

SPARKS INSTRUMENTS SA

Coordinated Vulnerability Disclosure Policy

How to report a security vulnerability in a Sparks Instruments product

Document POL-CRA-14-02 | Version 1.1 — Approved | Planned effective date 14 September 2026 | PUBLIC

Document Control

Company Name	Sparks Instruments SA
Registered Office	Route de Montena 85, CH-1728 Rossens, Switzerland
Document Title	Coordinated Vulnerability Disclosure Policy
Document Reference ID	POL-CRA-14-02
Version	1.1 — Approved
Status	Controlled policy, published. It states what Sparks Instruments SA undertakes towards a person who reports a vulnerability, and it binds only Sparks Instruments SA.
Scope	Sparks Instruments products
Classification	PUBLIC — intended for publication
Author	Sébastien Kuenlin, Head of R&D and Security Manager
Document Owner	Sébastien Kuenlin
Accountable Executive	Olivier Ducry, Chief Executive Officer
Approved By	Olivier Ducry, Chief Executive Officer — Accountable Executive under GOV-CRA-00-01 §5.3
Legal Basis	Articles 13 and 14 of Regulation (EU) 2024/2847 (Cyber Resilience Act); ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability handling)
Effective Date	14 September 2026, on approval.
Key Dates	11 September 2026 — Article 14 reporting obligations apply. 11 December 2027 — the remainder of the Regulation applies.
Review Cycle	11 September 2027, or earlier upon any change to our security contact details
Canonical URL	https://www.sparksinstruments.com/security/vulnerability-disclosure.pdf

PUBLIC DOCUMENT

This policy may be freely copied, quoted and redistributed. It states how Sparks Instruments SA receives, handles and discloses security vulnerabilities affecting its products. Where a copy differs from the version published at the canonical URL above, the published version prevails.

Revision History

Version	Date	Description of Change	Approved By
1.0	28.08.2026	Original issue.	O. Ducry (CEO)
1.1	14.09.2026	Modification of service level Section 6 recast: the remediation targets by CVSS severity are withdrawn and replaced by response service levels. Consequential changes at §1.3, §6 and §7.1.	O. Ducry (CEO)

Contents

Document Control	1
Revision History	2
Contents	2
1. Our Commitment to Product Security	3
1.1 Welcome	3
1.2 Who this policy is for	3
1.3 What we undertake	4
2. Scope	4
2.1 In scope	4
2.2 Out of scope	5
2.3 Findings we do not normally treat as vulnerabilities	5
3. How to Report a Vulnerability	6
3.1 Reporting channels	6
3.2 What to include in your report	6
3.3 Encryption	7
3.4 Anonymous and pseudonymous reports	7
3.5 Languages	7
4. Rules of Engagement	7
4.1 Guiding principles	7
4.2 Activity we authorise	8
4.3 Activity that is strictly forbidden	8
4.4 Handling of data you encounter	9
4.5 Customer and third-party deployments	9
5. Safe Harbour	9
5.1 Our undertaking to you	9
5.2 Conditions	9
5.3 Limits of this safe harbour	10
5.4 If the conditions were not met	10
6. Our Response — Service Levels	10
7. Coordinated Disclosure	11

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 3 of 15

7.1 The process	11
7.2 Disclosure timeline and embargo	11
7.3 CVE assignment and attribution	12
7.4 Regulatory notification under the Cyber Resilience Act	12
7.5 Advisories	12
7.6 If we disagree	12
8. General Terms	13
8.1 No bug bounty and no public acknowledgements	13
8.2 Confidentiality of your report	13
8.3 Personal data	13
8.4 Governing law	13
8.5 Changes to this policy	13
8.6 Contact	13
Annex A — Vulnerability Report Template	14
Annex B — Our security.txt	15

Page references are to this issue of POL-CRA-14-02 and are verified at each revision.

1. Our Commitment to Product Security

1.1 Welcome

Sparks Instruments SA designs and builds insulation monitoring instrumentation and the software that runs it, for use in industrial and laboratory environments. Our customers rely on our products to monitor high-voltage assets and to acquire the data on which real decisions are made. We take the security of those products seriously, and we know that no development process, however careful, produces hardware or software without defects.

For that reason we welcome reports of security vulnerabilities from anyone — independent security researchers, academics, customers, integration partners, upstream maintainers and national authorities. If you have found a weakness in one of our products, we want to hear from you, and we would rather hear it from you than read about it later.

This document explains how to reach us, what we ask of you while you are testing, what legal protection we offer you in return, how quickly we will respond, and how we will handle publication. It is written to be read before you start, and we encourage you to contact us if anything in it is unclear.

1.2 Who this policy is for

This policy is addressed to:

- Security researchers and ethical hackers who wish to test our products and report findings to us;
- Customers and integration partners who discover a security issue in the course of normal use or internal assessment;
- Upstream maintainers, vendors and CERT / CSIRT teams notifying us of an issue affecting a component we use;
- Anyone who has received a vulnerability report about our products from a third party and wishes to pass it on to us.

It is not a licence to test systems belonging to our customers or to any other third party. Section 4.5 explains this limitation.

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 4 of 15

1.3 What we undertake

When you report a vulnerability to us in good faith and in accordance with this policy, Sparks Instruments SA undertakes to:

- **Acknowledge your report promptly** and give you a reference under which we will track it (Section 6);
- **Treat you as a partner, not as an adversary** — we will not pursue or support legal action against you for good-faith research conducted within the rules set out in Section 4 (Section 5);
- **Keep you informed** at defined intervals, in plain terms, for as long as your report is open (Section 6);
- **Investigate every report** on its technical merits, and tell you honestly if we conclude it is not a vulnerability and why;
- **Coordinate publication with you** and not disclose your identity or your report to anyone outside the handling process without your consent, save where the law requires it (Sections 7 and 8);
- **Work to remediate confirmed vulnerabilities as quickly as the nature of the fix allows, keep you informed of progress at the intervals set out in Section 6, and publish a security advisory so that our users can protect themselves.**

A note on expectations

Sparks Instruments SA is a small engineering company. We do not operate a bug bounty programme and we do not offer monetary rewards (Section 8.1). What we do offer is a real technical contact, an honest answer, a published response timeline that we hold ourselves to, and the legal assurances set out in Section 5.

2. Scope

This section defines what you are invited to test and report under this policy, and what falls outside it. If a system or product you are interested in is not listed below, please ask us at cybersecurity@sparksinstruments.com before you begin.

2.1 In scope

Asset	What is covered
UDL-8000	The device, its embedded firmware, and the software delivered with it — UDL-Configurator, UDL-System Updater, UDL-Monitor, UDL-Filemanager and UDL-DAQ — in any currently supported version.
UDL-DataServer Software Package	The UDL-DataServer service and the UDL-Data Client application, and the configuration of the PostgreSQL database we deploy with them, in any currently supported version.
Installers and update packages	Installers, patch bundles, update packages and the mechanism by which updates are delivered and verified on a user system.
Release integrity	Code signatures on our released artefacts, signature verification logic, and the integrity of the artefacts published through our official distribution channel.
Published advisories	The security advisories we publish for our products, including errors or omissions in them. Note that we do not publish our Software Bill of Materials: it is drawn up for every release and made available to market surveillance authorities on request, but it is not a public artefact and is therefore outside the scope of this policy.
Third-party components	Vulnerabilities in open-source or commercial components that are reachable in a shipped configuration of one of our products. Please tell us even if the root cause lies upstream — we will coordinate with the maintainer.
Security contact infrastructure	Our security.txt file, our published PGP key, and the security mailbox at cybersecurity@sparksinstruments.com .
sparksinstruments.com	Security issues in the corporate website that expose customer data, allow content to be modified, or affect the integrity of anything we distribute.

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 5 of 15

2.2 Out of scope

The following are not covered by this policy, and testing them is not authorised by us:

- Any deployment of our products operated by a customer or third party, including customer instruments, laboratory networks and hosted environments — see Section 4.5;
- Third-party services and platforms that we use but do not control, including cloud providers, e-mail and content-delivery services, hosted marketing tools, and code-hosting or package repositories operated by others;
- The corporate IT systems, internal networks, endpoints and accounts of Sparks Instruments SA, and any system not listed in Section 2.1;
- Our employees, contractors, customers and suppliers as individuals — no social engineering, phishing or pretexting of any kind;
- Our physical premises, hardware and personnel;
- Product versions that have reached end of support, unless the finding also affects a supported version;
- Findings that require an attacker to already hold full administrative control of the host, or unrestricted physical access to it, unless a specific security control of the product is thereby defeated.

2.3 Findings we do not normally treat as vulnerabilities

We will read and answer every report. However, the following are unlikely to be accepted as security vulnerabilities unless you can demonstrate a concrete, realistic security impact. If you can demonstrate that impact, please send the report — the list below is about evidence, not about categories we refuse to look at.

- Missing or misconfigured HTTP security headers, cookie flags or TLS cipher preferences, with no demonstrated exploitation path;
- SPF, DKIM or DMARC configuration observations, and e-mail spoofing reports without a working demonstration;
- Output of an automated scanner submitted without manual validation or a proof of concept;
- Reports that a component version is outdated or that a published CVE exists in a dependency, without evidence that the affected code path is reachable in a shipped configuration of the product;
- Self-XSS, or issues that require the victim to paste attacker-supplied content into their own browser or application;
- Clickjacking, tabnabbing or UI-redressing on pages that carry no sensitive action;
- Username, licence or account enumeration, and absence of rate limiting, without a demonstrated consequence;
- Descriptive banners, version disclosure, directory listings and verbose error pages that reveal no sensitive information;
- Physical, theoretical or purely local attacks requiring privileges the attacker would not realistically obtain;
- Denial of service, volumetric or resource-exhaustion findings — see Section 4.3, which prohibits testing them.

3. How to Report a Vulnerability

3.1 Reporting channels

There is one intake point for all security reports. It is monitored on business days and reaches our security team directly.

Channel	Details	Use it for
E-mail — primary	cybersecurity@sparksinstruments.com	All vulnerability reports. This is the address declared in our security.txt and the fastest route to a human who can act on your report.
security.txt	https://www.sparksinstruments.com/.well-known/security.txt	Machine-readable confirmation of our current security contact, our PGP key, our preferred languages and the canonical location of this policy, in accordance with RFC 9116.
PGP public key	https://www.sparksinstruments.com/.well-known/pgp-key.asc Fingerprint: BDD3 90F8 8BC6 60D7 5C05 D019 39BD 44C8 E919 44F0	Encrypting the technical detail of your report, including proof-of-concept code and any sensitive material.
Postal address	Sparks Instruments SA, Security Team, Route de Montena 85, CH-1728 Rossens, Switzerland	Reports where written correspondence is required, for example by a legal representative. Postal reports cannot be handled within the service levels in Section 6.

Please do not

Please do not report vulnerabilities through our general sales, support or contact forms, through social media, or to individual employees. Those routes are not monitored by the security team, and using them will delay our response and may expose the detail of your finding to people who are not part of the handling process.

3.2 What to include in your report

The more of the following you can give us, the faster we can validate and fix the issue. Please do not delay a report because you cannot supply every item — send what you have.

- The product and the exact version affected, including build number where you have it;
- The operating system, configuration and any prerequisites needed to reproduce the issue;
- A clear description of the vulnerability and the security impact you believe it has;
- Step-by-step reproduction instructions, and a proof of concept if you have one;
- Any logs, screenshots, network captures or crash dumps that support the finding, with sensitive data removed;
- Your assessment of severity, with a CVSS v3.1 or v4.0 vector if you use one;
- Whether you believe the vulnerability is already known publicly or being exploited;
- Whether you have reported the issue to anyone else, including another vendor, a CERT / CSIRT or a coordinator;
- How you would like to be credited if a CVE is assigned, or that you prefer not to be named;
- Your preferred disclosure timeline, if you have one in mind (see Section 7.2).

A template you may use is provided at Annex A.

SPARKSINSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 7 of 15

3.3 Encryption

We strongly encourage you to encrypt the technical content of your report with our PGP public key, particularly where you are attaching working exploit code. Our public key is published on our website and referenced from the "Encryption" field of our security.txt. If you would like us to reply encrypted, please include your own public key or its fingerprint.

If you are unable to use PGP, send the report unencrypted rather than not at all, and tell us that you have sensitive material to transfer. We will arrange a secure channel with you.

3.4 Anonymous and pseudonymous reports

You may report anonymously or under a pseudonym. We will handle the report on the same terms. Please note two practical consequences: we cannot send you progress updates or a triage outcome unless you give us some means of contact, and the safe harbour in Section 5 protects conduct, not identity — it applies to good-faith research whether or not we know who you are, but we cannot confirm your standing to a third party if we do not know who you are.

3.5 Languages

We accept reports in English and French. English is preferred for technical detail, as it avoids translation ambiguity in the handling and in any subsequent advisory. We will reply in the language you write in wherever we can.

4. Rules of Engagement

These rules define good-faith security research for the purposes of this policy. Staying within them is the condition of the safe harbour in Section 5. They exist to protect our users: our products monitor high-voltage assets and acquire measurement data, and disturbing a live installation can destroy work that cannot be repeated — or leave an asset unmonitored.

4.1 Guiding principles

- **Minimise harm.** Use the least intrusive method that demonstrates the issue. Once you have established that a vulnerability exists, stop.
- **Test only what is yours to test.** Use your own installation, your own licence and your own data — or a system whose owner has given you written authorisation.
- **Stop and report.** If you encounter personal data, credentials, customer measurement data, proprietary information or any other sensitive material, stop immediately, do not download or retain more than is needed to evidence the finding, and tell us in your report.
- **Give us a reasonable opportunity to fix the issue** before discussing it publicly, in accordance with Section 7.
- **Ask if you are unsure.** If you are not certain whether a particular test is permitted, write to cybersecurity@sparksinstruments.com and ask. We would much rather answer a question in advance than deal with the consequences afterwards.

4.2 Activity we authorise

Within the scope defined in Section 2.1, and subject to the prohibitions in Section 4.3, we authorise you to:

- Install, run and configure our software on systems you own or control, and test a device you own, for the purpose of security testing;
- Analyse the product statically and dynamically, including reverse engineering, debugging, disassembly and decompilation, to the extent necessary to identify and demonstrate a security vulnerability, notwithstanding any contrary term in the licence agreement;
- Inspect installers, update packages, signed artefacts and their verification logic;
- Perform proportionate, non-destructive testing against our public website and security contact infrastructure;
- Develop and run a proof of concept sufficient to demonstrate the issue on your own system.

Licence terms and this policy

To the extent that our end-user licence agreement or terms of use would otherwise prohibit the activity described in this section, Sparks Instruments SA waives that prohibition for research carried out in good faith under this policy, and will not treat such research as a breach of contract. This waiver is limited to the activity described above and does not extend to anything listed in Section 4.3.

4.3 Activity that is strictly forbidden

The following are never authorised, in any circumstances, and fall outside the safe harbour:

Prohibited activity	Why
Denial of service of any kind	No volumetric attacks, stress testing, load testing, resource-exhaustion attacks, fuzzing against systems that are not yours, or any test whose foreseeable effect is to degrade or interrupt a service. Our products monitor live high-voltage assets; an interruption can destroy an experiment or a production run, or leave an asset unmonitored.
Manipulation, destruction or exfiltration of production data	Do not create, modify, encrypt, corrupt or delete data in any environment that is not yours, and do not download data beyond the minimum needed to evidence the finding.
Accessing data belonging to other people	If a vulnerability gives you access to another user's or customer's data, stop at the point of proof, do not browse further, do not retain it, and tell us.
Social engineering and phishing	Do not target our employees, contractors, customers, suppliers or their families by phishing, vishing, smishing, pretexting or any other manipulation, and do not attempt to obtain credentials from them.
Physical attacks	Do not attempt physical access to our premises, hardware, mail or waste, and do not attempt to test physical security controls.
Persistence, backdoors and malware	Do not install implants, backdoors, web shells or any persistence mechanism, and do not introduce malicious code into any system, artefact, package or repository.
Lateral movement and privilege escalation beyond proof	Do not pivot to other systems, escalate privileges further than needed to demonstrate the issue, or expand access once the vulnerability is established.
Credential attacks	Do not brute-force, spray or stuff credentials, and do not use credentials obtained from third-party breaches or from any source other than your own accounts.
Supply chain tampering	Do not attempt to publish, modify or typosquat packages, dependencies or artefacts, and do not attempt to submit malicious code to our repositories or those of our upstream dependencies.
Testing third-party systems	Do not test customer deployments, partner systems or third-party services in our name — see Section 4.5.
Public disclosure before coordination	Do not publish details, proof-of-concept code or screenshots of an unfixed vulnerability before the date agreed under Section 7.
Extortion and payment demands	Do not make disclosure, or the withholding of disclosure, conditional on payment. We do not pay for reports (Section 8.1), and a demand of this kind will be treated as extortion rather than as security research.

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 9 of 15

4.4 Handling of data you encounter

If your testing gives you access to data that is not yours, we ask you to:

- Stop testing that path immediately and record only what is necessary to evidence the finding;
- Not copy, retain, transmit or publish the data, and not use it for any purpose;
- Tell us in your report exactly what you were able to access, so that we can assess the impact and meet our own notification obligations;
- Securely delete any copy in your possession once we confirm that we no longer need it, and confirm the deletion to us in writing.

We will treat prompt, complete disclosure of an accidental access as evidence of good faith.

4.5 Customer and third-party deployments

This policy authorises testing of our products on systems you own or control. It does not authorise you to test an installation belonging to one of our customers or to any other third party, and Sparks Instruments SA cannot give you permission to do so.

If you believe you have identified a vulnerability by observing a third-party deployment, please report it to us with the technical detail, but do not continue to test that deployment. Where a customer has engaged you to test their own environment, that engagement is a matter between you and them; the safe harbour in Section 5 covers you in respect of Sparks Instruments SA only.

5. Safe Harbour

5.1 Our undertaking to you

Sparks Instruments SA considers security research conducted in good faith and in accordance with this policy to be authorised conduct, and a valuable contribution to the security of our users. Where you have complied with this policy, we undertake that:

- We will not initiate, pursue or support any civil claim against you in connection with your research;
- We will not treat your research as a breach of our end-user licence agreement or terms of use, and we waive any contractual prohibition to the extent set out in Section 4.2;
- We will not seek to have your access suspended or your accounts terminated on account of your research;

You do not need to ask our permission before you begin research within the scope of Section 2.1. This policy is that permission.

5.2 Conditions

The safe harbour applies where all of the following are true:

- You acted in good faith, in security research intended to identify, report or help remediate a security issue, without intent to cause harm or to obtain an unauthorised benefit from exploitation;
- You stayed within the scope defined in Section 2.1 and did not engage in any activity prohibited by Section 4.3;
- You reported the finding to us promptly through a channel in Section 3.1, and gave us a fair opportunity to remediate before any public discussion, in accordance with Section 7;
- You did not access, retain, alter or disclose data beyond what was strictly necessary to demonstrate the vulnerability, and you complied with Section 4.4;
- You did not make any demand for payment or other benefit in exchange for disclosure or for silence;
- You complied with applicable law.

5.3 Limits of this safe harbour

Please read this section carefully

This safe harbour is given by Sparks Instruments SA and binds Sparks Instruments SA only. We cannot and do not grant protection on behalf of anyone else. In particular it does not bind our customers, our partners, our suppliers, the operators of any third-party service, or any public prosecutor or other authority, and it cannot displace mandatory criminal law.

If your research affects a system that is not ours, you will need the authorisation of the party that operates it. Nothing in this policy provides that authorisation.

This policy is not a contract and does not create rights for anyone other than as described. It does not limit any right you may have under applicable law.

If you are uncertain whether a planned activity falls within this policy, contact us at cybersecurity@sparksinstruments.com before you carry it out. A question asked in advance will be answered in good faith and will never be held against you.

5.4 If the conditions were not met

Where we reasonably conclude, on documented evidence, that conduct fell outside the conditions of this policy, that decision is taken by our Chief Executive Officer, recorded with reasons, and communicated to you in writing, stating which condition in Section 5.2 we consider was not met. We will give you the opportunity to respond before we take any further step, unless we are prevented from doing so by law or by an ongoing incident.

6. Our Response — Service Levels

We publish the following service levels and hold ourselves to them. They apply to reports received through the channels in Section 3.1.

Stage	Our commitment	What happens
Acknowledgement of receipt	Within 5 business days	A member of our security team confirms that a human has read your report, tells you what happens next, and asks for any detail we still need.
Report asserting active exploitation	Prioritised ahead of every other report	Where your report states that the vulnerability is being exploited in the wild, say so in the subject line. It is escalated as soon as it is read and takes priority over every other report. We are a small team and do not operate rostered out-of-hours cover, so we make no promise of a response time outside business hours — we would rather say that than miss a commitment.
Triage outcome	Within 10 business days	We tell you whether we have accepted the report as a valid vulnerability, could not reproduce it, consider it out of scope, or hold it as a duplicate — with our reasoning in each case.
Progress updates	Every 30 days	For as long as your report remains open, we send you an update on the current stage and on what we expect to happen next, whether or not there is news.
Notification that a fix is available	On release	We tell you when the corrective release is available, give you the CVE reference where one has been assigned, and confirm the intended advisory publication date.
Closure	Within 5 business days of publication	We send you a closing summary of how the report was handled.

The service levels above are internal commitments of Sparks Instruments SA and concern our response to you. We do not publish a fixed remediation deadline: how long a fix takes depends on the nature of the defect, on the components involved and, where the root cause lies upstream, on a third party we do not control. We will always tell you what we expect and why. These service levels are distinct from the regulatory notification deadlines described in Section 7.4, which are set by law and which we do not control.

Definitions used in this section A "business day" is Monday to Friday, 08:00 to 17:00 Central European (Summer) Time, excluding Swiss public holidays. Severity is assessed by us on the facts of the case. We use CVSS where it is informative, but we do not treat a score as decisive.. Where our assessment differs materially from yours, we will explain our reasoning and are willing to reconsider it on argument. These remediation targets are internal targets of Sparks Instruments SA. They are distinct from the regulatory notification deadlines described in Section 7.4, which are set by law and which we do not control.

7. Coordinated Disclosure

We practise coordinated disclosure. The purpose is that users of our products should be able to protect themselves at the moment a vulnerability becomes public, and not before. That requires a short period of confidentiality between your report and publication, and it requires us to use that period to produce a fix rather than to delay one.

7.1 The process

Stage	What we do	What we ask of you
1. Receipt	We acknowledge, allocate a reference and begin triage (Section 6).	Send the report through a channel in Section 3.1 and keep it confidential from this point.
2. Validation	We reproduce the issue, determine the affected version range, assess severity and confirm the finding to you.	Answer our questions where you can, and let us know if you learn anything new — for example that the issue is being exploited.
3. Remediation	We develop, test and sign a corrective release, and prepare a security advisory. We update you at the interval set out in Section 6.	Continue to hold the finding in confidence while we work.
4. Agreement on disclosure	We propose a publication date and, where a CVE applies, the credit wording. We aim to agree the date with you rather than impose it.	Tell us if the proposed date does not work for you, and why. We will try to accommodate it.
5. Publication	We release the fix, notify affected users, and publish the advisory.	You are free to publish your own account from the agreed date.
6. Closure	We send you a closing summary.	—

7.2 Disclosure timeline and embargo

Our default position is that we publish as soon as a corrective or mitigating measure is available, and that we will not ask you to hold a finding confidential beyond 90 calendar days from the date we confirm it as valid without your agreement. Within that period we ask you to keep the finding confidential.

- **We would rather publish early than late. Where the fix is ready sooner, we publish sooner, subject to giving affected users a reasonable opportunity to update. Where remediation is genuinely not complete at 90 days, we will tell you why and propose a new date rather than publish a vulnerability our users cannot yet remedy — but that is a conversation with you, not a decision we take alone.**
- **Extensions are by agreement.** If remediation genuinely requires more than 90 days — for example because an upstream maintainer must act first, or because coordination with other affected vendors is needed — we will explain the reason, propose a new date and seek your agreement. We will not extend silently.
- **Active exploitation shortens the clock.** Where we establish that a vulnerability is being exploited in the wild, protecting users takes priority over the embargo. We may publish an advisory and issue mitigations at short notice, and we will tell you before we do.
- **Publication elsewhere ends the embargo.** If the vulnerability becomes public through any other route, the embargo lapses and we will publish our advisory as soon as we are able.
- **We will not ask for an open-ended embargo.** A request to delay publication will always carry a specific date and a stated reason.

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 12 of 15

7.3 CVE assignment and attribution

Where a report is confirmed as a vulnerability in our product, we will request a CVE identifier and reference it in the advisory. We are not ourselves a CVE Numbering Authority: the request goes to the CNA whose scope covers the affected component, and failing that to the CNA of Last Resort operated by MITRE through its public request form. If the root cause lies in a third-party component, we will coordinate with the upstream maintainer and support their identifier rather than duplicate it.

We will name you as the reporter in the CVE record and in our advisory if you wish. Tell us in your report, or at any time before publication, whether you would like to be named, how you would like to be identified, or that you would prefer to remain anonymous. The default, if you tell us nothing, is that we do not name you.

7.4 Regulatory notification under the Cyber Resilience Act

Sparks Instruments SA places products with digital elements on the market of the European Union and is therefore subject to Article 14 of Regulation (EU) 2024/2847, the Cyber Resilience Act. Where a vulnerability in our product is actively exploited, or where a severe security incident affects it, we are legally obliged to notify the CSIRT designated as coordinator and ENISA within fixed deadlines measured in hours, through the single reporting platform established under Article 16.

What this means for your report That notification is confidential and is made to the authorities alone. It is not a public disclosure and it does not release you, or us, from the embargo agreed under Section 7.2. The obligation is statutory, and we cannot agree to defer or waive it. If your report concerns a vulnerability that we determine is being actively exploited, we will notify the authorities within the statutory deadline, and we will tell you that we have done so — and, where the timetable allows, before we file. Article 14(8) of the same Regulation also obliges us to inform affected users of an actively exploited vulnerability and of the measures they can take. Where that duty is engaged, we will inform users at the point the law requires, which may be before the publication date agreed with you. We will tell you in advance if that becomes necessary. We do not disclose your identity to an authority as part of a notification unless you ask us to, or unless we are legally required to do so.

7.5 Advisories

Security advisories for our products are sent directly to registered customers for any issue affecting a supported version in the field. Each advisory states the affected versions, the severity, the corrective release, any mitigation available to users, and the CVE reference.

Our reporting and disclosure process is designed to ensure that those actively using our products receive timely, direct notifications, keeping them fully informed of what to expect when a vulnerability is addressed.

7.6 If we disagree

It is possible that we will disagree with you about severity, about whether a finding is a vulnerability, or about the publication date. If that happens, we will set out our reasoning in writing and give you the opportunity to answer it. We would rather reach agreement, but we accept that you may decide to publish your own account, and we will not treat a reasoned disagreement, or publication after the 90-day period in Section 7.2, as bad faith or as a breach of this policy.

Publishing your own account. Once the embargo has expired, or once we have published our advisory — whichever comes first — you are free to publish your own account of the finding, including technical detail and proof-of-concept code, and to do so under your own name. We ask only that you say when the issue was reported and when it was fixed, so that readers can judge the timeline for themselves, and that you do not include customer data or anything that would identify a specific installation. We will not ask you to withhold publication indefinitely, and we will not treat publication after embargo as a breach of this policy or of the safe harbour at Section 5.

SPARKS INSTRUMENTS	Coordinated Vulnerability Disclosure Policy	POL-CRA-14-02	
Author: S. Kuenlin	Version: 1.1 Date: 14.09.2026	PUBLIC	Page 13 of 15

8. General Terms

8.1 No bug bounty and no public acknowledgements

Sparks Instruments SA does not operate a bug bounty programme. We do not pay for vulnerability reports, we do not offer swag or other rewards, and we do not maintain a hall of fame or a public acknowledgements page. No submission under this policy creates any entitlement to payment or benefit of any kind.

We state this plainly so that you can decide before you invest your time. What we do offer is set out in Section 1.3 and Section 6: a monitored channel, a named response, a published timeline that we hold ourselves to, the legal assurances in Section 5, and attribution in the CVE record and advisory if you want it (Section 7.3).

8.2 Confidentiality of your report

Your report and the technical detail in it are handled confidentially. They are shared only within the small team handling the issue, with an upstream maintainer where the root cause lies in their component, and with the authorities where the law requires it (Section 7.4). We do not pass your report to any other party without your consent.

8.3 Personal data

If you give us your name, e-mail address or other contact details, we use them solely to coordinate your report, to send you the updates promised in Section 6, and to evidence how the report was handled. We do not use them for marketing and we do not sell or share them.

We retain the correspondence for as long as we are required to evidence our vulnerability handling — under the Cyber Resilience Act this may be for the supported life of the affected product version and for a period afterwards. Your name is not published without your written consent. You may ask us at cybersecurity@sparksinstruments.com what we hold about you, and ask us to correct it.

8.4 Governing law

This policy and any dispute arising from it are governed by Swiss law, with jurisdiction at the registered seat of Sparks Instruments SA — Route de Montena 85, CH-1728 Rossens, Switzerland — without prejudice to any mandatory protection available to you under the law of your place of residence.

8.5 Changes to this policy

We may update this policy. The current version is always the one published at the canonical URL shown in the Document Control table and referenced from our [security.txt](#). Changes take effect on publication and are recorded in the Revision History. The version of this policy in force when you began your research is the version that governs it.

8.6 Contact

Security reports	cybersecurity@sparksinstruments.com
Postal address	Sparks Instruments SA, Security Team, Route de Montena 85, CH-1728 Rossens, Switzerland
security.txt	https://www.sparksinstruments.com/.well-known/security.txt
This policy	https://www.sparksinstruments.com/security/vulnerability-disclosure.pdf
Encryption	PGP public key published on our website and referenced from security.txt
Languages	English, French

Thank you for taking the time to make our products safer.

Annex A — Vulnerability Report Template

You are welcome to use this template. It is a convenience, not a requirement: a report in any form will be handled on the same terms. Please encrypt it with our PGP key where it contains proof-of-concept code or sensitive material.

REPORTER	
Name or pseudonym	[Optional — see Section 3.4]
Contact e-mail	[Required if you would like updates and a triage outcome]
Your PGP key or fingerprint	[Optional — supply this if you would like our replies encrypted]
Attribution preference	☐ Credit me as: [name / handle] ☐ Do not name me ☐ Decide later
Have you reported this elsewhere?	[State any other vendor, CERT / CSIRT, coordinator or platform you have informed, and when]
AFFECTED PRODUCT	
Product	[Which product, and which version]
Version and build	[Exact version and build number]
Component	[Executable, DLL, driver, installer, service or dependency]
Environment	[Operating system, version, architecture, and any relevant configuration]
THE VULNERABILITY	
Summary	[One or two sentences describing the issue]
Vulnerability class	[For example: memory corruption, injection, authentication bypass, insecure deserialisation, path traversal, cryptographic weakness, privilege escalation]
Security impact	[What can an attacker achieve? What is required of them — network position, authentication, user interaction?]
Severity	[Your assessment. CVSS v3.1 or v4.0 vector if you use one]
Steps to reproduce	[Numbered, complete, from a clean installation where possible]
Proof of concept	[Attach separately and encrypted where possible. Describe what it demonstrates]
Supporting evidence	[Logs, screenshots, crash dumps, network captures — with sensitive data removed]
EXPLOITATION AND EXPOSURE	
Do you believe this is being exploited?	☐ Yes — please say so in the subject line, we escalate it first ☐ No ☐ Unknown — [Basis for your view]
Is it already public?	☐ Yes — [where and since when] ☐ No ☐ Unknown
Did you access data that is not yours?	☐ No ☐ Yes — [what, how much, and confirmation that you have retained nothing beyond the evidence described above. See Section 4.4]
DISCLOSURE	
Your preferred publication date	[If you have one in mind. Our default is set out in Section 7.2]
Suggested remediation	[Optional — any fix or mitigation you would suggest]
Anything else we should know	[Free text]

Annex B — Our security.txt

In accordance with RFC 9116, Sparks Instruments SA publishes a security.txt file at <https://www.sparksinstruments.com/.well-known/security.txt>. It is served over HTTPS as text/plain and signed with our PGP key. The fields we publish are as follows.

Field	Value	Meaning
Contact	mailto:cybersecurity@sparksinstruments.com	The address to which security reports should be sent.
Contact	https://www.sparksinstruments.com/security/advisories	Our advisory page, which also states how to reach us.
Encryption	https://www.sparksinstruments.com/.well-known/pgp-key.asc	The key with which you should encrypt the technical content of your report. Fingerprint: BDD3 90F8 8BC6 60D7 5C05 D019 39BD 44C8 E919 44F0.
Canonical	https://www.sparksinstruments.com/.well-known/security.txt	The authoritative location of the security.txt file itself.
Policy	https://www.sparksinstruments.com/security/vulnerability-disclosure.pdf	The canonical location of this policy.
Preferred-Languages	fr, en	The languages in which we accept reports.
Expires	2027-08-31T00:00:00.000Z	The date after which the file should no longer be considered current. We renew it before it expires.

Verifying that you are talking to us

The security.txt file at the canonical location above is the authoritative source of our security contact details and of the location of this policy. If you encounter a different address, key or policy URL presented as ours, please treat it with suspicion and check against the canonical file before sending anything sensitive.

— End of document POL-CRA-14-02 —