AXIOMATIC

Beveiligingsoverzicht

Axiomatic B.V. en Inora

Versie 1.4, 9 november 2026

1. Inleiding

Axiomatic B.V. ontwerpt, bouwt, implementeert en beheert Inora. Zorgmedewerkers stellen Inora een vraag in gewone taal en krijgen antwoord uit de bronnen die hun organisatie heeft aangewezen; één tik op een markering toont de bron van de organisatie waarop een zin rust. De eigen documenten van de organisatie zijn intern, en de vragen kunnen over cliënten gaan. Dit overzicht beschrijft hoe wij die gegevens beschermen: wie erbij kan, waar ze staan, hoe wij ze gescheiden houden, versleutelen, back-uppen en bewaken, en hoe wij herstellen.

Dit document is bedoeld voor de privacyfunctionaris, de informatiebeveiliger en de ICT-afdeling van een zorgorganisatie die Inora beoordeelt. Het hoort bij de beveiligingsmaatregelen waarnaar Bijlage 2 van onze verwerkersovereenkomst verwijst. De voorgestelde termijnen en maatregelen worden pas afspraken na bevestiging en ondertekening van de verwerkersovereenkomst.

2. Organisatie en mensen

2.1 Het team

De mensen die Inora bouwen, implementeren en beheren:

- Engineering bouwt en beheert Inora. De directeur is verantwoordelijk voor beveiliging en privacy binnen Axiomatic.
- Implementatie en partnerschappen werken met zorgorganisaties tijdens de implementatie, zonder toegang tot gegevens van organisaties of tot de productieomgeving.
- De adviseurs hebben geen toegang tot gegevens van organisaties of tot de productieomgeving.

Alleen met naam genoemde engineers hebben toegang tot de productieomgeving, vastgelegd in de verwerkersovereenkomst. Wij werken niet met externe krachten die toegang hebben tot de productieomgeving of tot gegevens van organisaties.

2.2 Geheimhouding en screening

Iedereen bij Axiomatic heeft een geheimhoudingsverklaring getekend die ook na vertrek blijft gelden. Die verklaring is ook wat de Uitvoeringswet AVG vraagt van mensen die gezondheidsgegevens verwerken zonder eigen beroepsgeheim (artikel 30, lid 4 UAVG). Iedereen met toegang tot productie heeft een verklaring omtrent het gedrag (VOG).

Iedereen leest en tekent onze beveiligingsregels bij de start en daarna elk jaar opnieuw.

2.3 Apparaten

Wij werken op laptops met volledige schijfversleuteling, automatische beveiligingsupdates, een firewall en een schermvergrendeling na enkele minuten. Gegevens van organisaties staan nooit op laptops. Een verloren of gestolen laptop melden wij dezelfde dag, en de toegang ervan trekken wij in.

2.4 Accounts en toegang

- Alleen persoonlijke accounts. Geen gedeelde accounts, geen gedeelde wachtwoorden.
- Multifactorauthenticatie op elk account dat toegang geeft tot code, infrastructuur, e-mail of documenten. Beheertoegang tot de productieomgeving vereist een fysieke beveiligingssleutel.
- Toegang tot de productieomgeving is beperkt tot de met naam genoemde engineers, en tot wat zij nodig hebben.
- Elke toegang door medewerkers van Axiomatic tot de omgeving van een organisatie wordt vastgelegd. Elk kwartaal controleren wij de toegangsrechten.
- Vertrekt iemand, dan vervalt zijn toegang dezelfde dag.

3. Opbouw

3.1 Eén omgeving per organisatie

Elke organisatie heeft in Inora een eigen omgeving: een eigen database, eigen documentopslag en een eigen zoekindex. Er is geen gedeelde database waarin organisaties alleen door een kolom van elkaar zijn gescheiden. Een vraag die binnen de ene organisatie wordt gesteld, kan alleen de documenten van die organisatie bereiken.

3.2 Inloggen

Inora koppelt aan de eigen single sign-on van de organisatie, meestal Microsoft Entra ID, via OpenID Connect of SAML 2.0. Met single sign-on bewaart Inora geen wachtwoorden; multifactorauthenticatie en wachtwoordregels stelt de organisatie in, in haar eigen identiteitsbeheer. Schakelt de organisatie daar een account uit, dan kan die persoon niet meer inloggen op Inora. Een al geopende sessie kan actief blijven tot deze wordt ingetrokken of verloopt. Een sessie eindigt uiterlijk na acht uur.

De toestemming in Entra ID geeft Inora alleen openid, profile, email en User.Read, gedelegeerd en alleen-lezen; de groepen van de organisatie komen als claim in het inlogbewijs. 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. Die accounts schakelt de beheerder van de organisatie in Inora uit.

Inora kent twee rollen. Beheerders beheren documenten, instellingen en het rapportageregister. Gebruikers stellen vragen en maken rapportages. De organisatie bepaalt welke groepen medewerkers welke rol krijgen.

3.3 Hoe een vraag wordt beantwoord

1. Een gebruiker stelt een vraag in Inora.
2. Inora zoekt in de eigen index van de organisatie naar de passages die over de vraag gaan.
3. De vraag en die passages gaan naar het taalmodel, binnen de Europese Unie.
4. Het model schrijft een antwoord op basis van de passages. Inora toont het antwoord met een markering bij elke zin die op een bron van de organisatie rust; één tik toont het document en de passage. Beantwoordt geen passage de vraag, dan zegt Inora dat, en waar het zocht.

5. De vraag, het antwoord en de bronnen worden bewaard in de gespreksgeschiedenis van de gebruiker, in de omgeving van de organisatie, voor de bewaartermijn die de organisatie heeft ingesteld.

Bij rapportages komen de kopjes uit een register dat de organisatie zelf bijhoudt. Het model schrijft alleen de inhoud eronder.

De bronnen van de organisatie blijven in haar eigen documentsysteem staan; Inora werkt met een kopie die haar handboekbeheerder aanlevert en bijwerkt. Er is geen koppeling met dat documentsysteem.

Het cliëntdossier blijft in het eigen ECD van de organisatie. Inora leest het met de login en rechten van de zorgmedewerker zelf, in een eigen microVM per gebruiker, dus de pilot vraagt geen koppeling. Koppelingen komen na de pilot, en de ICT van de organisatie zet ze aan.

Bij het opbouwen van de zoekindex gaan ook documentpassages naar het embeddingmodel in de EU. Voor het antwoord gaan de vraag en de gevonden passages naar het taalmodel; in dezelfde stap deelt het model het gesprek in naar onderwerp, voor de teamverslagen (hoofdstuk 6).

4. Hosting en locatie

Onderdeel	Leverancier	Locatie
Applicatie, database, documentopslag, zoekindex	Amazon Web Services (Amazon Web Services EMEA SARL)	Regio Europa (Ierland), eu-west-1
Back-ups	Amazon Web Services	Regio Europa (Ierland), eu-west-1
Taalmodel	Amazon Bedrock, EU-inferentieprofiel	Regio's van Amazon Web Services in de EU
Taalmodellen via Azure OpenAI; het systeem kiest het model	Microsoft Ireland Operations Limited (Azure OpenAI)	Een Azure-regio in de EU
Website axiomatic.digital (geen gegevens van organisaties)	Amazon S3 en Amazon CloudFront	Bestanden in regio Europa (Ierland); levering via het wereldwijde netwerk van CloudFront

Alle gegevens in Inora worden in de Europese Unie verwerkt en opgeslagen. Verwerking buiten de EU vereist eerst een schriftelijke wijziging van de afspraken met de organisatie. Voor doorgifte buiten de EER is bovendien een geldige grond uit hoofdstuk V AVG nodig; toestemming van de organisatie alleen volstaat niet. Toegang op afstand en ondersteuning vallen ook onder deze beoordeling. Artikel 3.5 van de verwerkersovereenkomst beschrijft dit.

De fysieke beveiliging van de datacenters is de verantwoordelijkheid van Amazon Web Services. AWS publiceert zijn eigen certificeringen en auditrapporten. Die gaan over de diensten van AWS, niet over Axiomatic.

De moederbedrijven, Amazon.com, Inc. en Microsoft Corporation, zijn Amerikaans; beide nemen deel aan het EU-VS-kader voor gegevensbescherming (EU-US Data Privacy Framework). Opslag in de EU sluit een verzoek van een buitenlandse overheid niet uit; hoofdstuk 13 beschrijft wat wij dan doen.

5. Versleuteling

- **Tijdens transport.** Al het verkeer van en naar Inora, en tussen de onderdelen ervan, gebruikt TLS 1.2 of hoger. Oudere protocollen worden geweigerd.
- **Bij opslag.** Databases, documentopslag, zoekindexen en back-ups zijn versleuteld met AES-256.
- **Sleutels.** De sleutels staan in AWS Key Management Service, in de EU; de toegang is beperkt en elk gebruik wordt vastgelegd.
- **Geheimen.** Wachtwoorden van diensten, API-sleutels en certificaten staan in een sleutelkluis, nooit in de broncode.

De grens. Tijdens het beantwoorden van een vraag zijn de vraag en de passages alleen ontsleuteld zolang het antwoord wordt gemaakt; het model bewaart ze niet. Dat gebeurt op onze servers en bij het taalmodel. Versleuteling tijdens transport en bij opslag voorkomt die verwerking van leesbare tekst niet. Dit is geen end-to-endversleuteling waarbij alleen de gebruiker de tekst kan lezen. Medewerkers met toegang tot de productieomgeving zouden de inhoud op dat moment in principe kunnen zien; hoofdstuk 2 beschrijft wie dat zijn en hoe hun toegang wordt vastgelegd.

6. Kunstmatige intelligentie

- **Model.** Inora gebruikt taalmodellen in Amazon Bedrock, via het EU-inferentieprofiel. Vragen en antwoorden worden alleen in regio's binnen de EU verwerkt. Amazon Bedrock bewaart de vraag en de passages niet en geeft ze niet aan de maker van het model.
- **Azure OpenAI.** Het systeem kiest per taak het taalmodel; via Azure OpenAI draait het in een EU-regio. Axiomatic draait het met de aangepaste misbruikmonitoring die Microsoft goedkeurt voor gevoelige gegevens: Microsoft bewaart geen vragen of antwoorden, en geen medewerker van Microsoft leest ze (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).
- **Teamverslagen.** 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.
- **Training en opslag.** Gegevens van organisaties worden niet gebruikt om modellen te trainen of bij te trainen, noch door Axiomatic, noch door de modelleverancier.
- **Zoekindex.** Om documenten doorzoekbaar te maken, zet Inora passages om in numerieke representaties met een embeddingmodel in dezelfde EU-inrichting. Die worden opgeslagen in de eigen index van de organisatie en verdwijnen met de documenten.
- **Bron op één tik.** Elke zin die op een bron van de organisatie rust, draagt een markering; één tik toont het document en de passage. Een taalmodel kan zich vergissen; met de bron kan de zorgmedewerker het controleren.
- **Grens.** Inora ondersteunt professionals met de kennis van hun organisatie. Het stelt geen diagnose, beslist niet over een behandeling en beoordeelt geen foto's van huid of wonden; bij triage triageren verpleegkundigen, en Inora legt het protocol van de organisatie naast hen en wijst aan wat ontbreekt. De professional beslist. Door dit beoogde gebruik valt Inora buiten de regels voor medische hulpmiddelen.

7. Logging en bewaking

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.

- Inora legt ook wijzigingen in documenten en instellingen vast.
- Wij krijgen een melding bij herhaald mislukt inloggen, ongewoon verkeer, fouten en onbeschikbaarheid.
- De logging staat in de EU en kan niet door de applicatie worden gewijzigd.

8. Back-ups en herstel

- Wij maken dagelijks een back-up van de omgeving van elke organisatie; hooguit 24 uur aan gegevens gaat verloren. Een herstel uit back-up duurt ten hoogste 8 uur.
- Back-ups: dagelijks, versleuteld, 30 dagen bewaard, in de regio Europa (Ierland), verspreid over meerdere beschikbaarheidszones.
- Elk kwartaal zetten wij een back-up terug in een aparte omgeving om te controleren of die volledig is.
- 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 de organisatie via support@axiomatic.digital, dag en nacht. Bij een storing krijgt de contactpersoon van de organisatie bericht per e-mail, tot de storing is verholpen.
- Elk van de met naam genoemde engineers kan de dienst alleen herstellen. De herstelprocedure staat op papier.

9. Ontwikkeling en wijzigingen

- Elke wijziging in Inora wordt door een tweede engineer beoordeeld voordat zij in productie gaat.
- Ontwikkelen en testen gebeurt in een aparte omgeving zonder gegevens van organisaties.
- Wij controleren de softwarebibliotheken waarop Inora draait op bekende kwetsbaarheden. Beveiligingsupdates voor kritieke kwetsbaarheden voeren wij binnen 72 uur door, andere beveiligingsupdates binnen 30 dagen.
- De OWASP Top 10 is onze checklist voor de risico’s van webapplicaties.

10. Testen

- **Penetratietest.** Elk jaar test een onafhankelijke specialist Inora, de applicatie en de infrastructuur, op de OWASP Top 10 en op de scheiding tussen organisaties. Kritieke bevindingen lossen wij op binnen 72 uur, andere binnen 30 dagen. De samenvatting van de laatste test krijgt u op verzoek.
- **Doorlopend scannen.** Code, softwarebibliotheken, containers en de inrichting in de cloud worden bij elke wijziging en elke dag automatisch gescand.
- **Beveiligingsonderzoekers.** Iedereen kan een kwetsbaarheid bij ons melden, volgens het beleid hieronder.

Een kwetsbaarheid meldt u door te mailen naar security@axiomatic.digital met ‘Beveiliging’ in de onderwerpregel. Wij bevestigen de ontvangst binnen drie werkdagen. Wij vragen onderzoekers geen gegevens van anderen in te zien of te wijzigen, de dienst niet te verstoren en ons 90 dagen te geven voordat zij publiceren. Tegen onderzoek dat te goeder trouw en binnen deze regels is gedaan, ondernemen wij geen juridische stappen.

11. Incidentbeheer

Wij werken met een vastgelegde incidentprocedure:

1. **Ontdekken.** Meldingen uit de bewaking, van gebruikers, organisaties of onderzoekers.
2. **Indammen.** De oorzaak stoppen en de schade beperken.
3. **Beoordelen.** Vaststellen om welke organisaties, gegevens en mensen het gaat.
4. **Melden.** Wij melden een datalek of een vermoeden daarvan zonder onredelijke vertraging, uiterlijk 24 uur na kennisname. Dit is een contractuele maximumtermijn, geen wachttijd. Een datalek kan ook bestaan uit verlies van beschikbaarheid, vernietiging of ongeoorloofde verstrekking. Wij delen wat bekend is over de aard, betrokken gegevens en mensen, waarschijnlijke gevolgen en maatregelen. Meldingen noemen de soorten gegevens en het aantal betrokkenen, nooit gegevens uit Inora. Aanvullingen volgen zodra ze beschikbaar zijn.

5. **Ondersteunen.** De zorgorganisatie is verwerkingsverantwoordelijke. Zij moet een datalek zonder onredelijke vertraging en, waar mogelijk, binnen 72 uur nadat zij ervan kennis heeft genomen melden bij de Autoriteit Persoonsgegevens, tenzij een risico voor de rechten en vrijheden van mensen onwaarschijnlijk is. Bij een waarschijnlijk hoog risico informeert zij de betrokkenen zonder onredelijke vertraging, tenzij een uitzondering uit artikel 34, lid 3 AVG geldt. Zij legt elk datalek vast, ook als een melding niet nodig is. Wij helpen haar daarbij. De termijn van 72 uur begint niet pas bij ons eindverslag. Bij een latere melding moet de organisatie de vertraging toelichten.
6. **Verslag.** Binnen tien werkdagen na kennisname sturen wij een schriftelijk verslag. Loopt het onderzoek nog, dan vermelden wij dat en vullen wij het verslag aan. Dit stelt eerdere meldingen niet uit.
7. **Leren.** Wij passen het systeem of de procedure aan, om herhaling te voorkomen.

12. Bewaren en verwijderen

Gegevens	Bewaartermijn
Gesprekken (vragen, antwoorden, opgestelde rapportages, de indeling naar onderwerp)	90 dagen, of de termijn die de organisatie instelt; een gesprek dat de functie uit bijlage 3 bij de verwerkersovereenkomst opvroeg, tot het onderzoek is afgerond (art. 5.5)
Documenten	Zolang de organisatie ze in Inora laat staan; binnen 30 dagen na verwijdering ook uit back-ups weg
Gebruikersaccounts	Zolang de gebruiker toegang heeft en tot 30 dagen daarna
Loggegevens	12 maanden, tenzij de overeenkomst eerder eindigt
Dienstmetingen (aantallen vragen en responstijden per gebruiker)	Per gebruiker 30 dagen; daarna alleen opgeteld per team van minstens vijf mensen
Bekwaamheidsdossier	Zolang de medewerker bij de organisatie werkt, plus 30 dagen; in die 30 dagen exporteert de organisatie het naar haar eigen personeelsdossier
Toetsset, alleen op schriftelijke opdracht van de organisatie	Tot de organisatie de opdracht intrekt, uiterlijk tot het einde van de overeenkomst; daarna binnen 30 dagen weg
Antwoordverslag (bronnen, versies, model, toets en datum per antwoord, en een kenmerk dat de medewerker bij het antwoord ziet)	2 jaar, bij Axiomatic; daarna binnen 30 dagen uit back-ups

Gegevens	Bewaartermijn
Back-ups	30 dagen
Alle gegevens na afloop van de overeenkomst	Naar keuze van de organisatie teruggeven of verwijderen; beschikbaar voor teruggave tot en met dag 30, tenzij eerder afgerond of om verwijdering gevraagd; actieve systemen, inclusief loggegevens en zoekindexen, leeg uiterlijk dag 30; back-ups leeg uiterlijk dag 60

Alleen een bewaarplicht uit het Unierecht of Nederlands recht kan een uitzondering op verwijdering rechtvaardigen. Wij melden dan welke gegevens, grond en termijn dat betreft, tenzij de wet dat verbiedt. De gegevens blijven beschermd zolang wij ze bewaren. Na verwijdering tijdens de looptijd kunnen kopieën nog maximaal 30 dagen in back-ups staan. Bij herstel passen wij verwijderingen opnieuw toe. Op verzoek bevestigen wij de verwijdering schriftelijk.

13. Verzoeken van overheden

Wij verstrekken gegevens van organisaties alleen aan een overheidsinstantie als het Unierecht of Nederlands recht ons daartoe verplicht, bijvoorbeeld op grond van een rechterlijk bevel, en dan niet meer dan nodig. Tenzij de wet het verbiedt, laten wij het de organisatie eerst weten. Tegen verzoeken zonder geldige wettelijke grondslag maken wij bezwaar.

Vordert de wet een gesprek, dan geeft Axiomatic alleen wat de vordering vraagt en legt dat vast, en de medewerker hoort ervan, tenzij de wet dat verbiedt.

14. Verantwoording

Voor de beoordeling door de organisatie:

- dit beveiligingsoverzicht;
- de verwerkersovereenkomst, met onderwerpen uit het model van de Brancheorganisaties Zorg, maar met eigen bepalingen;
- de lijst van subverwerkers;
- de controlematrix in paragraaf 15: elke beheersmaatregel van ISO 27001 en NEN 7510 en hoe wij die hebben ingericht, de basis voor uw verklaring van toepasselijkheid;

- een beschrijving van de verwerking, voor de gegevensbeschermingseffectbeoordeling (DPIA) van de organisatie.

Wij werken mee aan audits en inspecties door de organisatie of haar gemachtigde auditor over alle verplichtingen uit de verwerkersovereenkomst. Een reguliere audit vindt in beginsel eenmaal per jaar plaats. Extra controles blijven mogelijk waar nodig voor artikel 28 AVG, onder meer bij een incident, aanwijzingen van niet-naleving, een wezenlijke wijziging of een verzoek van de toezichthouder. De organisatie draagt de kosten van haar eigen auditor, tenzij de audit een wezenlijke tekortkoming aan onze kant aantoont.

15. Controlematrix

Ingericht volgens NEN 7510 en ISO 27001: elke beheersmaatregel uit bijlage A van ISO/IEC 27001:2022 en de maatregelen die NEN 7510 voor de zorg toevoegt, met hoe Axiomatic die voor Inora heeft ingericht en de status per regel.

Organisatorisch (37)

Nr.	Beheersmaatregel	Zo is het ingericht	Status
5.1	Beleidsregels voor informatiebeveiliging	Het beveiligingsbeleid en het beveiligings-overzicht 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 verantwoorde-lijkheden bij informatiebeveiliging	De directeur is verantwoordelijk voor beveiliging en privacy binnen Axiomatic. Het beveiligings-overzicht 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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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
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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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
5.17	Beheren van authenticatie-informatie	Met single sign-on bewaart Inora geen wachtwoorden. Beheertoegang tot de productie-omgeving 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 informatie-beveiliging in leveranciersovereen-komsten	Elke subverwerker heeft een overeenkomst getekend met verplichtingen die niet zwakker zijn dan die in onze verwerkersovereenkomst.	▪ Ingericht
5.21	Beheren van informatiebe-veiliging 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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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
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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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
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
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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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 antwoord-verslag, nooit een gesprek. Voor de teamver-slagen 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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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
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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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 informatiesystemen 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

Nr.	Beheersmaatregel	Zo is het ingericht	Status
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

16. Contact

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