1 RESPONSIBLE DISCLOSURE GELDMAAT

To keep our systems secure & reliable Geldmaat continuously works towards optimising the security posture and procedures. Nevertheless it might still be possible that some vulnerabilities exist. In case you found one, Geldmaat would appreciate reporting this and therefor realised this Responsible Disclosure procedure.

2 SCOPE

You can report all kinds of technical vulnerabilities in our systems; for example: Cross Site Scripting (XSS), SQL-Injection and crypto-related issues. For reporting outages, fraud, phishing emails and other topics please use our regular contact-form instead.

3 RULES OF ENGAGEMENT

The Geldmaat Responsible Disclosure procedure is based on the 'Guideline Responsible Disclosure' of the Dutch National Cyber Security Centre, resulting in the following Rules of Engagement:

- Do not use social engineering attacks to gain information/access
- Do not use brute force attacks to gain information/access
- Do not place backdoors or any other malicious software on compromised systems
- Do not make any changes to compromised systems
- Do not download or copy any Geldmaat data besides a minimum set to proof the vulnerability; like a screenshot or directory-listing
- Try to be as unintrusive and undisruptive as possible, only performing the minimum set of actions to proof the vulnerability; do not continue the attack after the initial compromise.

4 REPORTING AN ISSUE

You can send your report to: contact@geldmaat.nl. In this email, please provide a detailed list of steps taken to perform the attack (so we can try and reproduce/verify the issue at hand), including the target IP/URL/system name.

We will try & reply to your report within 3 workdays.

5 PLAYING BY THE RULES

Performing cyberattacks is considered a crime in most countries, including The Netherlands. In case you carefully followed the Rules of Engagement described here and reported the

vulnerability in good faith, Geldmaat will not report this to the authorities nor will we sue for damages.

Please note the Dutch government can always decide to start an investigation whenever it deems necessarily, even when Geldmaat decided not to report/pursue the issue.

As a positive incentive to report vulnerabilities in a responsible fashion, and as a token of our appreciation, Geldmaat might offer a small reward in return for reporting (serious, non low-hanging fruit) vulnerabilities, assuming the Rules of Engagement are followed and the vulnerability could be reproduced. The reward depends on the type of vulnerability and is only awarded for new, yet unknown vulnerabilities (i.e. to the first reporter).

Although still appreciated, Geldmaat does not offer rewards for reporting 'low hanging fruit' issues. Geldmaat employees, including it's suppliers, are also excluded from receiving these rewards.

6 PRIVACY

Geldmaat will only use your personal information to get in contact with you and to undertake actions with regard to your reported vulnerability. We will not distribute your personal information to third parties without your permission, unless we are required to do so by law, or if an external organisation takes over the investigation of your reported vulnerability. In that case, we will make sure that the relevant authority treats your personal information confidentially and conform the GDPR/AVG rules.