericht bij AWS
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Laptops hebben volledige schijfversleuteling. Een verloren of gestolen laptop melden wij dezelfde dag, en zijn toegang trekken wij in.	▪ Ingericht
7.10	Opslagmedia	Opslag met gegevens van organisaties is die van AWS, versleuteld met AES-256. De schijven van laptops zijn volledig versleuteld.	▣ Ingericht bij AWS
7.11	Nutsvoorzieningen	Stroom, koeling en netwerk van de datacenters zijn de verantwoordelijkheid van AWS.	▣ Ingericht bij AWS
7.12	Beveiligen van bekabeling	De bekabeling van de datacenters is de verantwoordelijkheid van AWS. Al het verkeer van Inora is versleuteld, ook over die kabels.	▣ Ingericht bij AWS
7.13	Onderhoud van apparatuur	AWS onderhoudt de apparatuur in zijn datacenters. Laptops installeren beveiligingsupdates automatisch.	▣ Ingericht bij AWS
7.14	Veilig verwijderen of hergebruiken van apparatuur	Schijven met gegevens van organisaties zijn die van AWS, die ze volgens zijn eigen gecontroleerde procedure wist of vernietigt. Op laptops staan geen gegevens van organisaties.	▣ Ingericht bij AWS

Technologisch (34)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.1	‘User endpoint devices’	Werklaptops: volledige schijfversleuteling, firewall, automatische updates en schermvergrendeling. Medewerkers van de organisatie gebruiken Inora in de browser, ingelogd via het eigen identiteitsbeheer van de organisatie.	▪ Ingericht
8.2	Speciale toegangsrechten	Beheertoegang tot de productieomgeving hebben alleen de engineers die Inora bouwen, met een persoonlijk account, multifactorauthenticatie en een fysieke beveiligingssleutel. Elke toegang wordt vastgelegd.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.3	Beperking toegang tot informatie	Een vraag binnen de ene organisatie kan alleen de documenten van die organisatie bereiken. Niemand in de organisatie leest een gesprek van een medewerker. Axiomatic leest een gesprek alleen in op schriftelijk verzoek van de functie die de organisatie aanwijst, voor een incident of een klacht, of bij een wettelijke vordering (art. 5.6); elke inzage wordt vastgelegd en de medewerker hoort ervan, tenzij de wet dat verbiedt. Bij een storing of beveiligingsincident onderzoekt Axiomatic de systeemlogging en het antwoordverslag, nooit een gesprek. Voor de teamverslagen deelt het taalmodel dat het antwoord schrijft, in dezelfde stap het gesprek in naar onderwerp, zonder namen; geen mens leest mee (art. 5.6).	▪ Ingericht
8.4	Toegangsbeveiliging op broncode	De broncode is alleen bereikbaar met een persoonlijk account met multifactorauthenticatie, en elke wijziging wordt door een tweede engineer beoordeeld.	▪ Ingericht
8.5	Beveiligde authenticatie	Inloggen loopt via het eigen identiteitsbeheer van de organisatie, met SAML of OpenID Connect, en haar eigen regels voor multifactorauthenticatie; SCIM maakt accounts aan en sluit ze af. Bij Entra ID geeft de toestemming Inora alleen openid, profile, email en User.Read, gedelegeerd en alleen-lezen; geen toegang tot mail, bestanden, Teams of SharePoint. Inora leest alleen de groepen die de organisatie aan de app toewijst, zodat de claim nooit overloopt. Een sessie eindigt uiterlijk acht uur nadat zij begon.	▪ Ingericht
8.6	Capaciteitsbeheer	Belasting, opslag en modelcapaciteit worden per omgeving gemeten, met een melding voordat een grens wordt bereikt.	▪ Ingericht
8.7	Bescherming tegen malware	Elk document dat in Inora komt, wordt op malware gescand voordat het in de zoekindex komt. Laptops draaien de malwarebescherming van het besturingssysteem.	▪ Ingericht
8.8	Beheer van technische kwetsbaarheden	De bibliotheken van Inora worden automatisch gecontroleerd op bekende kwetsbaarheden. Kritieke beveiligingsupdates voeren wij binnen 72 uur door, andere binnen 30 dagen.	▪ Ingericht
8.9	Configuratiebeheer	De infrastructuur wordt als code vastgelegd en beoordeeld als software, langs dezelfde tweede engineer als een wijziging in Inora.	▪ Ingericht
8.10	Wissen van informatie	Gesprekken verdwijnen na 90 dagen, of na de termijn die de organisatie instelt; een gesprek dat de functie uit bijlage 3 bij de verwerkersovereenkomst opvroeg, blijft tot het onderzoek is afgerond (art. 5.5). Na de overeenkomst zijn de actieve systemen uiterlijk op dag 30 leeg en de back-ups op dag 60, schriftelijk bevestigd.	▪ Ingericht
8.11	Maskeren van gegevens	Ontwikkelen en testen gebeurt zonder gegevens van organisaties. De metingen die Axiomatic ziet, bevatten geen namen en geen inhoud van documenten, vragen of antwoorden.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.12	Voorkomen van gegevenslekken (‘data leakage prevention’)	Een vraag kan alleen de documenten van de eigen organisatie bereiken. Gegevens van organisaties komen nooit op een laptop en nooit in de AI-hulpmiddelen waarmee wij software schrijven.	▪ Ingericht
8.13	Back-up van informatie	Elke dag een back-up van elke omgeving, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland). Elk kwartaal zetten wij er een terug om te controleren of die werkt.	▪ Ingericht
8.14	Redundantie van informatieverwerkende faciliteiten	Inora draait verdeeld over meerdere beschikbaarheidszones van de regio Europa (Ierland), zodat het uitvallen van één datacenter het niet stillegt. Ook de opgeslagen gegevens staan bij AWS verspreid over meerdere zones.	▪ Ingericht
8.15	Logging	Inora legt inlogmomenten, beheerhandelingen en elke toegang door medewerkers van Axiomatic vast, 12 maanden lang. Op verzoek krijgt een organisatie de beveiligingslogging van haar omgeving, opgeteld per team van minstens vijf mensen en per dag, en elke toegang door Axiomatic; een dag met minder dan vijf inlogs staat er als ‘<5’. Inlogmomenten en IP-adressen van één medewerker gaan nooit naar de organisatie. Bij een beveiligingsincident onderzoekt Axiomatic het logboek zelf en rapporteert een bevinding over het systeem, zonder een zorgmedewerker te noemen.	▪ Ingericht
8.16	Monitoren van activiteiten	Wij krijgen een melding bij herhaald mislukt inloggen, ongewoon verkeer, fouten en onbeschikbaarheid.	▪ Ingericht
8.17	Kloksynchronisatie	Elke server neemt zijn tijd van de tijdsdienst van de cloudleverancier, zodat de logging van alle onderdelen op de seconde gelijkloopt.	▪ Ingericht
8.18	Gebruik van speciale systeemhulpmiddelen	Beheerhulpmiddelen die de applicatie kunnen omzeilen, bereiken de productieomgeving alleen via de persoonlijke accounts van de engineers, met een fysieke beveiligingssleutel. Elke toegang wordt vastgelegd.	▪ Ingericht
8.19	Installeren van software op operationele systemen	Software komt alleen als beoordeelde release via de uitrolstraat in productie; niemand installeert met de hand iets op een draaiende server.	▪ Ingericht
8.20	Beveiliging netwerkcomponenten	Al het verkeer naar Inora en tussen de onderdelen ervan gebruikt TLS 1.2 of hoger; oudere protocollen worden geweigerd.	▪ Ingericht
8.21	Beveiliging van netwerkdiensten	Inora is alleen bereikbaar via de load balancer van AWS, achter een webapplicatiefirewall die bekende aanvalspatronen tegenhoudt.	▪ Ingericht
8.22	Netwerksegmentatie	Elke organisatie heeft een eigen omgeving, gescheiden in de infrastructuur en niet alleen in de software. Ontwikkelen en testen gebeurt apart van de productie.	▪ Ingericht

Nr.	Beheersmaatregel	Zo is het ingericht	Status
8.23	Toepassen van webfilters	Werklaptops filteren het webverkeer op DNS-niveau en blokkeren bekende kwaadaardige domeinen.	▪ Ingericht
8.24	Gebruik van cryptografie	TLS 1.2 of hoger tijdens transport, AES-256 bij opslag voor databases, documentopslag, zoekindexen en back-ups. De sleutels staan in AWS Key Management Service, in de EU; elk gebruik wordt vastgelegd. Geheimen staan in een sleutelkluis.	▪ Ingericht
8.25	Beveiligen tijdens de ontwikkelcyclus	Elke wijziging wordt door een tweede engineer beoordeeld, met de OWASP Top 10 als checklist. Geeft de organisatie daarvoor een schriftelijke opdracht, na instemming van haar ondernemingsraad waar zij er een heeft, dan wordt elke nieuwe versie getest op haar toetsset, haar eigen vragen en gemarkeerde antwoorden ontdaan van namen, voordat haar medewerkers die versie zien.	▪ Ingericht
8.26	Toepassingsbeveiligingseisen	Naast de OWASP Top 10 telt wat eigen is aan Inora als beveiligingsfout: een antwoord buiten de bronnen van de organisatie, of een organisatie die bij een andere komt. De ernstklassen op Kwetsbaarheid melden noemen ze.	▪ Ingericht
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Per organisatie een eigen database, documentopslag en zoekindex; geen gedeelde database met organisaties gescheiden door een kolom. Het taalmodel is uitwisselbaar, en de verwerking blijft in de EU.	▪ Ingericht
8.28	Veilig coderen	De OWASP Top 10 is de checklist bij elke beoordeling. Geheimen staan nooit in de broncode, en bibliotheken worden gecontroleerd op bekende kwetsbaarheden.	▪ Ingericht
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Geeft de organisatie daarvoor een schriftelijke opdracht, na instemming van haar ondernemingsraad waar zij er een heeft, dan wordt elke nieuwe versie getest op haar toetsset, haar eigen vragen en gemarkeerde antwoorden ontdaan van namen, voordat zij live gaat.	▪ Ingericht
8.30	Uitbestede systeemontwikkeling	Inora wordt gebouwd door de eigen engineers van Axiomatic. Geen externe kracht heeft toegang tot de productieomgeving of tot gegevens van organisaties.	▪ Ingericht
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkelen en testen gebeurt in een aparte omgeving, zonder gegevens van organisaties.	▪ Ingericht
8.32	Wijzigingsbeheer	Elke wijziging wordt door een tweede engineer beoordeeld voordat zij in productie gaat. Gepland onderhoud kondigen wij vooraf aan, en een functie waarop de organisatie rekent, verdwijnt niet zonder aankondiging.	▪ Ingericht
8.33	Testgegevens	Testgegevens bevatten geen gegevens van organisaties; ontwikkelen en testen gebeurt zonder.	▪ Ingericht
8.34	Bescherming van informatie-systemen tijdens audits	Audits en tests op productie worden vooraf afgesproken, waar het kan alleen-lezen en buiten de drukste uren.	▪ Ingericht

Zorg (NEN 7510) (8)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.38	Analyse en specificatie van informatiebeveiligingseisen	Voor elke functie gelden vooraf de OWASP Top 10 en de fouten die eigen zijn aan Inora: een antwoord buiten de bronnen, of een organisatie die bij een andere komt.	▪ Ingericht
5.39	Zorgontvangers op unieke wijze identificeren	Inora registreert geen zorgontvangers en kent dus geen dubbele registraties; de unieke identificatie en het samenvoegen gebeuren in het ECD van de organisatie. Inora vraagt niet om een burgerservicenummer.	▪ Ingericht
5.40	Validatie van getoonde/geprinte gegevens	Inora registreert geen zorgontvangers. Een rapportage over een cliënt gaat pas na akkoord het dossier in van de cliënt die de zorgmedewerker in het ECD open heeft; daar identificeert de organisatie de cliënt. Elke zin die op een bron van de organisatie rust, draagt een markering die het document en de passage toont.	▪ Ingericht
5.41	Openbaar beschikbare gezondheidsinformatie	Openbare bronnen die de organisatie aanwijst, zoals landelijke richtlijnen, leest Inora zoals ze zijn uitgegeven, onder de licentie van hun uitgever, en elk antwoord toont de bron waarop het rust.	▪ Ingericht
5.42	Communicatie in noodsituaties	Een storing die Inora onbruikbaar maakt, meldt de organisatie via support@axiomatic.digital, dag en nacht; reactie binnen een uur. Bij een datalek hoort haar contactpersoon het uiterlijk 24 uur na kennisname. Het kanaal en een tweede contactpersoon beproeven wij elk jaar met de contactpersoon van de organisatie.	▪ Ingericht
5.43	Incidenten extern melden	Wij melden een datalek uiterlijk 24 uur na kennisname aan de organisatie en helpen haar met haar melding bij de Autoriteit Persoonsgegevens, die waar mogelijk binnen 72 uur moet.	▪ Ingericht
6.9	Managementtraining	De directie volgt elk jaar een training in de plichten die de Cyberbeveiligingswet en NEN 7510 aan het bestuur stellen.	▪ Ingericht
8.35	Zero trust-beginselen	Geen toegang rust op een netwerklocatie: elke gebruiker logt in via de eigen identiteitsdienst van de organisatie, elke beheertoegang met een persoonlijk account en een fysieke sleutel, en elke toegang wordt vastgelegd.	▪ Ingericht

6. Per laag: wie het controleerde

6.1 Inora

Norm of toets	Wat het dekt	Door
Ingericht volgens NEN 7510 en ISO 27001	Elke maatregel en hoe die is ingevuld, in hoofdstuk 5	Axiomatic

Norm of toets	Wat het dekt	Door
Ingericht op 99,9% beschikbaarheid	Doel: 95% van de storingen binnen 4 uur opgelost; reactie binnen een uur, dag en nacht. Storingsbericht per e-mail aan uw contactpersoon.	Axiomatic
Penetratietest, elk jaar	De applicatie en de infrastructuur, op de OWASP Top 10 en de scheiding tussen organisaties; de samenvatting op verzoek	Een onafhankelijke specialist
Doorlopend scannen	Code, softwarebibliotheken, containers en de inrichting in de cloud, bij elke wijziging en elke dag	Axiomatic

Een kwetsbaarheid melden kan altijd: security@axiomatic.digital, met ‘Beveiliging’ in de onderwerpregel. Wij bevestigen de ontvangst binnen drie werkdagen.

6.2 De diensten van AWS en Microsoft eronder

De certificaten die Amazon Web Services en Microsoft publiceren voor de diensten waarop Inora draait, zoals AWS ze op 2 november 2026 op zijn eigen pagina’s noemt, en Microsoft voor Azure op de zijne. Ze gaan over de diensten van AWS en Microsoft, niet over Axiomatic of Inora; Axiomatic draagt ze niet mee.

Dienst	Norm	Wat het dekt	Door	Bron
Hosting, Europa (Ierland)	ISO/IEC 27001:2022	Informatiebeveiliging	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Hosting	ISO/IEC 27017:2015	Beveiligingsmaatregelen voor clouddiensten	EY CertifyPoint	aws.amazon.com/compliance/iso-27017-faqs
Hosting	ISO/IEC 27018:2019	Persoonsgegevens in de cloud	EY CertifyPoint	aws.amazon.com/compliance/iso-27018-faqs
Hosting	ISO/IEC 27701:2019	Privacybeheer	EY CertifyPoint	aws.amazon.com/compliance/iso-27701-faqs
Hosting	BSI C5	Duitse cloudnorm; regio Ierland in de reikwijdte		aws.amazon.com/compliance/bsi-c5
Hosting	SOC 1, 2 en 3	Rapporten van de auditor, in AWS Artifact		aws.amazon.com/compliance/services-in-scope/SOC
Amazon Bedrock	ISO/IEC 27001, 27017, 27018, 27701	Bedrock in de reikwijdte, Bedrock Marketplace niet	EY CertifyPoint	aws.amazon.com/compliance/iso-27001-faqs
Amazon Bedrock	ISO/IEC 42001:2023	Beheer van AI-systemen	Schellman	aws.amazon.com/compliance/iso-42001-faqs
Amazon Bedrock	BSI C5	Bedrock in de reikwijdte		aws.amazon.com/compliance/services-in-scope/C5

Dienst	Norm	Wat het dekt	Door	Bron
Amazon Bedrock	SOC 1, 2 en 3	Bedrock in de reikwijdte		aws.amazon.com/compliance/services-in-scope/SOC
Microsoft Azure (Azure OpenAI)	ISO/IEC 27001, 27017 en 27018	Informatiebeveiliging, clouddiensten en persoonsgegevens in de cloud; welke Azure-diensten erin vallen, staat in de Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001
Microsoft Azure (Azure OpenAI)	SOC 2 Type 2	Het rapport van de auditor over Azure, elk half jaar, op te vragen in de Service Trust Portal		learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

De fysieke beveiliging van de datacenters ligt bij Amazon Web Services. Het moederbedrijf van AWS is Amerikaans; wat dat betekent, staat in onze privacyverklaring.

7. De Cyberbeveiligingswet, plicht voor plicht

Plicht van uw bestuur	Artikel	Wat wij doen	Wat u in het dossier legt
Zorgplicht	21, lid 3, d: de toeleveringsketen	Elke maatregel staat beschreven, met hoe die is ingevuld. De verwerkersovereenkomst bindt ons eraan, en wij werken mee aan uw audit.	Beveiligingsoverzicht versie 1.4 en controlematrix versie 1.3, van 9 november 2026; verwerkersovereenkomst,
Meldplicht	26: waarschuwing binnen 24 uur	Een datalek of een vermoeden daarvan in uw omgeving melden wij uiterlijk 24 uur na kennisname, met wat u voor uw eigen melding nodig hebt. Het verslag volgt binnen tien werkdagen.	Melding en verslag van een datalek; Beveiliging
Training van bestuurders	24, lid 2 tot en met 5	Een uitleg voor uw bestuurders: wat Inora is, waar het stopt en hoe het beveiligd is.	Uitleg voor de training van uw bestuurders (op verzoek)
Eindverantwoordelijkheid	24, lid 1: het bestuur keurt goed	Eén partij staat ervoor in: wij bouwen Inora, voeren het in en beheren het, en blijven verantwoordelijk voor onze subverwerkers.	subverwerkers, versie 1.6 van 11 november 2026

8. Als er iets misgaat

- Wij melden een datalek of een vermoeden daarvan zonder onredelijke vertraging, uiterlijk 24 uur nadat wij ervan kennis hebben genomen. Dat is een maximumtermijn, geen wachttijd.
- Wij delen direct wat bekend is: de aard, de betrokken gegevens en mensen, de waarschijnlijke gevolgen en de maatregelen.
- Binnen tien werkdagen sturen wij een schriftelijk verslag: wat er gebeurde, wat de oorzaak was en wat wij veranderden.
- Uw termijn van 72 uur bij de Autoriteit Persoonsgegevens blijft van u en wacht niet op ons verslag. Uw 72 uur beginnen zodra wij u melden; onze 24 uur gaan eraan vooraf.
- Wij onderzoeken een fout zonder schuldvraag, met de oorzaak in het systeem.

9. Leveranciers, audits en het einde

- Wij staan in voor wat Inora met uw bronnen doet; u voor wat die bronnen zeggen.
- Wij blijven verantwoordelijk voor onze leveranciers. Een nieuwe subverwerker melden wij 30 dagen vooraf; u kunt bezwaar maken.
- Na afloop krijgt u alles kosteloos terug: documenten in hun eigen formaat, de rest machineleesbaar. Uit actieve systemen is alles uiterlijk op dag 30 weg, uit back-ups uiterlijk op dag 60, schriftelijk bevestigd.
- Wij werken mee aan audits door uw organisatie of uw auditor, over alle verplichtingen uit de verwerkersovereenkomst.

10. Wat u in het dossier krijgt

- Dit ICT-dossier.
- Het beveiligingsoverzicht, versie 1.4 van 9 november 2026, met elke maatregel.
- De controlematrix, versie 1.3 van 9 november 2026, de basis voor uw verklaring van toepasselijkheid.
- De lijst van subverwerkers, versie 1.6 van 11 november 2026.
- Op verzoek: de uitleg voor de training van uw bestuurders.

11. Contact

Axiomatic B.V., Delft. security@axiomatic.digital.

12. Zes regels die meeverhuizen met de server

Draait Inora bij ons of op uw servers: dit blijft gelden.

- **Geen model leert van uw gegevens.**
- **Elk antwoord met zijn bron en versie.** In elk antwoord is elke bron van uw organisatie gemarkeerd; één tik toont de titel en de versie waaruit het komt. Staat het antwoord niet in uw bronnen, dan zegt Inora dat, en waar het zocht.
- **Elke stap vastgelegd.** Inora legt bij elk antwoord elke stap vast: welke bronnen het las, in welke versie, en welke controle het antwoord doorstond. Op uw schriftelijk verzoek herleidt Axiomatic met dat logboek een fout antwoord tot zijn oorzaak in het systeem, nooit tot een persoon.
- **Ingericht volgens NEN 7510 en ISO 27001.**
- **Een nieuwe subverwerker hoort u dertig dagen vooraf.**
- **Stopt u, dan krijgt u uw kennis kosteloos terug.**