

### Responsible Disclosure

In de GGD Zeeland organisatie vinden wij de veiligheid van onze digitale systemen erg belangrijk. Ondanks onze zorg voor de beveiliging hiervan, kan het voorkomen dat zich daarin toch een zwakke plek bevindt. Vindt u zo'n zwakke plek, laat dat ons dan weten. Om zo snel mogelijk maatregelen te kunnen nemen, werken wij graag met u samen. Daardoor kunnen wij onze klanten en onze systemen beter beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar [informatieveiligheid@ggdzeeland.nl](mailto:informatieveiligheid@ggdzeeland.nl)
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van anderen te verwijderen of aan te passen.
- De kwetsbaarheid niet met anderen te delen totdat het is opgelost.
- Geen gebruik te maken van fysieke beveiliging, social engineering of een distributed denial of service aanval.
- Ons voldoende informatie te geven om de kwetsbaarheid te kunnen reproduceren, zodat wij het zo snel mogelijk kunnen oplossen. 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 informatie nodig zijn.

Wat wij beloven:

- Wij reageren binnen 2 weken op uw melding. U krijgt van ons een beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij ondernemen geen juridische stappen aangaande uw melding, mits u zich aan bovenstaande voorwaarden houdt.
- Wij behandelen uw melding vertrouwelijk en delen uw gegevens zonder uw toestemming niet met derden.
- Wij houden u op de hoogte van de status van de kwetsbaarheid.
- Wij vermelden indien u dit wenst, uw naam als de ontdekker in berichtgeving over de gemelde kwetsbaarheid.
- Wij streven ernaar om alle kwetsbaarheden zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat deze is opgelost.

### Security acknowledgements

GGDZeeland encourages the responsible disclosure of security vulnerabilities. Due to current affairs GGD Zeeland is not able to reply and take action in all the vulnerability calls. GGD Zeeland would like to thank the following individuals and organisations for responsibly disclosing a security vulnerability in a GGD Zeeland online service. To be eligible for this list, you must be first to responsibly disclose the issue, and you must allow us a reasonable amount of time to address the issue before publishing the information.

- NAAM ethisch hacker

### Vertaling:

GGDZeeland moedigt de verantwoordelijke onthulling van beveiligingsrisico's aan. Vanwege actuele zaken kan GGD Zeeland niet reageren op alle meldingen die kwetsbaar zijn. GGD Zeeland wil de volgende personen en organisaties bedanken om verantwoordelijk te zijn voor een beveiligingslek in een GGD Zeeland online dienst. Om in aanmerking te komen voor deze lijst, moet u eerst het probleem oplichten en u moet ons een redelijke hoeveelheid tijd geven om het probleem aan te pakken voordat u de informatie publiceert.