Vulnerability Disclosure Policy

Document Type	Policy
Document owner	Jonas Bruun Jacobsen, Chief Technology Officer, BeCause ApS
Approved by	Management Board
Approval date	January 2024
Review date	January 2024
Version	2.0
Amendments	January 2024
Related to	-

1. Introduction

BeCause ApS (the “Company”) offers companies a completely different approach to their sustainability information management infrastructure. Instead of collecting, coordinating, and communicating sustainability information via a complex, fragmented and manual stack of files, mails, and niche-purposed systems, we're a unified single source of truth and automated data hub for our customers, taking away 100% of the pain of management fragmentation. It's faster, safer, simpler, and above all, way better.

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

We value those who take the time and effort to report security vulnerabilities according to this policy.

2. Reporting

If you believe you have found a security vulnerability, please let us know by emailing us at privacy@because.eco.

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 aim to respond to you promptly, usually within 5 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

This policy is applicable to because.eco and any subdomains of because.eco.

You must not:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Continue the test if any personal data (other than your own) is encountered.
- Modify data in the Company's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt the Company'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 TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, 'phish' or physically attack the Company's staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

You must always:

- Comply with data protection rules and must not violate the privacy of the Company'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).

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 Company or partner companies to be in breach of any legal obligations.

6. Contact Information

If you have any questions regarding our Vulnerability Disclosure Policy, or if you want to report vulnerabilities, please find our contact details below:

BeCause ApS
Njalsgade 21 E, 1
2300 Copenhagen S, Denmark
Corporate Identity Number: 39745267
Email address: privacy@because.eco