KISTERS IS
Vulnerability Disclosure Policy

v.1.0, 2025-03-18

Owner:
KISTERS CISO

Table of contents

1 Introduction

1.1 Motivation and objectives

KISTERS has a strong focus on information security and data protection when providing solutions, systems and services to our clients and partners.
However, vulnerabilities can never be completely eliminated, despite best efforts. When vulnerabilities are identified and exploited, it puts at risk the confidentiality, integrity or availability of KISTERS systems or systems of KISTERS clients and partners and the information processed therein.
This Policy describes which solutions, systems and services are authorized to be subject to security tests, which types of security tests are authorised, who is authorized to perform these tests, and how to submit vulnerability reports. If you are a legitimate user of one of our solutions, systems or services or if you are a security researcher working independently or commissioned by our partners, clients, or by KISTERS, we encourage you to contact us to report potential security issues in our systems by following this Policy.
Please note that KISTERS does not operate a bug bounty program. By submitting a vulnerability report, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against KISTERS or our clients and partners related to your submission.

1.2 Scope

This Policy applies to persons performing security tests, and solutions, systems and services subject to security tests, as follows:

1.2.1 Systems operated by KISTERS

For legitimate users and for security researchers who work independently or are legitimately commissioned by KISTERS:
All internet facing systems

- from the KISTERS Group, including the entire KISTERS web presence;
- from KISTERScloud systems, i.e., systems operated by KISTERS which provide application services to our clients and partners.

1.2.2 Systems operated by clients or partners

For legitimate users, operators and administrators of our clients or partners and security researchers legitimately commissioned by the responsible clients or partners:

- Internet facing systems which are operated by our clients or partners and which are clearly marked or can be identified beyond any doubt as a KISTERS solution,
- KISTERS solutions installed and operated on client's premises, on client's servers, workstations or other devices, in access restricted networks or on access restricted IT systems.

1.2.3 Out of scope

Any persons and any solutions, systems or services not expressly included above are excluded from the scope of this Policy and are not authorised for any testing activities. If you are not sure whether a solution, system or service is in scope for testing by yourself or not, contact KISTERS by sending an email to the contact email address provided below.

1.3 Roles, Responsibilities and Dependencies

	Security Researcher / You	**KISTERS**	**System operators (3)**	**3rd party suppliers (2)**	**KISTERS clients (1)**	**National CSIRT (1)**
Commission security tests	C	A/R	A/R			
Perform security tests	A/R	C/I	C/I			
Report potential vulnerabilities	A/R	I	I		R (4)	
Confirm vulnerability report	I	A/R	C	C		
Inform stakeholders		A/R	I	I	I	I
Provide fix or mitigation	C/I	A/R	I	R	I	I
Confirm resolution	C/I	A/R	C	C	I	I

(1): as applicable and necessary
(2): if vulnerability is caused by 3rd party components
(3): if system operated by KISTERS client or partner
(4): if vulnerability is detected in normal business operation

1.4 Applicable legal and regulatory requirements

This Policy is in line with the requirements for the implementation of a process and communication methods to facilitate the sharing of information about potential vulnerabilities in our systems, services and solutions as mandated by the EU Cyber Resilience Act [1] and supporting the obligations mandated by EU NIS 2 Directive [2].
Applying security tests to any system outside the scope of this Policy, the application of any testing method not authorized by this Policy, by persons not authorised by this Policy, and any use of information obtained by security tests authorized by this Policy used for any other purpose than providing a vulnerability report to KISTERS, shall be considered unlawful, shall be treated as criminal offense within the meaning of the German Criminal Code (Strafgesetzbuch, StGB) [3] and shall be prosecuted accordingly.

2 Guidelines

2.1 Security research

Under this Policy, “security research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.

- Access KISTERS software solutions only as contractually permitted by your software or service licenses, or as permitted or contractually commissioned by authorized clients or partners with corresponding KISTERS software or service licenses.
- Make every effort to avoid privacy violations, degradation of user experience, disruption of systems in general, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence.
- Do NOT use an exploit to compromise or delete data, establish command line or persistent access, upload code, or use the exploit to pivot to other systems.
- Do NOT exfiltrate any data under any circumstances, in particular do NOT exfiltrate any personal data within the meaning of the General Data Protection Regulation [4].
- Do NOT cause harm to the systems and operations.
- Do NOT intentionally access the content of any communications, data, or information transiting or stored on the information system(s) – except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- Do NOT reveal any information and data used or retrieved during the discovery to the public or any other parties.
- Do NOT reveal the vulnerability or problem to the public or any third party.
    - Exception: If we fail to react to your vulnerability report within a reasonable time frame, in general within 10 business days, you may decide to engage in the "Coordinated Vulnerability Disclosure (CVD) Process" [5] of the German Federal Office of Information Security (BSI), and you may report the vulnerability to the BSI following this CVD process.

2.2 Excluded test methods

The following test methods are NOT authorized:

- Volumetric tests, i.e., overwhelming a system or service with a high volume of requests
- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g., office access, open doors, tailgating),
- Social engineering (e.g., phishing, vishing, quishing), or any other non-technical vulnerability testing.
- Full red-team penetration testing that involves unauthorized access to our servers or servers operated by clients or partners, including cloud servers and services.

3 Reporting a vulnerability

3.1 Content of a vulnerability report

If you have identified a vulnerability that has or may have an impact on the information security of solutions, systems or services, your qualified vulnerability report should provide us with

- sufficient information to identify the affected solution, system or service,
- sufficient details to reproduce the problem so that we can resolve it as quickly as possible - note that usually a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation in terms of technical information or potential proof-of-concept code,

- a short description of the vulnerability's potential security impact,
- if possible, an evaluation of the vulnerability score using the Common Vulnerability Scoring System CVSS 3.1 [6],
- the report in English preferably, or in German,
- valid contact information for further requests,
- an indication if we may reference your name and/or contact details as the reporter of the vulnerability in subsequent advisories, release notes, or other information we prepare for our clients, partners or the public.

3.2 Submission of a vulnerability report

Please submit your vulnerability report through our ticket system (KISTERS Customer ServiceDesk, link see below), following these steps:

- If you are a KISTERS client or partner with an active user account in the KISTERS Customer ServiceDesk
    - please open a new support ticket of type "Incident" in your Customer ServiceDesk ("Energy" (SDNRG), "HydroMet" (SDWTR), "EHS" (SDEHS), as applicable)
- If you do not have an active user account in the KISTERS Customer ServiceDesk, please
    - open a new ticket in the ServiceDesk "Vulnerabilty Report" (SDVR)
- begin the subject line with the keyword "VulnerabilityReport"
- fill in the required form fields
- provide a short description of the vulnerability
- use KISTERS SecretBin to upload your detailed report, **disable** the option "Burn after reading", add the SecretBin link to the description
- submit the ticket

Notes:

- The ServiceDesk "Vulnerability Report" is exclusively reserved for submission of vulnerability reports in case you do not have an active account in the regular KISTERS Customer ServiceDesk. Please do not use it for any other purpose, and always use the regular KISTERS Customer ServiceDesk if you have an active account.
- You have to provide a valid email address and a password when opening a ticket in the ServiceDesk "Vulnerability Report". You will have to use this email address and password in order to access your ticket later.

4 KISTERS reaction to a vulnerability report

Once we receive your vulnerability report via our KISTERS Customer ServiceDesk, we will

- confirm the receipt of your report by confirming the ticket, usually within seven business days;
- confirm the existence of the vulnerability to you to the best of our ability;
- be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution by appropriate comments in the ticket.

- process the personal data that you provide (such as your email address and name) in accordance with the applicable data protection legislation and will not pass on your personal details to third parties without your permission;
- publish your name as the discoverer of the problem, if you have agreed to this in your initial submission, when and if we disclose the problem publicly;
- not to pursue criminal charges against you as long as you have complied with this Policy. This does not apply if recognizable criminal or intelligence intentions have been or are being pursued.

5 BSI coordinated vulnerability disclosure process

As a provider of solutions, services and systems we strongly prefer to receive your vulnerability report directly as described above. However, if we do not react to your vulnerability report in a reasonable time frame or if you have major concerns regarding our vulnerability management process, you may decide to report the vulnerability you detected to the Federal Office of Information Security (BSI). The BSI provides a proven, neutral process for coordinated vulnerability disclosure [5] and acts as a mediator between you and KISTERS. Once you submit a vulnerability report to the BSI, the BSI is in control of the process and coordinates all further steps in the vulnerability management process.

6 Contact information

The KISTERS Customer Servicedesk can be accessed at https://conflks.atlassian.net/servicedesk.
Any questions regarding this Policy may be sent to itsecurity@kisters.de.

7 References

[1] "REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)", European Commission, 2024-11-20; URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (2025-02-26)

[2] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Document 32022L2555, European Commission, 2022-12-14; URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555, (2025-02-19)

[3] "German Criminal Code (Strafgesetzbuch, StGB)", Federal Republic of Germany, 2024-11-08; URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (2025-02-26)

[4] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", European Commission, 2016-04-27; URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (2025-02-26)

[5] "Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess", Federal Office for Information Security, 2022-12-01; URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf (2025-02-26)

[6] “Common Vulnerability Scoring System Version 3.1 Calculator”, Forum of Incident Response and Security Teams, Inc., 2015-2025; URL: https://www.first.org/cvss/calculator/3.1 (2025-02-26)

8 Document history

This document is checked at least once a year to ensure that it is up to date and amended if necessary. The official version of this document is managed online. Before using electronic copies or printed versions, these must be checked to ensure that they are up to date.

Version	Date	Editor	Action
1.0	2025-03-18	H.-J. Schlebusch	creation