Responsible Disclosure

Bij Curio vinden wij de veiligheid van onze informatie, ons bedrijfsnetwerk, informatiesystemen en onze producten erg belangrijk. Ondanks dat wij veel zorg besteden aan informatiebeveiliging, kan het voorkomen dat je een zwakke plek ontdekt. Indien dat het geval is, dan horen wij dit graag zo snel mogelijk, zodat we snel maatregelen kunnen treffen.

Dit beleid is geen uitnodiging om ons bedrijfsnetwerk of onze informatiesystemen uitgebreid actief te scannen op zwakke plekken. Wij monitoren ons netwerk zelf. Als wij het vermoeden hebben dat de zwakheid of gegevens misbruikt worden, of dat kennis over de zwakheid met anderen is gedeeld, zullen wij hiervan aangifte doen. Zie deze link voor meer informatie hierover.

Wij vragen je

- Bevindingen zo snel mogelijk te mailen naar privacy@curio.nl, geef ons voldoende informatie om het probleem te reproduceren;
- Deel het probleem niet met anderen totdat het is opgelost;
- Maak geen gebruik van aanvallen op fysieke beveiliging (forceren van ruimtes);
- Maak geen gebruik van social engineering, SPAM of phishing mails en dergelijke om studenten of medewerkers van Curio te misleiden;
- Maak geen gebruik van applicaties van derden (hacking tools, kwetsbaarhedenscanners etc.)
- Maak geen gebruik van dDos aanvallen (distributed denial of service);
- Misbruik de zwakheid niet voor het downloaden, veranderen of verwijderen van gegevens.

Wat wij beloven:

- Elk vermoeden van een kwetsbaarheid zullen wij nader onderzoeken;
- Wij reageren altijd op de melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Wij behandelen de melding vertrouwelijk en zullen jouw persoonlijke gegevens niet zonder toestemming met derden delen. Een uitzondering hierop is politie en justitie, in geval van aangifte of indien gegevens worden opgeëist;
- In berichtgeving over het gemelde probleem zullen wij, indien gewenst, jouw naam vermelden als de ontdekker;
- Als dank voor de hulp bieden wij een beloning voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte 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, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over het probleem, nadat het is opgelost.

Met dank aan Floor Terra voor de voorbeeldtekst op http://responsiblediscloure.nl/