AXIOMATIC

Een kwetsbaarheid melden

Vindt u een zwakke plek in Inora, op axiomatic.digital of in de infrastructuur die wij beheren, meld die dan bij ons. Wij bevestigen elke melding en houden u op de hoogte tot het lek dicht is.

Bijgewerkt op 9 november 2026

Waarom dit zwaar weegt

Zorgorganisaties zetten hun protocollen, werkafspraken en kwaliteitshandboek in Inora. Hun medewerkers typen er vragen en rapportages in die over cliënten kunnen gaan, en dus gezondheidsgegevens kunnen bevatten. Een zwakke plek in Inora raakt daarom niet alleen ons, maar ook zorgorganisaties, hun medewerkers en hun cliënten. Wij horen het liever van u dan van iemand die er misbruik van maakt.

Hoe wij Inora en die gegevens beschermen, staat op de pagina Beveiliging.

Wat onder dit beleid valt

- De webapplicatie van Inora, waarin medewerkers van zorgorganisaties vragen stellen en rapporteren.
- De API’s van Inora.
- Deze website, axiomatic.digital.
- De infrastructuur die Axiomatic zelf beheert voor Inora en voor deze website.

Wat er niet onder valt

- Diensten en koppelingen van anderen, zoals de identiteitsdienst van een zorgorganisatie (bijvoorbeeld Microsoft Entra ID) of haar elektronisch cliëntdossier. Meld een kwetsbaarheid daarin bij die organisatie of bij de maker. Raakt die ook Inora, laat het ons dan ook weten.
- Social engineering en phishing van medewerkers van Axiomatic of van zorgorganisaties.
- Aanvallen die de dienst overbelasten of platleggen (DoS en DDoS).

- Geautomatiseerd scannen of testen dat de dienst voor anderen trager of onbereikbaar maakt.
- Fysieke aanvallen op kantoren of datacenters.
- Software en systemen die niet van Axiomatic zijn.

Hoe u meldt

Mail security@axiomatic.digital met ‘Beveiliging’ in de onderwerpregel.

Vermeld in uw melding:

- wat de kwetsbaarheid is en wat iemand ermee zou kunnen;
- de stappen om haar na te bootsen;
- wat het laat zien, zoals schermafbeeldingen, een proof of concept of verzoeken en antwoorden;
- hoe wij u kunnen bereiken voor vragen.

Stuur geen gegevens van anderen mee die u bent tegengekomen. Beschrijf wat u zag, niet de gegevens zelf.

Het adres en dit beleid staan ook in security.txt op axiomatic.digital, volgens RFC 9116.

Wat wij doen, en wanneer

- **Ontvangst.** Wij bevestigen uw melding binnen drie werkdagen.
- **Beoordeling.** Wij onderzoeken de melding, bepalen de ernst volgens de klassen hieronder en laten u weten wat wij vinden.
- **Herstel.** Wij dichten een kritieke kwetsbaarheid binnen 72 uur en andere binnen 30 dagen. Lukt dat niet, dan zeggen wij u waarom en wanneer wel.
- **Op de hoogte.** Tot het lek gedicht is, houden wij u op de hoogte van de voortgang.
- **Zorgorganisaties.** Zijn door de kwetsbaarheid gegevens van een zorgorganisatie ingezien, gewijzigd of verloren gegaan, dan melden wij dat aan die organisatie zonder onredelijke vertraging, uiterlijk 24 uur nadat wij het weten, zoals de pagina Beveiliging beschrijft.
- **Erkenning.** Met uw toestemming noemen wij uw naam zodra het lek gedicht is.

Wat wij van u vragen

- Zie geen gegevens in die niet van u zijn, en wijzig of verwijder ze niet.
- Komt u gegevens van een zorgorganisatie, een medewerker of een cliënt tegen, stop dan meteen, meld het ons en bewaar er geen kopie van.
- Verstoor de dienst niet. Er wordt ook ’s nachts mee gewerkt, als er geen collega is om op terug te vallen.
- Test alleen met accounts die van u zijn of waarvoor u uitdrukkelijk toestemming hebt. Inora kent geen openbare aanmelding: elk account maakt een zorgorganisatie aan, via haar eigen inlog. Wilt u Inora zelf testen, vraag ons dan om toegang.
- Gebruik een kwetsbaarheid niet verder dan nodig is om haar aan te tonen.
- Maak niets openbaar voordat het lek gedicht is, en geef ons daarvoor 90 dagen na uw melding. Is het eerder gedicht, dan spreken wij samen af wanneer u publiceert.
- Doe niets wat verder gaat dan dit beleid toestaat.

Wat wij u toezeggen

Houdt u zich aan dit beleid en handelt u te goeder trouw, dan doen wij geen aangifte en stellen wij geen vordering tegen u in. Spreekt een ander u erop aan, dan verklaren wij dat u binnen dit beleid handelde. Namens anderen, zoals het Openbaar Ministerie of een zorgorganisatie, kunnen wij niet van stappen afzien.

Wij behandelen uw melding en uw gegevens vertrouwelijk, en delen uw naam alleen met uw toestemming.

Hoe wij de ernst bepalen

Klasse	Voorbeelden
Kritiek	Code op afstand uitvoeren; het inloggen omzeilen; toegang tot de omgeving van een andere organisatie; op grote schaal gesprekken, rapportages of documenten inzien; sleutels of geheimen buitmaken.

Klasse	Voorbeelden
Hoog	Binnen een organisatie meer rechten krijgen dan het eigen account geeft; de gesprekken van een andere medewerker inzien; opgeslagen cross-site scripting; SQL- of commando-injectie; Inora laten antwoorden buiten de bronnen van de organisatie of laten oordelen over een cliënt.
Middel	Cross-site request forgery; gegevens zonder gevoelige inhoud die uitlekken; fouten in toegangsrechten met beperkte gevolgen.
Laag	Te uitgebreide foutmeldingen, ontbrekende beveiligingsheaders en andere afwijkingen van goede praktijk met weinig gevolgen.

Wij kijken naar wat een aanvaller in de praktijk kan bereiken, niet alleen naar het type fout. Gaat het om gegevens van cliënten, dan wegen wij de melding zwaarder.