

Security Terms & Control Position

DOCUMENT ID ATX-SOC-08	TITLE Security Terms & Control Position
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 5.20, 5.24, 5.26, 5.34, 8.10; SOC 2 TSC CC2.3, CC6.5, CC7.4, CC9.2, A1.2, A1.3	

1. Purpose

This document summarises security, notification and data-handling topics for contract review across Atlas Automate, Atlastix Observability, Atlastix Device Intelligence, product extensions, integrations and custom software solutions. The executed customer agreement and data-processing terms define binding scope, responsibilities, timing and remedies.

2. Scope

Current delivery is generally in customer- or MSP-controlled cloud tenancies. Deployment-specific architecture, data flows, locations, retention and operational responsibilities are governed by the deployed configuration and applicable agreement. These topics cover what Atlastix controls: development, customisation, release, delivery and support; corporate systems; approved customer data it receives across those activities; and the conduct of its personnel. The current Device Intelligence customer annex is in section 4.

3. Security topics

#	TOPIC	CURRENT POSITION	CONTROL REFERENCE
1	Shipped-software security	Release changes use security consideration, pull-request change control with senior review of junior-authored changes, applicable automated checks, pre-release testing and controlled delivery. Confirmed vulnerabilities are handled through the vulnerability-management process.	ATX-ENG-01, ATX-ENG-02, ATX-TEC-07
2	Release integrity	GitHub Actions builds releases and GitHub Actions artifacts or GitHub Releases store them. Each unique version traces to the exact commit and workflow run that produced it. Atlastix provides upgrade and rollback or recovery guidance appropriate to the change.	ATX-ENG-01, ATX-ENG-02
3	Shipped-software vulnerability response	Atlastix risk-ranks confirmed vulnerabilities and provides fixes, mitigation guidance, advisories and support according to severity, exploitability, exposure and the applicable agreement. No universal public remediation period applies.	ATX-TEC-07, ATX-SOC-06

#	TOPIC	CURRENT POSITION	CONTROL REFERENCE
4	Customisation and custom-solution change control	Per-deployment customisations and custom software follow management-approved change control with senior review of junior-authored changes, applicable automated checks, testing and versioned delivery, with rollback or recovery procedures proportionate to the change.	ATX-ENG-01, ATX-ENG-02
5	Approved engagement-data handling	Customer-approved extracts or uploads, and temporary customer-tenancy access, are used only for an approved engagement; protected through the approved service or tenancy configuration; limited to named engagement personnel; and recorded with owner, purpose, location, retention and deletion due date. Data content, location and lifecycle are deployment- and agreement-specific.	ATX-ENG-05, ATX-ENG-06, ATX-TEC-03
6	Dataset retention and deletion	Primary copies are retained and deleted under the applicable product, deployment and agreement; storage-level replicated copies follow the primary and are deleted with it. Atlastix provides written confirmation where required by the applicable agreement. The current Device Intelligence lifecycle is stated in section 4.	ATX-ENG-06
7	Deployment data paths	Extracts, uploads, temporary access and any ongoing integration or feed require a documented purpose, approved scope, security and retention controls and applicable customer terms. The absence of a feed is not asserted globally; the current Device Intelligence position is stated in section 4.	ATX-ENG-05, ATX-ENG-06, ATX-TEC-01
8	Support-access conduct	Access into a customer or MSP tenancy occurs only as customer-granted, temporary, scoped to the task, and logged in the customer's environment; personnel are bound by confidentiality and acceptable use obligations.	ATX-TEC-01, ATX-PPL-01
9	Incident notification	Atlastix coordinates and provides customer notification according to the applicable customer agreement, legal obligations and incident circumstances. The MSP owns onward end-client notification unless otherwise agreed. No universal public notification period applies.	ATX-RES-01
10	Data breach cooperation	Incidents involving personal information are assessed under the Notifiable Data Breaches scheme where applicable, and Atlastix provides cooperation required by applicable law and the customer agreement.	ATX-RES-05
11	No training on customer data	Customer data received by Atlastix is processed only for approved purposes, is not sold and is not used by Atlastix to train AI models. Provider treatment of data sent through a customer's AI account follows the customer's provider terms and configuration.	ATX-PPL-06, ATX-ENG-07
12	Subprocessor and AI-provider transparency	Current Atlastix-managed processing and known corporate-tool context are published in ATX-SOC-07. Atlastix currently operates no AI model-provider account receiving customer workflow content; current AI use is through customer provider/accounts/keys or customer cloud-native services. An Atlastix-managed provider is prohibited until separately approved and disclosed before customer content flows.	ATX-PPL-05, ATX-ENG-07
13	Assurance status and sharing	Public assurance materials are maintained in the Trust Centre. Controlled documentation and future third-party assurance materials are shared subject to applicable confidentiality and distribution terms.	ATX-SOC-05
14	Security review	A management-led documentation and control walkthrough may be arranged under confidentiality. The applicable agreement defines audit rights and the scope of supporting-record access.	ATX-SOC-04, ATX-GOV-08

#	TOPIC	CURRENT POSITION	CONTROL REFERENCE
15	Vulnerability disclosure	A public disclosure channel at support@atlastix.io with safe harbour for qualifying good-faith research covers Atlastix-operated systems and reports about shipped software. Response timing follows applicable terms rather than a universal public service level.	ATX-SOC-06, ATX-TEC-07

4. Current Device Intelligence customer annex

The current Device Intelligence deployment is a staging instance in the MSP tenancy, in user acceptance testing ahead of production; workloads and primary data there remain under the MSP's controls. There is no separate ongoing Device Intelligence product or telemetry feed to Atlastix for this deployment. Approved paths are a customer-approved point-in-time extract or support upload processed in an access-restricted Atlastix Azure environment in Australia East, or temporary access within the MSP tenancy. Extracts and uploads exclude credentials, tokens and secrets. Primary copies are deleted within 30 days after the engagement ends; storage-level replicated copies follow the primary and are deleted with it, and no separate backup copies are currently retained.

The current Device Intelligence deployment uses the customer's AI provider, account and keys, or a customer cloud-native service. No Atlastix-managed AI provider is used for this deployment. The customer controls provider terms, configuration and processing location.

Because this Device Intelligence deployment runs in the MSP tenancy, several controls depend on the customer or MSP. Applicable agreements identify complementary controls including securing the tenancy (infrastructure, network and access management), operating backups and availability, applying released updates under applicable terms, following deployment and hardening guidance, granting and revoking scoped support access, keeping connector credentials, tokens and secrets in the MSP tenancy and unavailable to Atlastix personnel, excluding them from extracts and uploads, controlling the customer AI provider/account/keys, and maintaining current security and operational contacts.

5. Responsibilities

The **CEO** approves customer agreements and authorised deviations from this summary. The **Security Officer** maintains this document, coordinates agreement consistency, incident communications, engagement-data records and customer review. The **Engineering Lead** operates technical controls including release integrity, vulnerability handling, customisation change control and deletion. **All Personnel** are bound by applicable underlying policies.

6. Exceptions

Binding variations are agreed only through an applicable customer agreement or approved change, never informally. No exception may override applicable law. Incident notification, support and vulnerability-response timing remain governed by the applicable agreement rather than this public summary.

7. Enforcement

Only terms included in an executed customer agreement have contractual force. Internal non-compliance is managed under ATX-PPL-02 and the corrective-action and management-review processes (ATX-GOV-09, ATX-GOV-10).

8. Related documents

ATX-SOC-01 System Description; ATX-SOC-03 Atlastix Security Whitepaper; ATX-SOC-04 Vendor Security Questionnaire - Self-Assessment; ATX-SOC-05 Assurance Materials & Framework Status; ATX-SOC-06 Vulnerability Disclosure Policy; ATX-SOC-07 Subprocessor & Hosting Register; ATX-RES-01 Incident Response Plan; ATX-RES-05 Breach Notification Procedure; ATX-ENG-05 Data Classification & Handling Policy; ATX-ENG-06 Data Retention & Disposal Policy; ATX-ENG-07 AI Governance & Responsible Use Policy.

Revision history

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