



Vulnerability Disclosure Policy

Version 1.0 | July 2022

Confidentiality

All information in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Hansen's prior permission in writing and shall be held in safe custody. These obligations shall not apply to information, which is published or becomes known legitimately from some source other than Hansen.

Many of the product, service and company names referred to in this document are trademarks or registered trademarks.

They are all hereby acknowledged.

Copyright

© Hansen Technologies Ltd 2022, all rights reserved.

Issue History			
Version	Date	Description of Reissue / Modification	Approved by
0.1	Sept 2021	Initial Document	
1.0	July 2022	Published Document	

Table of Contents

1.	Introduction	2
2.	Reporting	2
3.	What to expect	2
4.	Guidance.....	3
4.1	You must not:	3
4.2	You must:.....	3
5.	Legalities	3

1. Introduction

Hansen's customers rely on the solutions provided by Hansen to safeguard information and prevent any unauthorised access to the data stored in these solutions. We take extensive measures to deliver secure products, and minimise any security risks to our systems but appreciate the fact that vulnerabilities in products cannot be avoided entirely.

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us (the "Organisation"). We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always act in compliance with it.

2. Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following link/email:

vulndisclosure@hansencx.com

In your report please include details of:

- The website, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example; "XSS vulnerability".
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.

3. What to expect

After you have submitted your report, we will respond to your report within 10 working days and aim to triage your report within 20 working days. We'll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

4. Guidance

4.1 You must not:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in the Organisation's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt the Organisation's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.
- Submit reports detailing SSL/TLS configuration weaknesses, for example "weak" cipher suite support or the presence of support for legacy SSL/TLS.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, 'phish' or physically attack the Organisation's staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

4.2 You must:

- Always comply with data protection rules and must not violate the privacy of the Organisation's users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).
- Securely delete all Personally Identifiable Information (PII) data retrieved during your research as soon as disclosure has occurred.

5. Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organisation or partner organisations to be in breach of any legal obligations.