Responsible disclosure policy

At LEVANTOgroep, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present. LEVANTOgroep would appreciate it if this was reported in accordance with the guidelines below.

1.1. Guidelines for Reporters

- Do not exploit vulnerabilities to gain access to sensitive information, systems, or data that do not belong to you.
- Do not use social engineering techniques to gain access to systems.
- Do not use brute force or denial-of-service attacks.
- Do not share vulnerabilities with third parties before they are resolved.

1.2. Reporting a detected vulnerability

Vulnerabilities can be reported via datalek@levantogroep.nl. Provide the following information in a report:

- A detailed description of the vulnerability.
- Steps to reproduce the vulnerability.
- The potential impact of the vulnerability.
- Contact information for further correspondence.

1.3. Acknowledgment of Receipt and Timelines

- We will acknowledge receipt of your report within 3 business days.
- We aim to investigate and resolve your report within 30 days.
- We will keep you regularly updated on the progress.

1.4. Rewards and Recognition

Reporters who help us identify and resolve vulnerabilities may be eligible for a reward or public recognition, depending on the severity and impact of the vulnerability.

1.5. Legal Protection

If you adhere to this policy when reporting a vulnerability, we will not take legal action against you.