Responsible disclosure policy

Responsible disclosure Windesheim

Windesheim wishes to handle its information with due care, which means that security is important. Despite all our efforts to secure our systems, there is a risk of vulnerabilities having crept into our security.

Should you come across such a vulnerability in one of our systems, we would like to work together with you to remedy this security issue as soon as possible. We therefore request you to share this information with us.

To prevent any abuse of the security leak, we ask you to observe the following directives:

1. Report the problem by sending an email to CSIRT@windesheim.nl.
2. Do not actively abuse the security leak.
3. Do not share any information about this leak with others until the leak has been repaired and delete all data that may have been obtained due to the leak.
4. Do not use any physical security attacks, social engineering, distributed denial of service, spam or third-party applications.
5. Provide sufficient information so that we can reproduce the problem and repair it as soon as possible.

If you observe the above-mentioned directives, we will promise:

1. To try to contact you within 5 working days to let you know how long the repair is expected to take.
2. Not to take any legal action against you following your report.
3. To treat your report confidentially and not share your personal details with any third party, unless we are legally obliged to do so. It is possible to submit your report under a pseudonym or anonymously.
4. To keep you up to date on our progress in solving this problem.
5. To mention in any publications on this problem –if you wish– that it was you who first detected and reported it.

Our efforts are focused on the soonest possible repair of any detected security leaks. Should you wish to publish any information about the detected problem after it has been solved, we would like to be involved in this publication.