Responsible disclosure policy

Windesheim wil zorgvuldig omgaan met haar gegevens en daarom is veiligheid belangrijk. Ondanks alle inzet om onze systemen veilig te maken is het mogelijk dat er zwakke plekken in onze beveiliging zijn ontstaan.

Mocht je zo'n zwakke plek in één van onze systemen constateren dan willen we graag met je samenwerken om deze situatie zo spoedig mogelijk op te lossen. We verzoeken je dan ook deze informatie met ons te delen.

Om misbruik van het datalek te voorkomen vragen we jou om je aan deze richtlijnen te houden:

1. Meld het probleem door een email te sturen naar CSIRT@windesheim.nl.
2. Maak geen actief misbruik van het beveiligingslek.
3. Deel informatie over dit lek niet met anderen totdat het lek hersteld is en wis alle gegevens die eventueel door het lek verkregen zijn.
4. Maak geen gebruik van aanvallen op de fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
5. Geef voldoende informatie zodat wij het probleem kunnen reproduceren en het zo snel mogelijk kunnen oplossen.

Wanneer jij je aan de bovenstaande richtlijnen houdt zeggen wij toe:

1. Dat we er naar streven om binnen vijf werkdagen contact met je op te nemen met een inschatting van de herstelperiode.
2. Geen juridische stappen tegen jou te ondernemen betreffende de melding.
3. Jouw melding vertrouwelijk te behandelen en jouw persoonsgegevens niet zonder jouw toestemming met derden te delen, tenzij hiervoor een wettelijke verplichting geldt. Onder pseudoniem/anoniem melden is mogelijk.
4. Jou op de hoogte te houden over de voortgang van de oplossing van het probleem.
5. Indien je dat wenst, in eventuele berichtgeving over dit probleem jou als ontdekker ervan te noemen.

We streven ernaar geconstateerde beveiligingslekken zo spoedig mogelijk op te lossen. Mocht je nadat het probleem is opgelost hierover willen publiceren dan worden wij graag betrokken bij publicatie.