Responsible Disclosure Policy

Background, Scope & Purpose

DUCO attaches great importance to the security of its products and the data they are processing, as well as the protection of any personal data, or other confidential data we would be processing. Nevertheless, despite our best efforts and concern, it may occur that there still are vulnerabilities that e.g. an ethical hacker or computer scientist may discover.

DUCO has therefore opted for this policy of coordinated disclosure of vulnerabilities (also known as the 'Responsible Disclosure Policy') so that persons that discover a vulnerability can privately and securely inform us about them.

This Responsible Disclosure Policy applies to all DUCO products and information systems.

Policy Requirements

Reporting a vulnerability

Responsible disclosure is revealing vulnerabilities in a responsible manner in joint consultation between you and DUCO. If you discover a vulnerability in one of our products or systems, you must:

1. **Report the issue by sending an email to service @ duco.eu**
   - Write your message in English, French, German or Dutch.
   - Explain the issue and provide sufficient details to allow us to identify and/or reproduce the issue so that we can resolve the problem as quickly as possible.
   - Provide additional information such as product code, serial number, photo, screenshots, URL, etc.

2. **Leave your contact details so DUCO can contact you if needed to work together towards a solution.**
   Leave at least your name, e-mail address and/or telephone number.
   Reporting under a pseudonym is allowed, but make sure that we can contact you if we should have additional questions.

Do's and Don'ts that apply

Do not disclose any information regarding the security issue through other channels.
Do not share information concerning the vulnerability with third parties, including before or after informing DUCO about the issue or even after it has been resolved. Such behavior will be considered irresponsible and civil law proceedings may be instituted against you. If, after the vulnerability has been removed, you wish to publish information about the vulnerability, we ask you to notify us at least one month before publication, and to give us the opportunity to respond. Identifying us in a publication is only possible after we have given our explicit approval.

Do not abuse the vulnerability found.
Acts under this Responsible Disclosure Policy should be limited to conducting tests to identify potential vulnerabilities, and sharing this information with DUCO:

- Do not take any action that is not absolutely necessary to detect a potential vulnerability or report a vulnerability.
- Only collect the information necessary to inform us of the issue.
- Do not copy, delete, view or modify DUCO data.

Do not perform actions that could have an impact on the proper functioning of our connected products or our information systems, both in terms of availability and performance, but also in terms of confidentiality and integrity of the data. Therefore, it is e.g. not allowed to perform any of the following actions (non-exhaustive list): placing malware; copying, modifying or deleting data in a system; making changes to the system; using brute-force techniques in an attempt to access a system; (distributed) denial of service attacks.

Do not use attack methods that test the physical security of our buildings and premises.

Do not use attack methods that target our people (e.g. via phishing and other social engineering methods).

In case of doubt about the applicability of this policy, please contact us first via the above mentioned e-mail address, to ask for explicit permission.

Out of scope vulnerabilities

DUCO does NOT recognize trivial vulnerabilities or bugs that are difficult to abuse. The following are examples of known and accepted low risk vulnerabilities and risks that are not in scope of this policy:

- User interface bugs or typos.
- Missing HTTP security headers that do not lead directly to a vulnerability.
- Presence / absence of DNS records.
- Missing cookie flags without clearly identified security impact.
- CSRF or clickjacking with no practical use to attackers.
- CSRF that requires the knowledge of a secret.

- 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, security.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
- SPF, DKIM, DMARC issues
- Reporting older versions of any software, package or library without proof of concept or working exploit.
- Information leakage in metadata.

What we promise

- We will respond to your report within 10 working days, with our review of the report and any expected date for resolution. We strive to solve all problems within a short period of time.

- We will contact you again if we need any additional information.

- We will inform you of the progress of solving the issue identified.

- We will treat your report confidentially and will not share your personal data with third parties without your consent unless this is necessary to comply with a legal obligation.

Further considerations

We reserve the right to ignore low quality reports, including those that report vulnerabilities that are negligeable in terms of risk.

If you find a vulnerability, but do not follow the responsible disclosure rules set out above, we reserve the right to take action or legal proceedings and/or to report the matter to the police.

We reserve the right to change the content of this Policy at any time or to terminate the Policy.

Document Properties

Doc ID	
Version	1.0
Date	
Owner	