HZ Responsible Disclosure Statement

At HZ University of Applied Sciences we attach a great deal of importance to the security of our systems. Despite the careful attention we pay to the security of our systems, a weak spot may be present.

If you have found a weak spot in one of our systems or procedures, we would like to be informed of this, so we can take appropriate action as quickly as possible. HZ would like to work together with you in the manner described below in order to better protect our users and systems.

We ask you to:

- Send your findings to security@HZeeland.nl. Encrypt your findings with our PGP key (fingerprint: 7D55 B928 638A CF17 6A41 2477 A0F6 67BC DC89 9C3F) to prevent the information from falling into the wrong hands.

- Not to abuse the identified problem, for example by downloading more data than is necessary to point out the leak or by changing or deleting data, and to exercise extra restraint with regards to personal data.

- Not to share the problem with others until is has been resolved and to immediately delete all confidential information acquired through the leak.

- Not to use attacks on physical security or third-party applications, social engineering, distributed denial-of-service, or spam.

- To provide sufficient information to allow us to reproduce the problem so we can solve it as quickly as possible. Usually the IP address or the URL or the affected system and a description of the vulnerability and the actions performed is sufficient, but for more complex vulnerabilities additional information may be required.

What HZ promises:

- HZ will respond to your notification within 3 working days, stating our assessment of the notification and an expected date for a solution.

- We treat your notification confidentially and will not share your personal data with third parties without your permission unless this is necessary for complying with a legal requirement.

- We keep you informed of the progress in solving the vulnerability.

- You can submit a notification anonymously or under a pseudonym. You should be aware that this means we cannot contact you about, for example, the follow-up steps, progress in closing the leak or publication.

- If you so desire, we will list your name as the discoverer of the vulnerability in our reporting on the reported weakness.

You should know:

We strive to solve all problems as quickly as possible, keep the involved parties informed and we would like to remain involved in any publication about the identified vulnerability after it has been resolved.

Bounty hunting is not appreciated. To this regard we should also point out that HZ does not, without exception, consider financial gratification for reporting a vulnerability. However, the eternal gratitude of our IT-staff will be bestowed upon you.

Additionally, HZ University of Applied Sciences does not take into consideration trivial vulnerabilities or bugs that cannot be abused. The following non-exhaustive list of examples of known and accepted vulnerabilities & risks are outside the scope of the responsible disclosure policy and which will not be met with a reply when addressed:

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and Content Spoofing/Text Injection on these pages;
- fingerprint version banner disclosure on common/public services;
- disclosure of known public files or directories or non-sensitive information, (e.g. robots.txt);
- clickjacking and issues only exploitable through clickjacking;
- lack of Secure/HTTPOnly flags on non-sensitive Cookies;
- OPTIONS HTTP method enabled;
- anything related to HTTP security headers, e.g.:
    - Strict-Transport-Security;
    - X-Frame-Options;
    - X-XSS-Protection;
    - X-Content-Type-Options;
    - Content-Security-Policy.
- SSL Configuration Issues:
    - SSL forward secrecy not enabled;
    - weak / insecure cipher suites.
- SPF, DKIM, DMARC issues;
- host header injection;
- reporting older versions of any software without proof of concept or working exploit.
- information leakage in metadata;
- Systems and protocols that can be used in DDoS attacks.
- Intentional listing of directory contents for research or publication purposes;
- Missing DNSSEC configuration.