Sharesquare

These are our Coordinated Vulnerability Disclosure (CVD) engagement rules

1. Who are we and what do we do?

We are the Co-Ownership B.V., operating under the trade name Sharesquare (hereinafter, **Sharesquare**, **we**, and **us**). We believe that everyone who contributes to the success of a company should be entitled to share in such success. That is why we created the Sharesquare platform (the **Platform**) on app.sharesquare.co, accessible through www.sharesquare.co (the **Website**) which aims to facilitate financial participation by employees (the **Participants**) in companies (the **Clients**) (hereinafter, altogether, the **Services**).

This CVD engagement rules document (the **CVD rules**) applies to all the Services that we offer.

2. What is this?

This is our CVD engagement brochure. In this document we explain how a third party (the **submitting party**) should inform us of a potential security issue (the **issue**) found on one of our Services. We also explain what are the limits for such submissions, both in terms of admissibility and scope, as well as the requested behavior for the submitting party. Finally, the rewarding scheme is explained.

3. Required information for the identification of the submitting party

The submitting party must be a natural person. If the submitting party is representing a legal person (for example an employer), he or she (hereinafter **he**) must still identify himself or herself (h. **himself**) directly and on personal terms. The following information must be provided and verifiable:

- First name
- Last name
- Country of residence
- Email address (private)
- Email address (work)
- LinkedIn profile

4. Geographical admissibility

The country of residence of the submitting party must be a member of the European Economic Area (EEA).

5. Professional admissibility

The submitting party must be a recognized security professional, with a direct and proven affiliation to an organization operating in the Cybersecurity field, including but not limited to professional services firms, independent research consultancies, software vendors, university research groups or departments etc.

In an alternative yet equivalent fashion, the submitting party may also opt for proving its stature as a Subject Matter Expert (SME) in the Cybersecurity field instead, without any formal affiliation; it may do so by submitting a number achievements in related contexts (for example, *hall of fame* mentions, disclosure credits etc).

6. Direct stakeholder admissibility

As an alternative to the *Professional admissibility* criteria the submitting party may also be a stakeholder of Sharesquare. This can be the case, by way of example, when the submitting party has an established relationship as customer of Sharesquare, as a direct affiliate of a customer (e.g. an employee of a customer) or a shareholder or investor of Sharesquare.

For the avoidance of doubt, the *Required information for the identification of the submitting party* and *Geographical admissibility* criteria still apply.

7. Verification of the submitting party

Failure to provide the needed information as requested above or to clear the admissibility criteria in full results in the submission by the submitting party to be deemed as void and therefore discarded.

Sharesquare does not have to provide any details about the specific points on which the verification of the submitting party fails.

Sharesquare reserves the right to ask the submitting party for more information in the course of qualifying the submitting party itself as legit.

8. Submission format

When submitting a private CVD filing to Sharesquare concerning the issue the submitting party must provide the following information:

- Required and admissibility information (see previous sections)
- Concerned system (e.g. website)
- Brief description of the issue
- PoC (as a list of steps, or automated script)
- Perceived severity (low, medium or high)
- CVE references (if applicable)

The above information is to be sent via email to the email address e91e6348157868de9dd8b25c81aebfb9@sharesquare.co.

9. Prohibited activities

From the very moment it observes an issue and from that moment on indefinitely, regardless of a submission and the status of it, the submitting party is requested:

- to keep all of the information around the issue strictly private, and in particular:

- refrain from any typical full disclosure (FD) activities, including but not limited to sharing issue information on public and anonymous online communities, regardless of the destination of use and target audience
- refrain from any typical partial disclosure (PD) activities, including but not limited to sharing issue information with selected parties either directly or indirectly affiliated with Sharesquare, or other researchers

- not to try and take advantage of the issue itself, first-hand, for example by targeting a PoC script at the concerned system
- not to share, or make use of (directly or indirectly) any information or data extracted from the concerned system, regardless of how it was obtained
- to permanently delete any information or data extracted from the concerned system, regardless of how it was obtained
- not to try and solicit Sharesquare outside of the CVD engagement with the aim of promoting any form of remedies, services, software solutions etc. supposed to solve or mitigate the issue
- not to try to engage in negotiations about any form of compensation (both monetary and non-monetary) for the discovery and submission of the issue (see *Rewards*)

10. Consequences of engaging in prohibited activities

If the submitting party engages in any prohibited activities or activities equivalent to those (see above), the submission is deemed as void and therefore discarded.

The submitting party is reminded that in case of illegal cybercriminal activities it risks legal prosecution, with the natural person acting as submitting party being held liable on a personal level. In the Netherlands, cybercriminal activities are unlawful and therefore prosecutable (at the moment of writing, *Wet Computercriminaliteit III* and *Implementatie Richtlijn 2013/40/EU* among others*).*

11. Rewards, consequences of reward requests

By submitting a coordinated disclosure according to the terms outlined by this document the submitting party does not gain any entitlement to any reward whatsoever, whether monetary or non-monetary.

Any requests by the submitting party in this sense, namely pairing the submission with the request for a reward, whether conditionally or unconditionally, results in the voidance and discarding of the submission. Such requests may configure as extortion attempts, thus unlawful and therefore prosecutable (in the Netherlands at the moment of writing, articles 317 and 318 of the Criminal Code among others).

At its very own discretion and up to the exhaustion of a limited, undisclosed budget, Sharesquare may decide to attribute some form of reward to the submitting party, in connection with the gravity of the reported issue while still not having to disclose on which grounds such reward gets attributed.

In this attribution, the professionalism, empathy and kindness shown by the submitting party also count.

12. Information processing

Specifically for the personal and business information of the submitting party, our Privacy Policy applies.

The Co-Ownership Company B.V.

Hamerstraat 19-1

1021 JT Amsterdam

E: support@sharesquare.co

W: www.sharesquare.co

Chamber of Commerce number: 80460593

Version: February 2025