

Vulnerability Disclosure Policy

DOCUMENT ID ATX-SOC-06	TITLE Vulnerability Disclosure Policy
VERSION 1.0	CLASSIFICATION Public
OWNER Security Officer	APPROVED BY Chief Executive Officer
EFFECTIVE DATE 10 August 2026	NEXT REVIEW August 2027
STANDARDS MAPPING ISO/IEC 27001:2022 Annex A 5.6, 6.8, 8.8; SOC 2 TSC CC2.2, CC2.3, CC7.1, CC7.2	

1. Purpose

Atlastix accepts reports of security vulnerabilities in the systems it operates and in the software it ships from customers, MSPs, security researchers and any other party. This policy explains how to report a vulnerability, how Atlastix handles reports, and the safe harbour extended to qualifying good-faith research.

2. Scope

This policy covers:

- Systems operated by Atlastix** - websites and services under atlastix.io, and Atlastix's own cloud, build and corporate systems.
- Software shipped by Atlastix** - released versions of Atlas Automate, Atlastix Observability and Atlastix Device Intelligence, and product extensions, integrations, customisations and custom software solutions delivered by Atlastix, as deployed in customer or MSP tenancies. Reports about vulnerabilities in shipped or delivered software are accepted regardless of where the software is deployed.

It applies to any person reporting a vulnerability and to all Atlastix personnel handling reports.

Out of scope: underlying infrastructure operated by cloud, source-control or other service providers, which should be reported under that provider's programme; a customer's or MSP's own tenancy, including its infrastructure, account configuration and workflow logic; and denial-of-service, volumetric, social-engineering or physical-intrusion testing, which must not be performed under this policy.

Testing note: Atlastix cannot authorise testing against systems it does not operate. Testing a deployed instance of Atlastix software requires authorisation from the customer or MSP operating that instance, or use of an instance controlled by the researcher. The section 6 safe harbour extends only to systems Atlastix operates and activity Atlastix has legal authority to permit.

3. How to report

Email the monitored mailbox support@atlastix.io with:

- a description of the issue and where it was found;

- the affected product, version, URL or system;
- reproducible steps or a proof of concept where possible;
- the potential impact as the reporter assesses it; and
- contact details if follow-up or updates are requested.

Anonymous reports are accepted, although Atlastix cannot provide direct updates without contact details.

Do not include another organisation's data in a report. If data that is not yours is encountered, stop testing, note the minimum information needed to identify what happened, and report it. Do not copy, retain, modify, delete or further access that data. Credentials, tokens and secrets must not be included in a report unless Atlastix specifically provides a secure method and requests them.

4. How Atlastix handles reports

Reports are handled under the management-approved Incident Response Plan (ATX-RES-01) and Vulnerability and Patch Management Policy (ATX-TEC-07):

1. **Recording.** The report is entered into the applicable incident or vulnerability record and assigned an owner.
2. **Triage and severity assessment.** The Security Officer coordinates initial assessment; the Engineering Lead validates the finding and evaluates severity, exploitability, exposure and affected versions.
3. **Containment and remediation.** Atlastix develops a fix, mitigation or risk treatment appropriate to systems it operates and coordinates shipped-software action with affected customers or MSPs.
4. **Customer deployment coordination.** Atlastix may issue advisories, release information and upgrade guidance. Applying a released update within a customer or MSP tenancy remains the tenancy operator's responsibility unless the applicable agreement says otherwise.
5. **Reporter communications.** Atlastix may request further information and provide validation, progress or resolution updates where contact details are available.
6. **Credit, with consent.** A reporter who requests acknowledgement may be credited after coordinated disclosure and remediation, subject to legal, security, contractual and customer restrictions. Atlastix does not operate a paid bug bounty programme, and this policy creates no entitlement to payment.

Response, remediation, support, notification and communication timing is governed by the applicable customer agreement and circumstances. Atlastix does not publish a universal acknowledgement, fix or remediation service level in this policy.

Vulnerability reports and handling records are retained as ISMS records and may be considered in management review and corrective-action processes (ATX-GOV-09, ATX-GOV-10, ATX-GOV-11).

5. Rules of engagement

To remain within this policy, researchers must:

- act in good faith and comply with applicable law;
- make a good-faith effort to avoid privacy violations, service degradation, data modification and data destruction;
- use only accounts, data, systems and tenants they control or are expressly authorised to test;
- not access, modify, delete, copy or retain data that is not their own;

- not perform denial-of-service, volumetric, spam, social-engineering or physical attacks against Atlastix, its personnel, providers, customers or MSPs;
- stop testing and report promptly after confirming a vulnerability or encountering personal information, customer data or end-client data;
- avoid actions that establish persistence, pivot to other systems or exceed the minimum necessary to demonstrate the issue;
- allow reasonable time for investigation and remediation, and coordinate public disclosure with Atlastix; and
- not demand payment as a condition of disclosure.

6. Safe harbour

Atlastix considers security research against systems it operates to be authorised when conducted in accordance with this policy, and:

1. will not initiate or support legal action, or refer the matter to law enforcement, in respect of good-faith research that complies with this policy;
2. waives, to the extent of its rights, restrictions in its terms of service that would otherwise prohibit such research, for activity conducted in compliance with this policy; and
3. will state that the research was authorised if a third party initiates action against a researcher for policy-compliant activity, where Atlastix can lawfully and accurately do so.

This safe harbour does not extend to activity outside section 5, research against provider infrastructure, customer or MSP tenancies, or any system Atlastix does not operate. It does not cover conduct that Atlastix has no legal power to authorise. Obtain the tenancy operator's authorisation before testing a customer or MSP tenancy, or use an instance you control. If uncertain whether intended testing is in scope, ask support@atlastix.io before proceeding.

7. Responsibilities

The **Security Officer** owns this policy, oversees the monitored reporting mailbox, triages reports, communicates with reporters and coordinates disclosure. The **Engineering Lead** validates findings, identifies affected versions, develops fixes or mitigations and records closure evidence. The **CEO** approves public acknowledgements and material external statements. **All Personnel** promptly forward any vulnerability report they receive to support@atlastix.io and preserve its confidentiality.

For a vulnerability in a customer or MSP deployment, the tenancy operator controls testing authorisation, production access and application of released updates. Atlastix controls its shipped-software investigation and remediation work. Customer and end-client communications are coordinated according to the applicable agreement; the MSP owns onward end-client notification unless otherwise agreed.

8. Exceptions

No exception may remove safe harbour for research that complies with this policy. Any process exception follows the ISMS exception and risk-acceptance process and cannot authorise Atlastix to permit testing of a system it does not operate.

9. Enforcement

Reports or testing outside the rules of engagement may lose the protection of section 6 and are handled under the Incident Response Plan and applicable law. Internal mishandling of reports is managed under personnel, incident and corrective-action procedures.

10. Related documents

ATX-RES-01 Incident Response Plan; ATX-TEC-07 Vulnerability and Patch Management Policy; ATX-GOV-02 Information Security Policy; ATX-GOV-09 Management Review; ATX-GOV-10 Nonconformity and Corrective Action; ATX-GOV-11 KPIs & Measurement; ATX-SOC-03 Atlastix Security Whitepaper; ATX-SOC-08 Security Terms & Control Position.

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	10 Aug 2026	Initial release	Chief Executive Officer