Reporting vulnerabilities (CVD)

The municipality of Hof van Twente considers the security of its systems very important. Despite all precautions, it remains possible that a weak spot can be found in the systems. Have you discovered a weak spot in one of our systems? We would like to hear from you. Then we can quickly take the appropriate measures. This way of working together is called Coordinated Vulnerability Disclosure (CVD).

The fact that the municipality of Hof van Twente has a Coordinated Vulnerability Disclosure policy, is not an invitation to extensively and actively scan our corporate network for vulnerabilities. We monitor our own network. If you are investigating a vulnerability in one of our systems, please consider the proportionality of the attack.

By submitting a report, you agree to the Coordinated Vulnerability Disclosure agreements below. The municipality of Hof van Twente will handle your report according to the agreements below.

2 Reporting

Email your findings to informatiebeveiliging@hofvantwente.nl. If possible, encrypt the findings. Or send the report via secure mail. This prevents the information from revealing to not involved people. Submit the report as soon as possible after discovering the vulnerability.

We need at least the following information from you:

- Leave your details so that we can contact you. Be sure to leave an e-mail address or telephone number.
- Provide sufficient information to reproduce the problem. We can then solve it as quickly as possible. Usually you only need to send us the IP address or the URL of the affected system and a description. For an extensive vulnerability, more information may be required. For example, a Proof of Concept.

Conditions:

- You delete all confidential information obtained in your investigation. You should do this immediately after we have resolved the weakness.
- We always appreciate help in solving a problem. Provide information about the vulnerability that we can check. Avoid giving advice that amounts to advertising for other (security) products.
- Do not abuse the vulnerability by, for example:
    - Downloading more data than necessary to demonstrate the vulnerability.
    - Changing or deleting data.

3 Not permitted

The following actions are not permitted:

- You may not place malware on our systems. Nor on those of others.
- You may not "bruteforce" access to the system. This is only permitted if there is no other option. For example, to show that the security is very poor. This means that it

must be easy to crack a password with easily and cheaply available hardware and software. This password can then be used to expose the system to danger.

- You may only use social engineering if you have no other choice. You may only do this if you can demonstrate that employees who have access to sensitive data are not being careful. You must have legally persuaded employees to give this kind of data to people who should not have. It is not permitted to harm employees of the municipality.
- You may only use what you have found to demonstrate that the municipality's procedures and practices are flawed.
- You may not pass on the information about the security problem to others until we have solved the problem.
- You should only do what is really necessary to show us the security problem and report it to us. You may give us a directory listing, rather than copying an entire database. You may never change or delete data in the system.
- You may not use any techniques which impair the use and/or availability of the system or services (DoS attacks).

4 Handling of your report

What you may expect from us

- If you meet all the conditions, we will not file a criminal complaint. We will not file a civil suit against you.
- If you have not complied with these conditions, we may bring legal proceedings against you.
- We will treat the report as confidential. We will only share your personal data with others if you have given us permission to do so. We also share the data if we are obliged to do so by law. Or if this is required by a court ruling.
- Municipalities share their experiences with each other. That is why we always share the report received with the Information Security Service for Municipalities (IBD).
- You remain anonymous as the discoverer of the weak spot. If you want us to mention your name, we will do so.
- You will receive confirmation of receipt within 2 working days.
- Within 5 working days you will receive a response from us with an assessment of the report.
- We will solve your reported security problem as quickly as possible. We will keep you informed of the progress. We don't want to take longer than 90 days to fix the problem. However, we are often dependent on others to do so.
- After we have solved the problem, we can decide together whether the problem will be made public and how we will communicate this.
- We may, but are not obliged to, give you a reward for your research. The form of this reward is not fixed in advance. We determine this on a case-by-case basis. Whether we give a reward and the form this takes, depends on:
    - the diligence of your investigation
    - the quality of the report
    - the seriousness of the weakness.