



Responsible disclosure

Doc.no **03906** | Versie **001** | Verantwoordelijke **Koen Verhulst**

Samenvatting

Via responsible disclosure moedigt het ziekenhuis onderzoekers, leveranciers en andere betrokkenen aan om mogelijke kwetsbaarheden in de IT-systemen en de digitale toepassingen **vertrouwelijk en zonder misbruik** te melden. Het ziekenhuis engageert zich om zulke meldingen zorgvuldig te behandelen, gepast op te volgen en samen te werken aan een oplossing.

Doelstelling

De doelstelling van deze procedure is het op een veilige, gecontroleerde en wettelijk conforme manier mogelijk maken van het melden en opvolgen van kwetsbaarheden in de informatiesystemen van het ziekenhuis, met als doel schade aan patiëntenzorg, persoonsgegevens en IT-systemen te voorkomen.

Toepassingsgebied

Indicatie

Dit Responsible Disclosure Agreement beleid is van toepassing op kwetsbaarheden in:

- IT-systemen
- Digitale toepassingen

Tegenindicatie

Dit Responsible Disclosure Agreement beleid is niet van toepassing op:

- Fysieke toegangen, zoals toegangen tot gebouwen en/of afgeschermd infrastructuur
- Social engineering-aanvallen en/of phishing-varianten gericht op medewerkers
- Het uitvoeren van aanvallen die de beschikbaarheid van onze systemen verstoren (bv. DDoS-aanvallen)
- Geautomatiseerde kwetsbaarheidsscans zonder voorafgaande toestemming

Definities en afkortingen

- DDoS-aanvallen: Een DDoS-aanval (Distributed Denial of Service) is een cyberaanval waarbij een website, server of netwerk wordt overspoeld met een enorme hoeveelheid nepverkeer vanaf talloze besmette apparaten (een botnet). Hierdoor raakt de infrastructuur overbelast en wordt de dienst traag of onbereikbaar voor legitieme gebruikers.

Procedure

Responsible Disclosure Agreement

OLV van Lourdes Ziekenhuis Waregem draagt de veiligheid van haar systemen en de informatie die wordt opgeslagen en verwerkt binnen het ziekenhuis in het hoogste vaandel. Echter is het steeds mogelijk dat er kwetsbaarheden zijn in haar systemen, ondanks het feit dat haar medewerkers alles in het werk stellen om deze te beschermen. We vragen om zulke kwetsbaarheden steeds te melden



Responsible disclosure

Doc.no **03906** | Versie **001** | Verantwoordelijke **Koen Verhulst**

wanneer je ze ontdekt. Zo help jij ons ziekenhuis om deze kwetsbaarheden snel en met adequate maatregelen af te dekken en om de veiligheid van onze systemen en gegevens te waarborgen.

Wij vragen jou zo snel mogelijk contact op te nemen via het

mailadres cybersecurity@ziekenhuiswaregem.be wanneer je een kwetsbaarheid ontdekt.

Gevraagde inhoud van melding

- Een gedetailleerde beschrijving van de kwetsbaarheid.
- De genomen stappen om de kwetsbaarheid te ontdekken met als doel dat wij deze kunnen reproduceren en zo snel mogelijk kunnen oplossen.
- Eventuele bewijsstukken, zoals screenshots, logbestanden of codefragmenten.
- Jouw contactgegevens zodat OLV van Lourdes Ziekenhuis Waregem contact kan opnemen om samen te werken aan een oplossing voor de gevonden kwetsbaarheid.

Minimumvereisten:

- Naam
- E-mailadres en/of telefoonnummer

Indien je anoniem wenst te blijven, kan je gebruik maken van een pseudoniem en een tijdelijk e-mailadres, zolang we in staat zijn om jou te contacteren indien we bijkomende vragen hebben.

Opgelegde beperkingen

- **Het is strikt verboden om schade te veroorzaken aan onze systemen en gegevens.**
Dit omvat, maar is niet beperkt tot het gebruik van de gevonden kwetsbaarheid om onze systemen aan te passen, gegevens te verwijderen of toegang te krijgen tot gegevens die niet voor jou bedoeld zijn.
- **Veroorzaak minimale impact**
Test de kwetsbaarheid enkel op zo'n manier dat het de werking van onze systemen zo min mogelijk verstoort.
- **Het is strikt verboden om de kwetsbaarheid te openbaren**
De kwetsbaarheid mag slechts openbaar gemaakt worden (dit omvat ook het delen met anderen) nadat deze is opgelost en wij schriftelijke toestemming geven hiervoor.
- **Noodzakelijke toegang**
Beperk jouw handelingen om de kwetsbaarheid aan te tonen tot het absolute minimum dat strikt noodzakelijk is voor het aantonen van de kwetsbaarheid.
- **Het is strikt verboden om destructieve methoden te gebruiken**
Gebruik geen technieken zoals social engineering (phishing, spam, vishing, etc.), fysieke toegang, DDoS-aanvallen of andere tools die gegevens vernietigen of de beschikbaarheid van onze diensten verhinderen/vermoeilijken.
- **Werk ethisch en verantwoordelijk**
Hou rekening met zowel de Belgische, Europese, als lokale wetgeving en voer jouw handelingen uit binnen de grenzen van de geldende regelgeving. Wis na het melden van de kwetsbaarheid alle gegevens die zijn verkregen tijdens jouw onderzoek.

Wat doen wij met jouw melding?

- We behandelen jouw melding vertrouwelijk en delen jouw persoonlijke gegevens niet zonder jouw expliciete schriftelijke toestemming.
- Indien je je houdt aan bovenstaande voorwaarden en beperkingen van het Responsible Disclosure Agreement beleid en geen andere inbreuken hebt begaan, zullen wij geen juridische stappen ondernemen tegen jou.
- Wij bevestigen binnen 10 werkdagen dat we jouw melding hebben ontvangen.



Responsible disclosure

Doc.no **03906** | Versie **001** | Verantwoordelijke **Koen Verhulst**

- We onderzoeken jouw melding verder en bepalen er de ernst en de impact van
- We houden jou transparant op de hoogte van de voortgang van het oplossen van het probleem. We behouden ons het recht voor om meldingen van lagere kwaliteit te negeren.
- We lossen de kwetsbaarheid zo snel mogelijk op.
- Indien je het wenst, kunnen we jou vermelden als ontdekker van de kwetsbaarheid in onze rapportage.

Indien je vragen zou hebben over dit beleid, staat het jou steeds vrij contact op te nemen met ons op het mailadres cybersecurity@ziekenhuiswaregem.be. Gelieve bij twijfel over de toepasbaarheid van dit beleid steeds voorafgaand aan het testen van onze systemen contact op te nemen met ons op bovenstaand mailadres om expliciete toestemming te vragen.

Toepasselijk recht

Het Belgisch recht is van toepassing op geschillen in verband met de toepassing van dit beleid.

Geldigheidsduur

De regels opgenomen in dit beleid zijn toepasselijk vanaf 01/05/2026 totdat deze eventueel worden gewijzigd of opgeheven door OLV van Lourdes Ziekenhuis Waregem. Deze wijzigingen of opheffingen worden steeds bekendgemaakt op de website van OLV van Lourdes Ziekenhuis Waregem en zijn automatisch van toepassing 30 dagen na de bekendmaking ervan.

Opmerkingen en bijzonderheden

Referenties