Responsible Disclosure

Bij Landstede Groep vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met je samenwerken om (digitale) omgeving van Landstede Groep beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen te mailen naar sert@landstedegroep.nl;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen of informatie van andere leerlingen, docenten of andere medewerkers in te kijken, verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen en alle informatie die is verkregen na het verhelpen van het lek te wissen;
- Geen gebruik te maken van aanvallen op fysieke beveiliging, spam, malware, applicaties van derden of andere aanvalstechnieken;
- Voldoende informatie te geven zodat wij het probleem 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 nodig zijn.

Wij beloven dat:

- We geen juridische stappen* nemen.
- We reageren binnen vijf werkdagen.
- Wij behandelen je melding vertrouwelijk.
- Wij houden je op de hoogte van de voortgang.

* Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat je tijdens jouw onderzoek handelingen uitvoert die strafbaar zijn. Het feit dat Landstede Groep geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.