RESPONSIBLE DISCLOSURE STATEMENT

At Goede Doelen Lotterijen we consider the security of our systems a top priority. However, no matter how much effort we put into system security, there might still be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it. We would like to ask you to help us protect our clients/participants and our systems and therefore to notify us without delay should you have discovered a vulnerability (or problem), enabling us to take prompt measures.

If you have discovered a vulnerability, please do the following:

- Submit your findings to us by using the following URL: https://app.zerocopter.com/en/rd/53594918-f4de-44f4-96d8-3b495af1ac49 .
- Report the vulnerability as quickly as is reasonably possible, to minimise the risk of hostile actors finding it and taking advantage of it.
- Report in a manner that safeguards the confidentiality of the report so that others do not gain access to the information.
- Provide sufficient information to reproduce the problem, so we will be able to resolve it. 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.
- Always act in good faith, responsibility and with extreme care and caution when investigating the possible vulnerability.

And please don't do the following:

- Misuse any vulnerabilities.
- Cause damage while investigating vulnerabilities.
- Reveal the vulnerability to others until it is resolved.
- Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks.
- Utilise a vulnerability further than necessary to establish its existence.
- Copy, modify or delete data on the system. An alternative for doing so is making a directory listing of the system.
- Make changes to the system.
- Repeatedly gain access to the system or sharing access with others.
- Use brute force attacks, attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties to gain access to the system.

How we will treat your responsible disclosure report:

- If you have followed the instructions above, we will not take any legal action against you concerning the report.
- We will respond to your report within 5 business days after receipt of the report. In our response we will include our evaluation of the report and an expected resolution date.
- We will treat your report confidentially and will not pass on your personal details to third parties without your permission, unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible.
- We will keep you informed of the progress towards resolving the problem.
- Please note that we will be unable to contact you in case of anonymous reporting
- We will not retain any data of the person reporting if no longer necessary for resolving the issue and we will only use personal details to contact him/her in respect of the report.
- We will never go public with the reported problem before the problem has been resolved. If we make the issue public, we will give you credit for identifying it, if you wish.

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

The above procedure is based on the Responsible Disclosure Guidelines of the National Cyber Security Center of the Dutch Ministry of Security and Justice.