

# Beveiliging niet in orde? Meld het ons. Responsible disclosure

De volgende tekst beschrijft het beleid van Rivas Zorggroep op het gebied van responsible disclosure in aanvulling op de leidraad zoals deze is beschreven door het Nationaal Cyber Security Center (NCSC).

Bij Rivas vinden we de veiligheid van onze systemen en bescherming van informatie over onze cliënten erg belangrijk. We besteden dan ook veel aandacht aan beveiliging in het onderhoud en de ontwikkeling van onze systemen. Ondanks onze zorg en inzet kan het voorkomen dat er een zwakke plek ontstaat in onze ICT-systemen. Als u denkt een zwakke plek te hebben gevonden, dan werken we graag met u samen deze situatie spoedig mogelijk op te lossen. We verzoeken u dan ook deze informatie met ons te delen .

Om misbruik van het beveiligingslek door anderen te voorkomen, vragen we u om:

- uw bevindingen te mailen naar [responsible-disclosure@rivas.nl](mailto:responsible-disclosure@rivas.nl) , indien mogelijk versleuteld.
- voldoende informatie te geven, zodat we uw melding zo effectief mogelijk kunnen behandelen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- het probleem niet te misbruiken, bijvoorbeeld door meer data te downloaden dan nodig is om de zwakheid aan te tonen of om gegevens van derden in te kijken, te verwijderen of aan te passen.
- het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen door het beveiligingslek direct na het dichten van het lek te wissen.
- geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- geen actief misbruik te maken van het beveiligingslek.

U mag van Rivas verwachten dat we:

- binnen drie werkdagen op uw melding reageren met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- wanneer u zich heeft gehouden aan bovenstaande voorwaarden geen juridische stappen tegen u ondernemen betreffende de melding.
- uw melding vertrouwelijk behandelen en uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- u op de hoogte houden van de voortgang van het oplossen van het probleem.
- in berichtgeving over het gemelde probleem, indien u dit wenst, uw naam vermelden als de ontdekker.
- als dank voor uw hulp een beloning bieden voor elke melding van een ons nog onbekend

beveiligingsprobleem. De hoogte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding.

Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

- Het beleid voor responsible disclosure is geen uitnodiging om onze ICT-systemen actief te scannen om zwakke plekken te ontdekken. Rivas monitort zelf haar ICT-systemen.

Wij willen de volgende personen bedanken voor het ontdekken en delen van kwetsbaarheden op onze website of systemen. Samen hebben wij gewerkt aan een oplossing.

- Luuk van Beek (2018)
- Huy Kha, Twitter: @huykha10 (2017)
- Daniel Bakker (2016)
- Vishnu Medarametla (2016)
- Harika Naidu, LinkedIn: [www.linkedin.com/in/haarikavi/](https://www.linkedin.com/in/haarikavi/); (2018)