Coordinated Vulnerability Disclosure Policy

Coordinated Vulnerability Disclosure (CVD) · LineStrategy product

Regulation (EU) 2024/2847 (Cyber Resilience Act) — Art. 13(17) (single point of contact)

Controlled document

• • •

Document Data

Document	Coordinated Vulnerability Disclosure (CVD) Policy
Organization	Nimax S.p.A.
Document type	Policy
Version	1.0.1
Effective Date	17/09/2026
Last revision	October 20, 2026
Next revision	within 12 months
Document Owner	IT Security — CSIRT Contact
Contact	cybersecurity@nimax.it
Classification	Controlled document

Table of Contents

1. Why This Policy 2
2. Scope of Application 2
3. How to Report a Vulnerability 3
4. What We Do: Our Commitments 4
5. Classification and Fix Times 4
6. Coordinated Disclosure 5
7. Reporter Protection (Safe Harbor) 5
8. Rewards 5
9. Processing of Personal Data 5
10. Escalation 6

1. Why This Policy

The security of the software products we develop is an integral part of their quality. No software is free of defects: what matters is how quickly and transparently we identify and fix them.

Nimax S.p.A. welcomes reports of security vulnerabilities from independent researchers, customers, partners, and suppliers. This document describes how to report a vulnerability to us, what we do when we receive it, and what mutual commitments we undertake.

This policy implements the obligations set forth in Regulation (EU) 2024/2847 (Cyber Resilience Act)—specifically Article 13, paragraph 17 (single point of contact) and Annex I, Part II, points 5 and 6 (coordinated disclosure policy and contact address for reporting)—and is based on the ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability management and resolution) standards.

The effective dates vary: the requirements regarding the single point of contact and the coordinated disclosure policy (Article 13, paragraph 17, and Annex I, Part II, points 5 and 6) apply as of December 11, 2027, and this policy voluntarily anticipates their implementation; the notification obligations set forth in Article 14, on the other hand, are already applicable as of September 11, 2026, and, where the conditions are met, also apply to products already placed on the market.

This policy is written in Italian; in the event of any discrepancy with translations (e.g., into English), the Italian version shall prevail.

2. Scope of Application

2.1 Covered Products and Services

Product	Scope
LineStrategy	All currently supported versions, including server and client components, integration interfaces, and associated cloud services

This scope also includes domains and public systems directly used for the delivery or distribution of LineStrategy.

Research activities are authorized exclusively on environments that Nimax is authorized to access; this excludes customer installations and systems where LineStrategy is installed, as well as third-party systems.

This list is updated whenever a new Nimax product is added to the program. The version published on this page is the official one.

2.2 Exclusions

The following are excluded from this policy:

- third-party products distributed or resold by Nimax, for which reports should be directed to the respective manufacturer (if you contact us anyway, we will act as an intermediary);
- institutional and marketing websites not affiliated with LineStrategy;
- reports that do not describe a concrete security impact, specifically:
  - output from automated scanners lacking manual verification and proof of exploitability;
  - the absence of "best practice" security HTTP headers without a demonstrable attack vector;
  - TLS configuration issues or support for legacy ciphers without a practical exploit;
  - user enumeration, rate limiting, self-XSS, or clickjacking on non-sensitive pages;
  - vulnerabilities requiring unauthorized physical access to the user's device, or a device that has already been compromised;
  - vulnerabilities in versions of LineStrategy that are no longer supported.

2.3 Prohibited Activities

While conducting your research activities, you must not:

- access, modify, exfiltrate, or destroy data that does not belong to you;
- degrade service availability (denial-of-service tests, stress tests, fuzzing on production environments);
- use social engineering, phishing, or pretexting techniques against Nimax employees, customers, or suppliers;
- physically attack Nimax facilities or infrastructure;
- install backdoors, malware, or persistence mechanisms;
- exploit the vulnerability beyond what is strictly necessary to demonstrate its existence.

If you accidentally come across personal or confidential data during your research, stop what you're doing immediately, do not copy it, and report it to us.

3. How to Report a Vulnerability

3.1 Reporting Channel

Email: cybersecurity@nimax.it

This email address is monitored by Nimax staff on business days. It is the single point of contact pursuant to Article 13, paragraph 17 of the Cyber Resilience Act.

If you believe that the technical details or proof of concept are too sensitive to be sent via unencrypted email, please write to us without attaching them: we will arrange a secure channel with you to transmit them.

We accept reports in Italian and English. We accept anonymous reports: you do not need to identify yourself, although a contact channel allows us to ask you for clarification and keep you updated.

Our contact information is also published in a machine-readable format according to the RFC 9116 standard at https://www.nimax.it/.well-known/security.txt

3.2 What to Include in Your Report

The more complete the report, the faster we can fix the issue. If possible, please include:

1. The affected product and version (e.g., LineStrategy 4.2.1) and the environment in which you reproduced the issue;
2. Type of vulnerability (e.g., SQL injection, privilege escalation, data exposure);
3. Steps to reproduce the issue, as detailed as possible;
4. Impact: what an attacker could achieve by exploiting the issue;

5. Prerequisites: Is authentication required? What role? Is access to the internal network required?
6. Supporting material: screenshots, logs, proof of concept, code;
7. If applicable, a CVE identifier that has already been assigned;
8. How you would like to be credited (name, handle, organization) or whether you prefer to remain anonymous;
9. Whether you have a publication commitment (conference, article) with a set date.

4. What We Do: Our Commitments

The timelines and commitments set forth in this document constitute service objectives: they are not guaranteed, do not constitute contractual service levels (SLAs) or third-party rights, and are subject to mandatory legal requirements.

Phase	Nimax Commitment
Acceptance	We will confirm receipt within 2 business days
Initial Assessment	We will notify you of the triage result—confirmed vulnerability, unreproducible, out of scope, or duplicate—within 10 business days
Updates	We'll keep you informed at least every 30 days until the issue is closed
Fix	We address the issue based on its severity (see §5)
Publication	We publish a security advisory in accordance with the criteria in §6 (whichever comes first: availability of the fix, expiration of the 90-day period, or the agreed-upon date).
Acknowledgment	We will credit you in the advisory and on our acknowledgments page, if you wish

Additionally:

- We do not require you to sign a confidentiality agreement as a condition for reporting.
- We do not require you to waive your right to disclose the vulnerability once the agreed-upon period has elapsed.
- If we disagree with your assessment of the severity, we'll let you know and explain why.

5. Classification and Fix Times

We assess severity using CVSS v4.0, supplemented by LineStrategy's real-world usage context. The timeframes indicated begin upon confirmation of the vulnerability and represent our service targets.

The acceptance and initial assessment (triage) begin on the date the report is received through the channel specified in §3.1. The timeframes are calculated in business days, unless otherwise indicated, and may be suspended pending receipt of necessary information from the reporter. These timeframes are operational goals and not contractual obligations.

Severity	CVSS	Remediation Objective
Critical	9.0 – 10.0	15 calendar days
High	7.0 – 8.9	30 calendar days
Medium	4.0 – 6.9	90 calendar days
Low	0.1 – 3.9	Next scheduled release

For critical or actively exploited vulnerabilities, we may release a temporary mitigation or an out-of-cycle patch.

If a LineStrategy vulnerability is found to be actively exploited, or if a serious incident occurs that affects the product's security, Nimax will notify the relevant CSIRT and ENISA in accordance with the terms and procedures set forth in Article 14 of the Cyber Resilience Act. These notification obligations rest with Nimax as the manufacturer; they do not fall on the

reporter and are fulfilled in accordance with the law, which takes precedence over the response times to the reporter specified in this policy.

6. Coordinated Disclosure

- The standard disclosure period is 90 calendar days from confirmation of the vulnerability. This period is a target, adjusted based on risk and available mitigation measures; mandatory statutory deadlines and the notification obligations set forth in §5 remain unaffected.
- We publish the advisory on the earliest of the following: the availability of the fix, the expiration of the 90-day period, or the date agreed upon with you.
- If the fix takes longer (for example, due to a third-party dependency or architectural impact), we will notify you before the deadline and agree on a new date together.
- If the vulnerability is made public by a third party or is found to be actively exploited, we may publish the advisory early to protect users.
- We ask that you not disclose any details before the agreed-upon date.
- We require a CVE identifier for confirmed vulnerabilities affecting already released versions.

Our security advisories are published at: https://www.nimax.it/security/advisories

7. Reporter Protection (Safe Harbor)

If you conduct your research in good faith, in accordance with this policy, and on environments that Nimax is authorized to permit, Nimax S.p.A. undertakes to:

- not initiate or support any legal action against you, whether civil or criminal, in connection with your research activities, subject to legal obligations, requests from competent authorities, and the rights of third parties;
- not to voluntarily report your research activities to the authorities, subject to legal obligations and any obligations to report or cooperate with the competent authorities;
- consider your activities to be authorized only within the environments that Nimax is authorized to permit and within the limits of the LineStrategy license terms; this authorization does not extend to customers' installations and systems or to third-party systems;
- support you, to the extent possible, should a third party take action against you for an activity carried out in compliance with this policy.

This protection does not extend to activities conducted in violation of §2.3, to activities intended for extortion, or to activities on third-party systems or on customers' installations and systems.

If you have any doubts about whether a specific activity falls under this policy, please contact us first at cybersecurity@nimax.it.

8. Rewards

Nimax S.p.A. does not currently operate a bug bounty program and does not pay monetary rewards for reports.

We acknowledge researchers' contributions by crediting them in security advisories and on the acknowledgments page, subject to their consent.

9. Processing of Personal Data

Personal data provided or otherwise processed in connection with the handling of reports is processed by Nimax S.p.A. as the data controller, as follows.

Purposes: management and response to vulnerability reports; compliance with the notification and documentation obligations set forth in the Cyber Resilience Act; potential public recognition of the reporter, subject to their consent.

Legal bases: For the handling of reports and product safety, the data controller's legitimate interest (Art. 6, para. 1, subpar. f, GDPR), subject to a balancing test; for notification and documentation requirements, compliance with a legal obligation (Art. 6, para. 1, subpar. c, GDPR).

Data Processed: The contact information provided by the reporter and any data contained in the report. Even in the case of an anonymous report, personal data may be processed, such as data found in logs, metadata, IP addresses, and attachments.

Recipients: Authorized Nimax personnel (IT Security / CSIRT), any vendors acting as data processors, and, where required by law, the competent authorities (CSIRT / ENISA).

Retention: for the time necessary to handle the report and, subsequently, for the periods required by the documentation obligations of the Cyber Resilience Act; the specific retention criteria and timeframes are defined in consultation with the Privacy Officer/DPO.

Data subjects' rights and contact information: The rights that may be exercised and the contact information for the data controller and the Data Protection Officer are set forth in Nimax's privacy policy, which this section supplements with regard to this specific processing activity.

General Privacy Policy (supplemented by this section): https://www.nimax.it/privacy

10. Escalation

If you do not receive a response within the timeframes specified in §4, or if you believe your report has not been handled appropriately, you may:

1. contact Nimax's IT Department (IT Manager) by emailing cybersecurity@nimax.it and including "Escalation" in the subject line;
2. contact CSIRT Italia (National Cybersecurity Agency), which acts as a trusted intermediary within the framework of coordinated disclosure provided for in Article 12 of Directive (EU) 2022/2555 — https://www.acn.gov.it/portale/csirt-italia