Vulnerability Disclosure Policy

Kader Digital B.V.

This policy is in English since the information within is also intended for the ethical hacker community which usually operates in this language.

Brand Promise

Kader Digital is an organization that delivers several QHSSE solutions. As such, we are very aware of the importance of information security. QHSSE reports often contain business sensitive information. And they might even contain personal data, e.g. social or physical incidents. This takes the importance of information security to the next level within the context of GDPR.

Kader Digital utilizes multiple paths to detect vulnerabilities in its software. We have automated monitoring for vulnerable software components, we contract 3rd parties for vulnerability and penetration tests, etcetera.

Even with those measurements in place, we are aware that it is hard to stay on top of the security curve. Therefore we employ a responsible disclosure directive: we will notify suppliers of vulnerabilities we find in their software and we are grateful for reports by organizations and individuals that point out vulnerabilities in our software.

Finally, we are ISO 27001 compliant. This ensures that we employ effective procedures when vulnerabilities in our software or our organization are reported.

Initial program and scope

Kader Digital develops two products in house, and those products are within the scope of this policy.

Arbo management system (AMS)

- arbomanagementsysteem.nl
- ams08.nl

Kader Platform

- Smile SaaS Suite (smilesaas.eu; suiteacc.eu; suiteont.eu)

- Custom applications (kader-platform.nl)

Other websites and applications

If you find any vulnerabilities within other applications or websites related to our parent company Kader B.V. this document does not apply. We will still take appropriate actions to report, resolve or mitigate any vulnerabilities reported.

“We will take no legal action if”

We will not take legal action if the vulnerability is disclosed in a responsible manner and if the research did not impact the services we provide for our customers.

Specifically:

- You will not disclose the fact that our software is vulnerable to other organizations for 90 days after reporting to us. This enables Kader Digital to communicate with affected parties and it enables Kader Digital to solve or mitigate the reported vulnerability.
- You will limit access to data on our servers to the minimum required to proof the vulnerability.
- You will not disclose any data you accessed on our servers, including but not limited to code, configuration or user data.
- You will not adversely affect the availability or performance of our systems without explicit consent from Kader Digital.

Communication mechanisms and process

Mail to privacyofficer@kader.nl

If the report contains sensitive data, please can use this mail address to request a more secure way to transfer the information.

All mails will be answered within 7 days.

Nonbinding submission preferences and prioritizations

All reported vulnerabilities will be assessed based on the following criteria, in order of importance:

- Are we aware of the vulnerability?
- Does the vulnerability impose an immediate risk to the confidentiality of customer data?
- Does the vulnerability impose an immediate risk to the integrity of customer data?
- Does the vulnerability impose a risk to the availability of our application?

- Does the vulnerability impose a risk on the confidentiality or integrity of our own data?
- Does the vulnerability impose a risk on the performance of our systems?

Depending on the perceived risk we will formulate a strategy to mitigate or resolve the vulnerability.
All reports will be answered with a sincere thank you. Vulnerabilities that we were unaware of can be rewarded with a reward of up to €1000,-.