

Atlastix Security Whitepaper

DOCUMENT ID ATX-SOC-03	TITLE Atlastix Security Whitepaper
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 (reference framework); SOC 2 Trust Services Criteria - Security, Availability (reference framework); Privacy Act 1988 (Cth) / APPs	

1. About Atlastix

Atlastix is an Australian software company headquartered in Sydney, with a team of 6–15 people. It develops products and custom software solutions for customers, including:

- **Atlas Automate** - a workflow automation platform for business processes (accounts payable, IT service management, security operations, compliance workflows) with AI decision-making and audit trails.
- **Atlastix Observability** - an observability platform deployed as an in-tenancy collector; customer metrics, logs and traces remain in the customer tenancy. Operational telemetry reaches Atlastix only where disclosed and approved under the applicable agreement.
- **Atlastix Device Intelligence** - a platform customised per deployment and deployed into managed service providers (MSPs). MSP staff and the MSP's customers log in to Device Intelligence. It can ingest data from dozens of customer-configured source platforms via API integrations, including ITSM (for example ServiceNow), endpoint management (Intune and Microsoft Graph), security (Defender, CrowdStrike and Tenable), monitoring (LogicMonitor and others), and ERP systems. It supports MSP planning, insights, customer service and uplift programmes, and customer-facing insights on desktop health, device lifecycle and user experience.
- **Product and custom software solutions** - product extensions, integrations, workflow implementations and customer-specific software designed, built and delivered under agreed requirements.

This whitepaper describes the security controls governing software Atlastix develops and ships, approved customer data it receives, and its own environment. The ISMS assigns control ownership across governance, risk, engineering, data, people, suppliers and resilience. ISO/IEC 27001:2022 and the SOC 2 Security and Availability criteria are used as control references.

2. Deployment model and shared responsibility

Current delivery is generally into customer- or MSP-controlled cloud tenancies. The tenancy operator controls the production cloud environment, while Atlastix controls the software and customisations it develops and delivers and the activities and data within its own environment. The exact architecture, integration paths, data flows, operational responsibilities and support model are governed by the deployed

configuration and applicable agreements. The current Device Intelligence deployment is a specific example described in section 7.

Responsibility divides as follows:

AREA	CUSTOMER / MSP	ATLASTIX
Infrastructure, network and account security of the deployment tenancy	Owns	-
Backups, capacity and availability of the deployed software	Owns	-
Access management for users of the deployed software	Owns	-
Applying released updates and security fixes	Owns, under applicable release and agreement terms	Provides releases, advisories and guidance under applicable terms
Security of the shipped software (code, dependencies and build)	-	Owns
Customisations delivered by Atlastix	Operates	Builds under change control
Hardening and deployment guidance	Applies	Provides as applicable to the release
Atlastix development, build and corporate environment	-	Owns
Customer-approved extracts or uploads for an engagement	Provides under approved terms	Holds and protects under the deployment- and agreement-specific location and lifecycle
Temporary support access into a customer or MSP tenancy	Grants, scopes, logs and revokes	Uses only as granted and for the approved purpose

Atlastix's own cloud accounts and approved SaaS services support development, build/CI, testing, customisation, release, delivery, support, approved engagement-data processing and corporate workloads. They are not generally used to host current customer production workloads.

3. What customer data Atlastix holds

Across its products and custom solutions, Atlastix may hold three categories of customer-related data:

- 1. Customer-approved extracts or uploads.** A customer or MSP may provide data for a defined development, customisation, testing, delivery or support engagement. It may include personal information and end-client data where necessary and approved. Credentials, tokens and secrets must be excluded unless an agreement and approved secure process specifically require them.
- 2. Temporary customer-tenancy access.** A customer or MSP may grant named Atlastix personnel temporary, scoped and logged access for an approved engagement instead of transferring a copy.
- 3. Business and support data.** HR/personnel records are held in Microsoft 365; financial and payroll-related records in Xero; sales, marketing and suppression records in an in-house CRM protected by Entra SSO and encryption; website enquiries are delivered through EmailJS from the Atlastix marketing and trust websites; and support@atlastix.io creates Jira Service Management tickets.

Location, retention and deletion follow the deployed configuration and agreement. Some deployments may include agreed integrations or continuing data flows. Current Device Intelligence deployment facts are stated in section 7.

4. Secure development and release integrity

- **Secure SDLC.** Product code, customer-specific customisations, custom software and Atlastix infrastructure-as-code changes are governed by security consideration at design, pull-request change control with senior review of junior-authored changes, applicable automated security checks and disciplined pre-release testing (ATX-ENG-01).
- **Change management.** Changes are tested and approved under the change management procedure; emergency changes require authorised approval and retrospective review (ATX-ENG-02).
- **Versioned release traceability.** GitHub Actions builds releases and GitHub Actions artifacts or GitHub Releases store them. Each unique version is traceable to the exact commit and workflow run that produced it. Upgrade and rollback procedures are documented as applicable to the change.
- **Hardening guidance.** Product deployment and hardening guidance identifies the secure configuration assumptions applicable to a release.
- **Vulnerability management.** Findings are risk-ranked according to severity, exploitability and exposure. Fix, mitigation, support and notification timing for shipped software follows the applicable agreement and release terms (ATX-TEC-07).
- **Security testing.** Atlastix performs automated dependency scanning via GitHub Dependabot on its release repositories; broader vulnerability-assessment tooling run against builds carrying the same security baseline deployed to customer nodes is a planned activity. Its platforms also run within customer and MSP-controlled networks that apply their own security controls and testing. Independent third-party penetration testing is a planned activity; none is currently engaged (ATX-TEC-07, ATX-GOV-05).
- **Vulnerability disclosure.** The public Vulnerability Disclosure Policy (ATX-SOC-06) provides a channel and safe harbour for qualifying good-faith research. Reports go to support@atlastix.io.

5. Approved engagement data

Where an approved product or custom-solution engagement requires customer data, Atlastix applies the following controls (ATX-ENG-05, ATX-ENG-06):

- Contractual authority and confidentiality terms are established before transfer, with the engagement and access approved.
- Data is accepted through a customer-approved extract or upload into an access-restricted environment, or accessed temporarily within the customer tenancy. The approved method and processing location are deployment- and agreement-specific.
- Raw data may contain personal information or end-client data where necessary and approved; credentials, tokens and secrets are excluded.
- Encryption is applied in transit and at rest through the approved Azure service configuration (ATX-TEC-03).
- Access is limited to named personnel working on the engagement, logged and removed when no longer required.
- A record identifies the data owner, approved purpose, storage location, applicable retention and deletion due date.
- Primary copies are retained and deleted under the product-, deployment- or agreement-specific lifecycle; storage-level replicated copies follow the primary and are deleted with it. The current Device Intelligence lifecycle is stated in section 7.

- Data is not copied to endpoints except where specifically approved and necessary, and is not used to train AI models.

Temporary, named and logged access within the customer or MSP tenancy may be used instead. The tenancy operator grants and revokes that access, and Atlastix personnel use it only for the approved purpose.

6. AI security and governance

Atlastix currently operates no AI model-provider account that receives customer workflow content. Current products and custom solutions use the customer's provider account and keys or a cloud-native model service in the customer's tenancy. The applicable configuration and agreement identify account ownership, approved purposes, data path and processing location. An Atlastix-managed provider is prohibited until separately approved through supplier, subprocessor, privacy, risk and customer review before any customer content flows.

Credentials, tokens and secrets must not be included in prompts, extracts or support uploads unless an approved design and secure process expressly require them. AI-assisted processing is governed through deployment configuration, authorised-purpose limits, scoped tool permissions, human-review controls where applicable, change control, testing and deployment audit records (ATX-RSK-02, ATX-ENG-01, ATX-ENG-07).

Customer data supplied to Atlastix is not used to train AI models.

7. Current Device Intelligence customer annex and security example

The current Device Intelligence customer deployment is a staging instance in the MSP's cloud tenancy, in user acceptance testing ahead of production. Workloads and primary data remain there under the MSP's controls, and Atlastix does not host that workload. There is no separate ongoing Device Intelligence product or telemetry feed to Atlastix for this deployment.

The approved Device Intelligence data paths to Atlastix are customer-approved point-in-time extracts or support uploads processed in an access-restricted Atlastix Azure environment in Australia East, or temporary access within the MSP tenancy. Extracts and uploads may include personal information and end-client data where approved, but 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.

AI features for the current Device Intelligence deployment use the customer's model provider, account and keys, or a customer cloud-native model service. No workflow content is sent to an Atlastix-managed AI provider. The customer controls the provider relationship, terms, configuration and processing location.

Device Intelligence can touch end-client data, MSP operational data (including tickets, configurations, billing and staff identities), and connector credentials for source systems such as ITSM, endpoint management, security, monitoring and ERP platforms.

- **Integration scopes.** Integration scopes are primarily for ingestion, with defined write-backs where configured, such as ticket creation. Least privilege is the design principle, and enabled permissions and write paths are determined by the deployed connector configuration.
- **Credential handling.** Connector credentials, tokens and secrets generally remain in the MSP tenancy and are excluded from point-in-time extracts and support uploads. Where the MSP provides a

credential to Atlastix for customisation or support, it is handled under the ATX-TEC-02 access and secrets controls: stored only in 1Password Business or the secrets services defined in ATX-TEC-03, never in code, tickets or chat, and rotated or revoked on suspected compromise.

- **Multi-tenancy.** Where an MSP instance serves multiple end clients, the MSP is responsible for configuring and operating role- and tenant-based segregation within its tenancy.
- **Customisation change control.** Per-deployment customisations are subject to the secure development and change controls in section 4, with delivery and rollback records appropriate to the change.
- **Data handling.** Approved extracts or uploads containing MSP or end-client data are handled under section 5 and the specific Australia East location and 30-day post-engagement deletion lifecycle stated above. The MSP remains responsible for its authority to provide end-client data.
- **Access.** Atlastix has no standing requirement for production access. Any in-tenancy access is temporary, named, logged and controlled by the MSP for an approved engagement.

8. Corporate environment security

Atlastix's management-approved control framework covers its development, build/CI, approved engagement-data and corporate systems:

- **Identity and access.** Controls require named identities, least privilege, MFA where supported, documented approval for privileged access, periodic access review and prompt revocation when access is no longer required (ATX-TEC-01, ATX-TEC-02).
- **Cloud configuration.** Atlastix cloud environments are governed by configuration baselines, logging and change controls (ATX-TEC-05, ATX-TEC-06).
- **Endpoints.** Approved endpoints are subject to encryption, screen-lock, update and endpoint-protection requirements; customer data may not be stored on unmanaged devices (ATX-TEC-08, ATX-PPL-03).
- **Logging and monitoring.** Applicable cloud, source-control and corporate audit records exist at the applicable service configuration and are governed under the logging and monitoring policy, which defines the target centralisation, retention and alerting architecture (ATX-TEC-04).
- **Controlled records.** ISMS documents, engineering runbooks and the threat-intelligence register are maintained in access-controlled GitHub repositories.
- **Personnel.** Personnel are subject to role-appropriate screening, confidentiality obligations, acceptable-use acknowledgement and security-awareness requirements (ATX-PPL-01, ATX-PPL-02, ATX-GOV-06).
- **Governance.** The CEO has ultimate accountability, the Security Officer coordinates the ISMS, and the Engineering Lead owns engineering controls. Roles are consolidated (ATX-GOV-02, ATX-GOV-03).

9. Incident response and continuity

- **Response.** The Incident Response Plan (ATX-RES-01) defines roles, severity assessment, escalation, communications, post-incident review and corrective-action handling. Response and support timing follows the applicable agreement.
- **Customer notification.** Customer notification timing and content follow applicable customer agreements, legal obligations and the incident circumstances. Notifications use nominated customer email contacts and Jira Service Management where applicable. For Device Intelligence, incidents are coordinated with the MSP, which owns onward end-client notification unless otherwise agreed.

- **Privacy.** Incidents involving personal information are assessed under applicable privacy obligations, including the Notifiable Data Breaches scheme where it applies (ATX-RES-05).
- **Continuity.** Atlastix continuity controls cover development, customisation, release, delivery, support, approved engagement-data processing and corporate systems. Customers or MSPs generally operate backup, capacity, recovery and availability for deployments in their tenancies, including the current Device Intelligence deployment.

Atlastix does not publish a universal incident-response, customer-notification, support or availability service level.

10. Framework status

Atlastix operates a management-approved ISMS aligned to ISO/IEC 27001:2022, with its controls mapped to the SOC 2 Security and Availability criteria; both are used as control references. Independent ISO/IEC 27001 certification and a SOC 2 examination are targets and are not yet held. ATX-SOC-05 describes the assurance materials available for customer review. Customer and MSP tenancies and customer-operated controls remain outside the Atlastix control boundary.

11. Contact and due diligence

- **Contact:** support@atlastix.io, which creates Jira Service Management tickets, for security questions, due diligence requests, support matters and vulnerability reports (ATX-SOC-06 sets the disclosure terms and safe harbour).
- **Questionnaire:** the public self-assessment (ATX-SOC-04) is available, and Atlastix may respond to reasonable customer-issued questionnaires.
- **Contractual commitments:** public context is provided in ATX-SOC-08.
- **Walkthrough:** a management-led control walkthrough may be arranged under confidentiality, subject to legal, security, contractual and customer restrictions. Raw internal records are not promised for external distribution.

Revision history

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