Responsible Disclosure leerlingen en volwassenen

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1.0	Maart 2019	L. van den Heuvel	
2.0	Juni 2026	Kennisnet/L. van den Heuvel	

Vaststelling

Naam	Functie	Versie	Datum
M.B. van den Berg	Directeur-bestuurder	2.0	Juni 2026

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld, wordt ook op de websit(s) vermeld in voettekst.

Responsible Disclosure

Bij het Christiaan Huygens College (CHC) 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 is. Heeft u een zwakke plek in één van onze systemen heeft gevonden? Dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij werken graag met u samen om onze gebruikers en onze systemen beter te kunnen beschermen.

Hoe kan men een zwakke plek in een ICT-systeem van het Christiaan Huygens College (CHC) melden (Responsible Disclosure)?

Een zwakke plek in een ICT-systeem van CHC, kunt u melden aan systeembeheer van CHC. U kunt dit melden via de e-mailadressen:

Frits Philips lyceum-mavo:	*helpdesk@fritsphilips.eu*
Huygens Lyceum:	*ict.hl@huygenslyceum.nl*
Olympia (incl. Onderwijsbureau):	*helpdesk@huygenscollege.nl*
Bestuur/Privacy-team:	*privacy@huygenscollege.nl*

Leerlingen kunnen de melding ook via een mentor of iemand van de schoolleiding doorgeven. Meld de kwetsbaarheid voordat u dit aan de buitenwereld kenbaar maakt. Zo kan CHC eerst maatregelen treffen. Dit heet Responsible Disclosure. Ook wordt de term Coördinated Vulnerability Disclosure (CVD) wel gebruikt.

Waar u aan moet denken bij Responsible Disclosure

Als u een melding doet van een kwetsbaarheid in een ICT-systeem, denk dan aan de volgende zaken:

- Geef voldoende informatie om het probleem te reproduceren. Zo kan CHC het probleem zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij ingewikkeldere kwetsbaarheden kan meer nodig zijn.
- Als u de melding versleuteld wilt versturen, meld dit dan bij ons zodat we u instructies kunnen geven.
- Laat contactgegevens (e-mailadres of telefoonnummer) achter zodat CHC met u contact kan opnemen.
- Doe de melding zo snel mogelijk na ontdekking van de kwetsbaarheid.
- De kwetsbaarheid niet te misbruiken, geen data te downloaden, of (persoons)gegevens van derden 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 fysieke beveiliging, social engineering, distributed denial of service (DDoS), spam of applicaties van derden.
- Ga verantwoordelijk om met de kennis over het beveiligingsprobleem. Verricht geen handelingen die verder gaan dan wat nodig is om het beveiligingsprobleem aan te tonen.

Voldoet u bij uw melding aan deze voorwaarden? Dan verbindt CHC geen juridische consequenties aan de melding.

Maak geen misbruik van een zwakke plek in een ICT-systeem

Als u een kwetsbaarheid ontdekt, maak hier dan geen misbruik van. Bijvoorbeeld door:

- Malware te plaatsen;
- Gegevens in een systeem te kopiëren, wijzigen of verwijderen (een alternatief hiervoor is een directory listing maken van een systeem);
- Veranderingen aan te brengen in het systeem;
- Herhaaldelijk toegang te verkrijgen tot het systeem of de toegang te delen met anderen;
- Gebruik te maken van het zogeheten 'bruteforcen' van toegang tot systemen;
- Gebruik te maken van denial-of-service of social engineering.

Wat het Christiaan Huygens College doet bij Responsible Disclosure

Heeft u een melding gedaan van een zwakke plek in een ICT-systeem? CHC behandelt deze melding als volgt:

- U krijgt binnen 1 werkdag een ontvangstbevestiging van CHC.
- CHC reageert binnen 3 werkdagen op uw melding. Deze reactie bevat een beoordeling van de melding en een verwachte datum voor een oplossing.
- CHC houdt u als melder op de hoogte van de voortgang van het oplossen van het probleem.
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen met betrekking tot de melding*.
- CHC lost het beveiligingsprobleem zo snel mogelijk op, maar uiterlijk binnen 60 dagen. CHC zal samen met u bepalen of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost.
- CHC biedt mogelijk een beloning als dank voor de hulp.
- CHC behandelt uw melding vertrouwelijk. CHC deelt persoonlijke gegevens niet zonder toestemming van u met derden. Behalve als dit wettelijk of door een rechterlijke uitspraak verplicht is. CHC kan, als u dat wilt, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

*Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Het is onze eigen verantwoordelijkheid om ons netwerk monitoren. Er bestaat een kans dat u tijdens uw onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat CHC geen aangifte tegen u zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar uw handelen gehouden kan worden dan wel dat u strafrechtelijk kunt worden veroordeeld.