primevision
smart vision, smart flow

CLASSIFICATION:
PUBLIC

Vulnerability Disclosure Policy

Information Security Policy

DOCUMENT TYPE: Policy

Olof Palmestraat 10, 2616 LR Delft, The Netherlands | +31 15 219 2090 | www.primevision.com

primevision
smart vision, smart flow

Document History

General Information

Document Info	Property in Document Info
Product Name	Information Security Policy
Document Name	Vulnerability Disclosure Policy
Date	28.10.2026
Release	Final
Owner	Security Team
Version Number	1.0
Review frequency	Annual
Classification	Public

Revision History

Version	Revision Date	Summary of Changes
1.0	30.10.2026	Initial version.

primevision
smart vision, smart flow

Table of Contents

Document History **2**

General Information *2*

Revision History *2*

1. Purpose **4**

2. Scope **4**

3. How to report **4**

4. Rules for responsible testing **5**

5. Information to include **5**

6. What to expect **6**

7. Safe Harbour **6**

8. Coordinated disclosure **6**

9. Recognition **7**

10. Data protection and confidentiality **7**

1. Purpose

Prime Vision takes the security of its products seriously and is committed to maintaining the confidentiality, integrity and availability of our products and services. We welcome reports from customers, partners, security researchers and anyone who discovers a potential security vulnerability in our products. We review reports in good faith, work with the reporter and prioritize actions to protect our customers and their operations.

Our products are typically supplied to businesses and deployed in customer-controlled environments, rather than made available on the public internet. This policy outlines how vulnerabilities identified in our products can be reported responsibly; it is not an invitation to access customer networks or installations.

2. Scope

This policy applies to security vulnerabilities identified in products with digital elements developed or maintained by Prime Vision such as sorting solutions, computer vision solutions, flow projector and robotics hardware and other application

Reports concerning products outside their support period are also welcome, but a report does not extend support or guarantee a fix.

If you identify a potential vulnerability affecting our product through a third-party component, we encourage you to report it to the respective manufacturer or maintainer.

This policy does not authorize testing of customer networks, third-party services or infrastructure, or Prime Vision's corporate IT, websites and public services. You may still report a suspected issue discovered without testing.

Only test products and environments you own or have explicit permission to test. Testing a customer installation requires prior authorization from the customer and any other party controlling the affected systems.

3. How to report

Please report a potential vulnerability by sending an email to securityofficer@primevision.com. Customers may also use their agreed support channel and ask for the report to be passed to the Security Team.

Start with a concise description. Do not send credentials, customer data or sensitive exploit material in an unencrypted email. If sensitive evidence is needed, encrypt it or ask us to agree a secure transfer method.

Please do not disclose the issue publicly until we have had a chance to review and respond.

4. Rules for responsible testing

Keep testing limited to what is needed to demonstrate the issue, preferably in an isolated test environment. In particular:

- do not access data that does not belong to you,
- do not modify, delete, or exfiltrate data,
- do not disrupt services, perform denial-of-service tests, establish persistent access or exploit identified vulnerabilities
- if you unintentionally gain access to data belonging to others, stop testing and inform us immediately,
- Keep vulnerability details confidential while we coordinate investigation, remediation and disclosure.

5. Information to include

To help us review your report as quickly as possible please include the following information:

Field	Description
Vulnerability type	e.g. CWE or OWASP category if applicable
Affected asset	E.g. product, software or service name and version, hardware model and type or URL for web applications.
Technical description	A clear and detailed description of the vulnerability.
Steps to reproduce	Minimal reproduction steps and the access or privileges needed.
Discovery date	Date and time of discovery and, where relevant, IP addresses used during research and redacted screenshots or logs, if available.
Potential impact	Your assessment of exploitability and impact on confidentiality, integrity and availability and whether exploit has been observed
Suggested remediation	Appreciated, but not required
Contact information	A way to contact you, if you want follow-up.

Do not include parcel labels, personal data, credentials or other customers' information. Describe accidental exposure without sending the exposed data. We can agree how to transfer additional evidence or large files if needed.

6. What to expect

Our Security Team coordinates the report with the relevant product team and, where needed, customer support. We record the report, provide a reference for follow-up and assess its severity in the context of the affected product and deployment.

Upon receipt of your report, we are committed to acknowledge your report within 7 days.

We will provide status updates during investigation and aim to have a remediate plan for confirmed vulnerabilities within 90 days.

We prioritize active exploitation, physical safety and significant operational or data risks. Depending on the issue, we may provide a workaround, configuration guidance, an update or replacement guidance. Deployment is coordinated with affected customers to allow testing and safe installation. Customer-specific support and maintenance arrangements remain applicable; this policy does not replace contractual or statutory obligations.

7. Safe Harbour

Prime Vision will not pursue legal action for good-faith research carried out in accordance with this policy and within the permissions granted by the relevant system owner. Within Prime Vision's authority, we consider such research authorized. If you make a mistake, stop and report it promptly so we can work together to limit any harm.

Prime Vision cannot authorize access to customer or third-party systems, waive their rights or provide protection against action by others. This statement does not remove statutory obligations or override agreed testing conditions.

8. Coordinated disclosure

Please coordinate public disclosure with us. After validation, we agree a disclosure date based on severity, remediation complexity and safe customer deployment. We aim to agree a plan within 90 calendar days of receipt. Where additional time is required, the reasons will be explained to the reporting person and an appropriate timeline coordinated.

We notify affected customers through agreed support or account channels, with mitigation and update instructions. Where wider disclosure is appropriate or required, we issue an advisory through

a suitable public channel agreed for the case, protecting customer identities, installation details and information that could unnecessarily aid exploitation.

We may share technical information needed for investigation and remediation with affected customers, suppliers, maintainers, vulnerability coordinators or competent authorities, on a need-to-know basis with appropriate confidentiality safeguards. Mandatory reporting and other legal obligations override agreed disclosure dates.

9. Recognition

With your consent, we may acknowledge your contribution by name or pseudonym in our security advisories once the issue is resolved and disclosed. We respect requests to remain anonymous.
This policy is not a bug bounty program and does not create an entitlement to payment, rewards or public recognition.

10. Data protection and confidentiality

We treat reports and reporter details as confidential and process personal data only as necessary to assess and handle the report, communicate with the reporter and meet applicable legal obligations. Access is restricted to those who need it. We do not publish your identity without your consent.

When technical details must be shared for coordination, we remove unnecessary personal and customer information. Reporter's contact details are shared only with consent or where legally required. Report records are retained in line with applicable retention requirements and deleted when no longer needed.

Please only submit personal data that is necessary for processing the report.