REGIONALE
BELASTING
GROEP

Responsible disclosure

It goes without saying that the IT systems of the Regionale Belasting Groep must be safe. This is why we pay a lot of attention to our IT security. However, you may discover a shortcoming in one of our systems. We would very much appreciate it if you report this shortcoming to us, so that we can work with you to investigate and solve the problem. It is very important, however, that you do this in a responsible way. Not only for us, but also for yourself. You may safely assume that your report does not have any legal consequences for you if you follow the guidelines below.

We ask you:

- To email your findings to info@derbg.nl.
- To make your report as soon as possible after you have discovered the vulnerability.
- Not to abuse the problem, for example, by downloading more data than is necessary for demonstrating the leak or by accessing, removing or adjusting third party data,
- Not to share the problem with others until it has been solved and to erase all data obtained through the leak immediately after the leak has been stopped,
- To provide sufficient information to reproduce the problem, so that we can solve it as soon as possible. The IP address or the URL of the affected system and a description of the vulnerability often suffice, but more may be required in the case of more complex vulnerabilities.
- To leave your contact details so that we can work with you on a safe result. We need at least an email address or telephone number of you.
- Not to make use of attacks on physical security, social engineering, distributed denial of service, spam or third party applications, and

The following acts are not permitted:

- Placing malware, neither on our systems nor on those of others.
- So-called "brute forcing" of access to systems
- Using social engineering.
- Disclosing or providing information about the security problem to third parties before the problem has been solved.
- Performing acts that go beyond what is strictly necessary for demonstrating and reporting the security problem, especially where it concerns the processing (including accessing or copying) of confidential data to which you have access as a result of the vulnerability. Instead of copying an entire database, you can usually limit yourself to e.g. copying a directory listing. Modification or removal of data in the system is never permitted.
- Using techniques that diminish the availability and/or utility of the system or services (DoS attacks).
- Abusing the vulnerability in any (other) way whatsoever.

What we promise:

- We will respond to your report with our assessment of the report and an expected date for a solution within 3 days,
- We will treat your report as confidential and will not share your personal data with third parties without your consent, unless this is necessary for performing a statutory obligation. Reporting using a pseudonym is possible,
- A period of time after which the person making the report may disclose the vulnerability, preferably 60 after reporting the problem in the case of software and six months in the case of hardware, will be agreed in that consultation.
- We will keep you informed of the progress on solving the problem.

- If you have complied with our conditions, we will not take legal action against you with regard to the report,
- If you wish, we will mention your name as the person who discovered the problem in communications about the problem, and

We aim to solve all problems as quickly as possible and would like to be involved in any publication about the problem after it has been solved.