Wat te doen bij het vinden van een zwakke plek in één van onze systemen?

Responsible Disclosure

Clusius College

Opgesteld door	N. Enklaar
Versie / Datum	1.0
Bronvermelding	Floor Terra (responsibledisclosure.nl), Kennisnet
Vastgesteld (door / d.d.)	

Responsible Disclosure

Bij het Clusius College vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Als je 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 de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

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 je 'zoektocht' een handeling uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat het Clusius College geen aangifte tegen je zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar je handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

Meld de kwetsbaarheid voordat je dit aan de buitenwereld kenbaar maakt. Zo kunnen wij eerst maatregelen treffen. Dit heet Responsible Disclosure.

Wij vragen jou:

- Je bevindingen te mailen naar privacy@clusius.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, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via de lek direct na het verhelpen van de lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging en de internetvoorziening van de school;
- De school voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wat wij doen:

- Wij reageren binnen 5 werkdagen op je melding en geven aan wat we zullen doen om de kwetsbaarheid aan te pakken;
- Als je de kwetsbaarheid netjes gemeld hebt en via bovenstaande stappen hebt gehandeld zullen wij geen juridische stappen tegen je ondernemen met betrekking tot de melding en geen melding maken bij de politie;
- Wij behandelen je melding vertrouwelijk en zullen je persoonlijke gegevens niet zonder jouw toestemming met anderen delen tenzij dit wettelijk verplicht is. Melden onder een pseudoniem is mogelijk;
- Wij houden je op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid.