Responsible Disclosure Policy

At SYS TEC electronic, we place great importance on the security of our products. Nevertheless, it is generally known that no product and no customer system can be 100 percent secure, regardless of how much effort is invested in product security.

The SYS TEC electronic Product Security Incident Response Team, PSIRT, would like to be informed about all potential security issues affecting our products so that we can take the necessary measures to remedy these issues promptly. Please report all other potential security issues concerning SYS TEC electronic AG itself to our Computer Security Incident Response Team (CSIRT).

We recognize the commitment of the security community and value the important contribution of its members to the continuous improvement of product security. Our goal is to promote an open, constructive, and mutually beneficial collaboration with security researchers.

Below you will find our considerations and expectations on how we can achieve this goal together.

What you can expect from us

- **Responsiveness**
  We respond to your communications in a timely manner and take them seriously.
- **Transparency**
  You will receive regular updates from us on the status of the investigation. In particular, we will inform you about the status of the reported vulnerability as soon as we have completed each phase of our incident response process.
- **Responsible handling of information**
  Your findings will not be published without your consent. If security relevant reasons make it necessary to share essential information with third parties, for example customers, we will inform you in advance and explain our reasons. If necessary, we will agree with you on an embargo period during which no details of the incident will be disclosed.
- **Fairness**
  After the investigation has been completed, we will coordinate with you regarding the possible publication of a security advisory. If we publish such an advisory, we will generally acknowledge your contribution and that of your team. Please note that we do not currently offer a bug bounty program.

What we expect from you

- **Responsiveness**
  Please respond to our communications in a timely manner so that we can react to your report more quickly and effectively.
- **Transparency**
  In order to effectively assess and remediate potential security vulnerabilities, we ask you to be open about your findings and your plans for public disclosure.
- **Responsible handling of information**
  We trust that you will not publish your findings without prior coordination with us, for example to customers or business partners, at least two weeks before the end of an agreed embargo period. Even if no embargo period exists, we ask for two weeks advance notice before information is shared internally or publicly. Early or incomplete disclosure can lead to misunderstandings and increase the risk for affected parties. By providing advance notice, we can jointly ensure that the shared information is accurate and complete.
- **Fairness**
  In order for us to resolve issues effectively and reduce risks for affected parties, we ask for fair and respectful cooperation. Mutual trust and a collaborative approach are the foundation for achieving our shared goal of continuously improving product security and minimizing the impact of security incidents on companies as well as on the public.

How to submit a vulnerability report

To submit a vulnerability report to the PSIRT or CSIRT of SYS TEC electronic AG in accordance with this policy, please visit our website. (https://www.systec-electronic.com/en/)

SYS TEC electronic AG tracks CVEs in the software and hardware used in our products.

Data processing in accordance with data protection regulations

As part of the responsible disclosure process, we process the personal data you provide on the basis of Article 6 paragraph 1 point f of the GDPR. This is done on the basis of our legitimate interest in the security of our systems and serves exclusively for the purpose of making contact.

The data is stored in compliance with statutory retention periods. It will only be shared with third parties if this is necessary for handling the incident or if there is a legal obligation to do so.

You have the right to obtain information about the data we process, to have it corrected or deleted, and to restrict processing under certain conditions. Further information about your rights and the processing of personal data can be found in our privacy policy, which is available on our website at any time.