GRAFISCH LYCEUM UTRECHT

Datum	1 april 2021
Versie	1.0 definitief
Auteur(s)	Wim Arendse

Kerngegevens

Documenteigenaar: CvB

Documentbeheerder: Kwaliteitsadviseur IBP

Review door: Barend de Ruijter, Koen Hillen, Martin Roberti, Paul 't Lam

Status: definitief

Samenvatting: Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze IT-beveiliging. Daarmee kunnen we mogelijke schade voorkomen en we kunnen ervan leren. Het beleid Responsible Disclosure regelt de voorwaarden en werkwijze rondom melding en afhandeling van kwetsbaarheden.

Verantwoording: Dit document is gebaseerd op de tekst van het Responsible Disclosure model mbo vs 2.0 (IBPDOC27, saMBO-ICT) en de tekst door Floor Terra (responsiblediscloSure.nl).

Versie-beheer

Versie	***Datum***	***Auteur***	***Opmerking***	***Vastgesteld door***	***Datum***
0.99	19-02-2021	Wim Arendse	Definitief, vast te stellen door CvB		
1.0	01-04-2021	Paul 't Lam	Gemelde kwtsbaarheden worden gerapporteerd aan het CvB en beheerder document is verantwoordelijk voor de communicatie	CvB	29-03-2021

GRAFISCH LYCEUM UTRECHT

Inhoud

1 Inleiding

1.1 Achtergrond

Hackers die, gedreven door nieuwsgierigheid, lekken vinden in de IT-systemen van organisaties, bevinden zich vaak in een juridisch grijs gebied. Ook al hebben ze geen kwade bedoelingen, het is vaak niet aantrekkelijk om de instelling te informeren over het lek. Organisaties pakken meldingen niet altijd op en het gebeurt soms dat een melder te maken krijgt met strafrechtelijke gevolgen. Dit beleid geeft helderheid over de spelregels voor de melder en over hoe het GLU een melding oppakt en afhandelt.

Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze IT-beveiliging. Daarmee kunnen we mogelijke schade voorkomen en we kunnen ervan leren. Het Responsible disclosure document regelt de voorwaarden en werkwijze rondom melding en afhandeling van kwetsbaarheden.

1.2 Doel

Doel van Responsible disclosure beleid is:

- de mogelijkheid bieden om op ethisch verantwoorde wijze kwetsbaarheden in de systemen van het GLU onder de aandacht te brengen,
- het verbeteren van kwetsbaarheden in de systemen van het GLU.

1.3 Reikwijdte

Dit Responsible disclosure beleid is van toepassing op alle informatiesystemen en de hele infrastructuur die onder het beheer van het GLU vallen. Daarom is dit is een openbaar document en is het bedoeld voor alle geïnteresseerden.

1.4 Context

Responsible disclosure beleid komt mede voort uit het IBP-beleid GLU (beleidsregel 8) en heeft een relatie met:

- Incidentbeheer en -registratie GLU

1.5 Communicatie over de richtlijn

De Kwaliteitsadviseur IBP is verantwoordelijk dat het Responsible disclosure beleid wordt gecommuniceerd naar de afdeling communicatie, de medewerkers ICT en baliemedewerkers. Via de website van het GLU is Responsible disclosure beschikbaar voor alle belangstellenden, ook buiten de organisatie.

Worden er wijzigingen aangebracht in het Responsible disclosure beleid? Dan zorgt de Kwaliteitsadviseur IBP ervoor dat de nieuwe versie van Responsible disclosure op de website wordt geplaatst.

1.6 Vaststelling en beheer

Het Responsible disclosure beleid is op 29-03-2021 vastgesteld door het CvB van het GLU.

Het beheer van dit document ligt bij de Kwaliteitsadviseur IBP. De Commissie IBP evalueert en actualiseert deze richtlijn een keer per jaar. Zijn er wijzigingen in wet- en regelgeving, wijzigingen in de gehanteerde normen of nieuwe ontwikkelingen, dan past de Kwaliteitsadviseur IBP het beleid eerder aan. Dat gebeurt ook als daar om een andere reden aanleiding voor is.

2 Reponsible Disclosure

Het GLU vindt de veiligheid van haar systemen en het verhelpen van kwetsbaarheden in die systemen belangrijk. Ondanks onze zorg voor de beveiliging van de systemen kan het voorkomen dat er toch een zwakke plek is. We werken daarin graag samen met degene die een kwetsbaarheid ontdekt en/of bij ons meldt. Dit beleid wordt op onze website gepubliceerd in Nederlands en Engels.

Wij vragen van de melder:

- De bevindingen te mailen naar ibp@glu.nl. Versleutel gevoelige informatie eventueel om te voorkomen dat de informatie in verkeerde handen valt.
- Voldoende informatie te geven om het probleem te reproduceren, zodat wij het 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.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken of te veranderen of verwijderen en extra voorzichtig te zijn bij persoonsgegevens.
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen direct te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, applicaties van derden, social engineering, distributed denial of service of spam, of op een andere manier ons netwerk uitgebreid actief te onderzoeken/scannen op kwetsbare plekken. Het GLU monitort het netwerk en de kans is groot dat de scan of aanval wordt gedetecteerd en dat er vervolgens onnodige kosten worden gemaakt.

Wij beloven aan de melder:

- Het GLU neemt geen juridische stappen tegen de melder als hij/zij zich houdt aan de bovenstaande voorwaarden.
- Wij reageren binnen vijf dagen op een melding.
- Wij houden de melder op de hoogte van de voortgang van het oplossen van het probleem,
- Wij behandelen een melding vertrouwelijk en delen geen persoonlijke gegevens van de melder met derden zonder zijn/haar toestemming, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Anoniem of onder een pseudoniem melden is mogelijk.
- In berichtgeving over het gemelde probleem vermelden wij de naam van de melder als de ontdekker, als hij/zij dat wenst.
- Wij kunnen je een beloning geven voor je onderzoek, maar zijn hiertoe niet verplicht. Je hebt dus niet zonder meer recht op een vergoeding. De vorm van deze beloning staat niet van tevoren vast en wordt door ons per geval bepaald. Of we een beloning geven en de vorm waarin dat gebeurt, hangen af van de zorgvuldigheid van je onderzoek, de kwaliteit van de melding en de ernst van het lek.

Meldingen van mogelijke kwetsbaarheden (responsible disclosure) in de IT-beveiliging van de GLU die worden gemeld, worden gerapporteerd aan het CvB.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en alle betrokken partijen op de hoogte te houden over de voortgang. Het GLU wordt graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Bijlage 1: Tekstvoorbeeld webpagina

Responsible disclosure

Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden in onze beveiliging ontdekken en bij ons melden. Daar kunnen we van leren en mogelijke schade voorkomen. Meld de kwetsbaarheid voordat je deze aan de buitenwereld kenbaar maakt, zodat we eerst maatregelen kunnen treffen. Als een ethisch hacker aan de onderstaande regels voldoet, doen wij geen aangifte bij het openbaar ministerie.

Wat we van jou vragen:

- Ons zo snel en volledig mogelijk te informeren, via ibp@glu.nl
- Geen openbaarmaking of misbruik/wijziging van onze gegevens
- De bevindingen niet te delen met anderen

Wat we beloven

- We nemen geen juridische stappen
- We reageren binnen 5 dagen
- We handelen dit vertrouwelijk af
- We houden jou op de hoogte

Lees hier ons volledige beleid voor responsible disclosure

Bijlage 2: Tekstvoorbeeld webpagina Engels

Responsible disclosure in English

Hackers may discover (in ethically responsible manner) discover and report vulnerabilities in our IT-security. If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. This helps us learn and avoid possible damage. If you as ethical hacker abide the stated rules, we will not take legal action against you in regard to the report.

What we ask

- Email your findings to ibp@glu.nl in a safe manner
- Do not take advantage of the vulnerability
- Do not reveal the problem to others

What we promise

- We will not take legal action
- We respond within five days
- We will handle your report with strict confidentiality
- We will keep you informed of the progress towards resolving the problem

Read our full policy for responsible disclosure

Bijlage 3: Responsible Disclosure Engels

2.1 Introduction

Hackers who, driven by curiosity, find vulnerabilities or leaks in the IT-systems of organisations, can often find themselves in a legal grey zone. They may not have bad intentions, but even then it is not always appealing to report the leak to an organisation. Organisations do not always follow up on such reports and sometimes the notifier faces legal consequences. This policy helps to eliminate ambiguities. It states the rules of play to the notifier and explains how the GLU handles the case.

2.2 Reponsible Disclosure

At the GLU we consider the security of our systems a top priority. However, no matter how much effort we put into system security, there can still be vulnerabilities present. If anyone discovers a vulnerability, we would like to know about it, so we can take steps to address it as quickly as possible, to help us better protect our systems. This policy is published in Dutch and English on the website of the GLU.

What we ask

- Email your findings to ibp@glu.nl. Encrypt sensitive information to prevent critical information from falling into the wrong hands.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Do not reveal the problem to others until it has been resolved.
- Do not use attacks on our physical security, social engineering, distributed denial of service, spam or applications of third parties, or scan our network in any other way to find vulnerabilities. The GLU monitors the network and it is very likely that this is detected, which leads to unnecessary costs.

What we promise

- The GLU will not take legal action if the instructions for reporting as stated above, are followed.
- We will respond to the report within five days.
- We will keep the notifier informed of the progress towards resolving the case.
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission, unless we are required to meet legal obligations. It is possible to report anonymous or using a pseudonym.
- In the public information concerning the problem reported, we will state the name of the notifier as the discoverer of the problem (unless he/she desires otherwise).

Vulnerabilities (hacks) in the IT security of the GLU that are reported will be reported to the CvB at all times.

We strive to resolve all problems as quickly as possible. The GLU would like to play an active role in the ultimate publication on the problem after it is resolved.

2.3 Evaluation of policy

This policy will be reviewed by the security and privacy commission every year and adjusted when required.

Bijlage 4: Relatie met saMBO-ICT Toetsingskader IBP/E

Met deze versie van het Responsible disclosure beleid GLU en de implementatie en naleving daarvan geeft het GLU invulling aan deze Statements uit het saMBO-ICT Toetsingskader Informatiebeveiliging, Versie 4.2:

Nr.	Statement
2.6	**Rapportage van zwakke plekken in de informatiebeveiliging (ISO 16.1.3)** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.