

Vendor Security Questionnaire - Self-Assessment

DOCUMENT ID ATX-SOC-04	TITLE Vendor Security Questionnaire - Self-Assessment
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	

This self-assessment answers 77 questions commonly asked in supplier due diligence questionnaires. Answers are current as at 10 August 2026 and reference Atlastix documentation by ID. The public trust documents are ATX-SOC-03 to ATX-SOC-08. Detailed policies, registers and deployment records are available through the controlled document tier. Direct questions and walkthrough requests to support@atlastix.io.

1. Company and governance

- Q1: Provide a brief description of your company and the products being assessed.** **A:** Atlastix is an Australian software company headquartered in Sydney with 6–15 personnel including contractors. It develops Atlas Automate (AI-powered workflow automation), Atlastix Observability (an observability platform designed for in-tenancy deployment), Atlastix Device Intelligence (a platform customised for managed service providers), and product extensions, integrations and custom software solutions for customers. Device Intelligence can ingest data from customer-configured ITSM, endpoint management, identity, security, monitoring and ERP sources. The current Device Intelligence deployment runs in the MSP's cloud tenancy under the MSP's controls.
- Q2: Do you have a documented information security programme?** **A:** Yes. Management has adopted a documented Information Security Management System (ISMS) comprising governance, risk, technical, engineering/data, people/supplier and resilience policies, procedures and registers (ATX-GOV-01 to ATX-RES-05). The master policy is ATX-GOV-02. ISO/IEC 27001:2022 and the SOC 2 Security and Availability criteria are control references.
- Q3: Who is accountable for information security in your organisation?** **A:** The Chief Executive Officer holds ultimate accountability and approves ISMS policy. A designated Security Officer coordinates the ISMS and incident response; the Engineering Lead owns secure development, release and vulnerability controls (ATX-GOV-03). Security leadership is consolidated in these senior roles rather than a separate security function.
- Q4: How often are security policies reviewed and approved?** **A:** Policy requires review at least annually and upon significant change under document control (ATX-GOV-04). The current version and effective date of each public trust document are recorded in its document header and the published document register; this document is version 1.0, effective 10 August 2026, with next review in August 2027.

Q5: How do you manage segregation of duties in a small team? A: Management-approved controls use senior review of junior-authored code and infrastructure changes, separate approval where practicable, documented approval for privileged access, and management review. Where roles must be consolidated, the conflict and compensating review are recorded (ATX-GOV-03, ATX-GOV-08).

Q6: Do you perform management reviews of the security programme? A: The management-review process is defined and covers security objectives and metrics, risk status, incidents, supplier matters and corrective actions (ATX-GOV-09). The first formal management review is scheduled for February 2027, with an interim governance checkpoint in October 2026. Minutes and records will be retained as controlled internal records from the first cycle.

Q7: Do you carry cyber insurance? A: Yes. Atlastix Pty Ltd holds professional indemnity and cyber insurance appropriate to its size and services. Certificates of currency and policy limits are available to customers under NDA. Both policies are recorded as insurance risk transfer under ATX-GOV-12, ATX-RSK-01 and ATX-RSK-04.

2. Certifications and compliance

Q8: Do you hold ISO/IEC 27001 certification? A: No. Atlastix uses ISO/IEC 27001:2022 as a reference framework but has not completed a certification audit and does not hold a certificate. Certification is a target only, subject to readiness, provider appointment, scope and successful completion (ATX-SOC-05).

Q9: Do you have a SOC 2 report? A: No. Atlastix has not completed a SOC 2 examination and no Type 1 or Type 2 report has been issued. SOC 2 is a target only. Prospective scope concerns development, customisation, release, delivery and support across Atlastix products and custom solutions, corporate systems and customer data Atlastix receives through those activities; it does not cover customer- or MSP-operated tenancies (ATX-SOC-01, ATX-SOC-05).

Q10: What assurance can you provide in the interim? A: This completed questionnaire, the Security Whitepaper (ATX-SOC-03), Subprocessor & Hosting Register (ATX-SOC-07), Security Terms & Control Position (ATX-SOC-08), and a management-led documentation walkthrough under confidentiality. Available control records may be discussed subject to legal, security, contractual and customer restrictions. These options are not independent assurance.

Q11: Are you subject to privacy legislation? A: Atlastix applies the Australian Privacy Principles as internal policy and assesses potential eligible data breaches under the Notifiable Data Breaches scheme where applicable (ATX-PPL-06, ATX-RES-05). Other privacy requirements are assessed according to the data, parties and jurisdiction involved.

Q12: Do your cloud and platform providers hold certifications? A: The major providers publish their own certifications: AWS publishes ISO/IEC 27001, 27017 and 27018 certifications and a SOC 2 Type II report (via AWS Artifact); Microsoft publishes ISO/IEC 27001:2022 certification and SOC 2 Type II reports for Azure and Microsoft 365 (via the Microsoft Service Trust Portal); and GitHub provides ISO/IEC 27001:2022 certification and a SOC 2 Type II report through its authenticated organisation or enterprise Compliance area (owner access required), not a public trust portal. These are the suppliers' certifications, not Atlastix's, and cover the supplier service rather than Atlastix configuration or customer-operated tenancies. Applicability depends on the contracted service, plan, tenant and region (ATX-PPL-05, ATX-PPL-07).

Q13: Have you undergone an independent penetration test? A: No. Atlastix has not completed an independent penetration test and no report or executive summary is available. Independent testing is a target only; provider, scope, timing and outcome are not guaranteed (ATX-TEC-07, ATX-SOC-05).

3. Deployment model and shared responsibility

Q14: Describe your hosting and deployment model. A: Current delivery is generally into customer- or MSP-controlled cloud tenancies. Deployment-specific architecture, data flows, integrations, operational responsibilities and support paths are governed by the deployed configuration and applicable agreement. Atlastix's own cloud environments support development, build, testing, customisation, release, delivery, approved engagement-data, support and corporate activities. The current Device Intelligence deployment is a staging instance in the MSP's cloud tenancy, in user acceptance testing ahead of production; workloads and data in that instance remain under the MSP's controls.

Q15: How is security responsibility shared between us and Atlastix? A: For current customer-tenancy delivery, the customer or MSP generally owns infrastructure and network security, production identity and access, backups, capacity and availability in its tenancy. Atlastix owns security of the products, customisations and custom software it develops, its release and delivery processes, its own environment, approved copies it receives, and its personnel's conduct when temporary access is granted. Update application and other deployment duties follow the applicable configuration and agreement. ATX-SOC-03 section 2 tabulates this division.

Q16: Do you host or process our production data? A: Current delivery is generally in customer- or MSP-controlled tenancies. Atlastix may process customer-approved extracts or uploads for a defined engagement, or use temporary access within the customer tenancy; location and retention are deployment- and agreement-specific. For the current Device Intelligence deployment, Atlastix does not host the production workload, approved extracts and uploads are processed in Azure Australia East, temporary MSP-tenancy access may be used, and there is no separate ongoing Device Intelligence product or telemetry feed.

Q17: For MSP deployments of Device Intelligence, how are end-client data and integration credentials handled? A: Device Intelligence can touch end-client data, MSP operational data (tickets, configurations, billing and staff identities), and connector credentials for ITSM, endpoint, identity, security, monitoring and ERP systems, all in the MSP tenancy. Enabled scopes and write-backs are determined by the deployed connector configuration and should follow least privilege. Connector credentials, tokens and secrets generally remain in the MSP tenancy and are excluded from extracts and uploads. Where a credential is provided 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, with access limited to named engagement personnel and rotation or revocation on suspected compromise. Any Atlastix in-tenancy access is MSP-granted, temporary, named, scoped and logged. An approved raw extract may contain personal information and end-client data; the MSP remains responsible for authority to provide it.

Q18: Are your product deployments isolated from other customers? A: Current deployments are generally separated by the customer's or MSP's tenancy controls. For the current Device Intelligence instance, the software runs in the MSP tenancy; where the MSP serves multiple end clients, it configures and operates role- and tenant-based segregation. Approved copies held by Atlastix are access-restricted to named engagement personnel under Q23.

4. Customer data held by Atlastix

Q19: What customer data does Atlastix hold? A: Atlastix may hold: (1) customer-approved extracts or uploads for development, customisation, testing, delivery or support; (2) data accessed through temporary customer-tenancy access without transfer; (3) data from an agreed product integration or feed where one

is configured and contractually governed; and (4) business and support data such as contacts, contracts, engagement records and correspondence. For the current Device Intelligence deployment, approved extracts or uploads may contain raw personal, business and end-client data but exclude credentials, tokens and secrets, and there is no separate ongoing Device Intelligence product or telemetry feed.

Q20: Where is customer data held by Atlastix stored? A: The location of approved customer data follows the deployed configuration and approved service. Business and support records are stored in the approved corporate tools disclosed in ATX-SOC-07. For the current Device Intelligence deployment, approved extracts and support uploads are stored and processed in an access-restricted Atlastix Microsoft Azure environment in Australia East; raw Device Intelligence extracts and connector secrets are not approved for corporate tools.

Q21: Is data encrypted in transit? A: Yes. ATX-TEC-03 requires TLS 1.2 or higher for approved transfers and access to Atlastix-operated systems. Temporary in-tenancy access uses the MSP's approved access path.

Q22: Is data encrypted at rest? A: Yes for approved engagement data: customer engagement data held by Atlastix is encrypted at rest with AES-256 using keys held in managed cloud key-management services under ATX-TEC-03. Current Device Intelligence engagement data uses the approved Azure service configuration; corporate-tool encryption follows the contracted service configuration.

Q23: What controls govern approved engagement data? A: Contractual authority and confidentiality terms are established before transfer or access; the engagement, method and access are approved; processing uses the approved location; access is limited to named personnel working on the engagement and logged; and a record identifies owner, purpose, location, retention and deletion due date. Credentials, tokens and secrets are excluded unless an approved design and secure process expressly require them, and customer data supplied to Atlastix is not used to train AI models (ATX-ENG-05, ATX-ENG-06, ATX-ENG-07). For current Device Intelligence extracts and uploads, the approved location is Azure Australia East.

Q24: How and when are provided datasets deleted? A: Retention and deletion are defined per product and engagement and tracked under ATX-ENG-06. For current Device Intelligence point-in-time extracts and support uploads, 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. Written confirmation may be provided where required by the applicable agreement.

Q25: What does the product data feed from deployed software contain, and how is it protected? A: Any ongoing integration or feed requires a documented purpose, approved data scope, security and retention controls, customer terms and appropriate disclosure. The current Device Intelligence deployment has no separate ongoing product or telemetry feed to Atlastix; its approved paths are the point-in-time extract, support upload and temporary in-tenancy access described in Q16-Q24.

Q26: Is customer production data used in your development or test environments? A: Only when customer-approved data or temporary customer-tenancy access is necessary for a defined development, customisation, testing, delivery or support engagement, and then only under Q23 and Q24. General development and test activities must use synthetic or non-customer data where customer data is not specifically approved and necessary (ATX-ENG-01, ATX-ENG-05).

Q27: How is data classified and handled? A: Under ATX-ENG-05 Data Classification & Handling Policy. Approved raw customer extracts, including personal and end-client data, receive Restricted handling, with rules for storage, access, transmission, sharing and disposal. Credentials, tokens and secrets are excluded from transferred datasets.

Q28: Do you use customer data for any purpose other than the contracted engagement? A: No. Approved extracts, uploads and temporary tenancy access are used only for the authorised engagement purpose. Customer data is not sold and is not used to train AI models. Any additional purpose requires lawful authority, customer agreement and updated control assessment.

5. Access control and identity

Q29: Do you enforce multi-factor authentication? A: Policy requires MFA for Atlastix work systems where supported and for privileged or remote access, with named identities and approved authentication controls (ATX-TEC-02). Customer-tenancy authentication is configured and controlled by the MSP.

Q30: How is access granted and on what principle? A: Least privilege, role need, named identity and documented approval. Privileged grants require justification; access to an approved customer dataset is limited to named engagement personnel; and temporary customer-tenancy access is granted and revoked by the MSP (ATX-TEC-01, ATX-ENG-05).

Q31: How often is access reviewed? A: ATX-TEC-01 requires periodic review of Atlastix accounts, privileged access, service identities and approved engagement-data access, reconciled against current personnel and role need. The MSP reviews access in its tenancy.

Q32: How quickly is access revoked when someone leaves? A: Policy requires revocation promptly through the offboarding process, with urgent action for elevated risk and completion recorded (ATX-PPL-02, ATX-TEC-01). The MSP controls revocation of any identity in its tenancy.

Q33: Who can access customer datasets held by Atlastix, and is that access logged? A: Only named personnel assigned to the relevant engagement and approved for the data, using named accounts. Azure access and activity records support review under ATX-TEC-01 and ATX-TEC-04. Access is removed when no longer required.

Q34: Are shared accounts used? A: Policy prohibits shared human accounts unless a system technically requires an exception. An exception must have a named owner, controlled credential storage, restricted use and review. Shared customer-tenancy identities remain under the MSP's controls and should not be issued to Atlastix where named access is available.

Q35: Under what conditions do Atlastix personnel access our tenancy? A: Only with the MSP's or customer's grant for an approved engagement. Access is temporary, named, scoped to the task, logged in the tenancy and revoked by its operator. Atlastix personnel are bound by confidentiality and acceptable-use obligations (ATX-TEC-01, ATX-PPL-01).

6. Atlastix environment security

Q36: Describe the environment Atlastix operates itself. A: Atlastix uses cloud and SaaS services for development, build/CI, testing, customisation, release, delivery, support, approved engagement-data processing and corporate activities. Processing locations follow the approved product, deployment and agreement. Current Device Intelligence extracts and uploads are processed in Azure Australia East. Corporate and engineering services include Microsoft, AWS, GitHub, Microsoft 365, Slack, Atlassian, Vercel, EmailJS and Xero, with an in-house Entra SSO-protected and encrypted CRM (ATX-SOC-07). The marketing and trust websites run on Vercel, while DNS is externally managed. Atlastix operates no physical data centre and current customer delivery is generally in customer- or MSP-controlled cloud tenancies.

Q37: How is your network segmented and protected? **A:** ATX-TEC-05 requires network boundaries, restricted administrative paths, least-access rules and separation appropriate to data sensitivity. Approved customer data is held in an access-restricted Azure environment rather than corporate messaging or issue-tracking tools. Configuration records and changes are controlled under ATX-TEC-06 and ATX-ENG-02.

Q38: How are cloud environments hardened and monitored for misconfiguration? **A:** Management-approved controls require configuration baselines, change control, logging and review of security-relevant deviations (ATX-TEC-06, ATX-TEC-07). Service-specific implementation follows the applicable account and service configuration.

Q39: Do you perform vulnerability scanning? **A:** The vulnerability-management control requires risk-based scanning and review across applicable Atlastix systems, code and dependencies, including release-related checks (ATX-TEC-07, ATX-ENG-01). Findings are prioritised by severity, exploitability and exposure. Remediation and support timing for shipped software follows the applicable customer agreement. Atlastix currently performs automated dependency scanning via GitHub Dependabot on its release repositories; broader assessment tooling is planned, and its platforms operate within customer and MSP-controlled networks that apply their own security controls and testing.

Q40: How do you manage patching? **A:** Managed-service providers patch provider-managed components under their service terms. Atlastix-owned dependencies, endpoints and configurations are tracked and treated according to risk under ATX-TEC-07. The MSP owns patching of its tenancy and application of released Device Intelligence updates unless otherwise agreed.

Q41: How are endpoints secured? **A:** Company laptops are managed through Microsoft Intune and protected by Microsoft Defender EDR and anti-malware, with screen lock, updates, encryption, tamper protection and malicious-site web/network protection enforced. Entra Conditional Access limits personal-mobile access to approved email/calendar controls. Customer data may not be stored on unmanaged devices, and approved extracts are not copied to endpoints except where specifically authorised and necessary for the engagement (ATX-TEC-08, ATX-PPL-03).

7. Application security and release integrity

Q42: Do you follow a secure development lifecycle? **A:** Yes. The management-approved SDLC requires security consideration during design, pull-request change control with senior review of junior-authored changes, applicable automated security checks and disciplined testing before controlled release for product code, customisations and infrastructure-as-code (ATX-ENG-01, ATX-ENG-02).

Q43: Is code peer-reviewed before release? **A:** Release code changes are required to use pull requests; force-pushes are disabled on release repositories, and fuller branch-protection enforcement is a planned control. Changes authored by junior or less-experienced engineers require senior review before merge; senior engineers may merge their own work under the team's testing discipline. Exceptions are handled through authorised emergency-change procedures (ATX-ENG-01, ATX-ENG-02). Review and change records are retained internally.

Q44: Do you scan code and dependencies for vulnerabilities? **A:** Automated dependency scanning runs via GitHub Dependabot on release repositories; further check types (static analysis, secrets detection) are planned and adopted per repository as configured, with coverage being extended. Findings are handled through vulnerability management (ATX-ENG-01, ATX-TEC-07).

Q45: How are changes controlled? **A:** ATX-ENG-02 requires a defined purpose, risk consideration, testing, approval, versioned delivery and rollback or recovery planning appropriate to the change. Emergency

changes require authorised approval and retrospective review. MSP deployment changes also require MSP approval.

Q46: How can we verify the integrity of the software you ship? A: 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. No universal cryptographic verification mechanism is applied. Release notes identify the version and deployment instructions (ATX-ENG-01, ATX-ENG-02).

Q47: Do you provide deployment, upgrade and rollback guidance? A: Deployment and hardening guidance describes secure configuration assumptions. Upgrade and rollback or recovery steps are documented proportionate to the release or customisation, and advisories identify recommended action (ATX-ENG-01, ATX-ENG-02, ATX-SOC-06).

Q48: How are per-deployment customisations and custom solutions controlled? A: Customisations follow the same management-approved design, change-control, testing and controlled-delivery process as product code, with change and rollback records appropriate to the deployment (ATX-ENG-01, ATX-ENG-02).

Q49: How are secrets and credentials managed in your development and build environment? A: Policy requires approved credential-management mechanisms and prohibits secrets in source code, tickets and chat (ATX-TEC-03, ATX-ENG-01). For Device Intelligence, connector credentials, tokens and secrets generally remain in the MSP tenancy and are excluded from extracts and uploads; where a credential is provided to Atlastix for customisation or support, it is handled under ATX-TEC-02, stored only in 1Password Business or the ATX-TEC-03 secrets services and never in code, tickets or chat.

Q50: Do you operate a responsible disclosure channel? A: Yes. ATX-SOC-06 provides reporting instructions and safe harbour for qualifying good-faith research against systems Atlastix operates, and accepts reports about shipped software. Reports go to support@atlastix.io. Atlastix does not operate a paid bug bounty programme or publish a universal acknowledgement service level.

Q51: What is your SLA for fixing vulnerabilities in software deployed in our tenancy? A: Fix, mitigation, advisory, support and notification timing follows the applicable customer agreement and considers severity, exploitability, exposure and affected versions (ATX-TEC-07, ATX-SOC-06). Atlastix does not publish a universal remediation commitment. Applying released fixes in the MSP tenancy is the operator's responsibility unless otherwise agreed.

8. AI-specific controls

Q52: Do your products make automated decisions using AI, and can they be overseen? A: AI-assisted workflows may be configured with human-review checkpoints and approval thresholds appropriate to the use case (ATX-ENG-07). Current customer workflow content uses the customer's provider account and keys or a customer cloud-native service. Atlastix operates no managed model-provider account receiving customer workflow content, and such use is prohibited until separately approved. The customer controls deployment configuration and its provider account.

Q53: Are AI-assisted decisions auditable? A: Audit recording of AI-assisted actions - relevant inputs, outputs and acting identity - is available and is configured per deployment. Whether recording is enabled, and how production audit records are retained, follows the deployed configuration, which the customer or MSP operates (ATX-ENG-07).

Q54: Is customer data used to train AI models? A: Atlastix does not use customer data supplied for an engagement to train AI models (ATX-ENG-07). Provider treatment of data sent through the customer's

account is governed by the customer's provider terms and configuration.

Q55: How do you address AI-specific risks such as prompt injection or data leakage through models?

A: AI-specific risks are assessed under ATX-RSK-01 and ATX-RSK-02 and addressed through approved-purpose limits, design controls, input and context handling, human review where appropriate, testing and deployment configuration (ATX-ENG-07, ATX-ENG-01). Credentials, tokens and secrets must not be placed in prompts.

Q56: Which AI model providers do you use, and are they your subprocessors? **A:** Current product and custom-solution customer-content AI uses the customer's own provider account and keys or a cloud-native model service in the customer's tenancy; those providers are generally the customer's suppliers. Atlastix operates no model-provider account receiving customer workflow content. An Atlastix-managed provider is prohibited until separately approved through supplier, subprocessor, privacy, risk and customer review before any content flows (ATX-SOC-07, ATX-ENG-07).

9. Personnel security

Q57: Are personnel screened before hire? **A:** ATX-PPL-02 requires screening proportionate to role, legal limits and access risk before relevant access is granted. The process applies to employees and contractors as appropriate.

Q58: Are staff bound by confidentiality obligations? **A:** Yes. Personnel are subject to confidentiality terms and acceptable-use obligations appropriate to their employment or contractor relationship (ATX-PPL-01, ATX-PPL-02).

Q59: Do staff receive security awareness training? **A:** ATX-GOV-06 requires security awareness at onboarding, periodically thereafter and following material changes or identified needs. Completion and follow-up are management records.

Q60: Do contractors follow the same security policies as employees? **A:** ISMS requirements defined for All Personnel apply to employees and contractors within scope. Access and obligations remain proportionate to role and engagement.

Q61: How is remote and home working secured? **A:** ATX-PPL-03 and ATX-PPL-04 require approved devices, protected authentication, screen locking, secure handling and safeguards appropriate to the working location. Customer data may not be stored on personal or unmanaged devices.

10. Incident response and resilience

Q62: Do you have a documented incident response plan? **A:** Yes. ATX-RES-01 defines severity assessment, roles, escalation, evidence preservation, communications, response coordination, post-incident review and corrective actions. Response timing is governed by applicable agreements and incident circumstances.

Q63: Will you notify us if an incident affects our data or software? **A:** Customer notification follows the applicable customer agreement, legal obligations and known incident circumstances. For the current Device Intelligence deployment, incidents are coordinated with the MSP, which owns onward end-client notification unless otherwise agreed. Atlastix does not publish a universal customer-notification period (ATX-RES-01, ATX-RES-05).

Q64: How do you handle notifiable data breaches? **A:** Suspected eligible data breaches involving personal information are assessed under the Notifiable Data Breaches scheme where it applies. Atlastix

coordinates with affected customers or MSPs and provides information required under applicable legal and contractual terms (ATX-RES-05).

Q65: What is your backup regime? A: For current in-tenancy delivery, the customer or MSP generally owns production backup, restore and availability; exact responsibilities follow the deployed architecture and agreement. Atlastix-held data follows the retention controls in ATX-ENG-06 and the backup requirements in ATX-RES-03; current protection for Atlastix systems is provider-managed durability plus zone-redundant (ZRS) and geo-redundant (GRS) object-storage replication, with implementation of separate backup copies tracked as treatment work under risk R-017. For current Device Intelligence extracts and support uploads, 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.

Q66: Are business continuity and disaster recovery plans tested? A: ATX-RES-02 requires an annual business continuity and disaster recovery exercise covering Atlastix development, build and support activities. The first end-to-end exercise has not yet been completed; results will be recorded and reported at management review once conducted. The MSP owns continuity and disaster recovery for Device Intelligence production in its tenancy.

Q67: How is your environment monitored for security events? A: Cloud, source-control, identity and corporate audit sources are governed by logging and monitoring controls; coverage and retention currently follow the applicable service configuration (provider defaults), and centralised retention, alerting and triage form the policy's defined target architecture, with escalation into incident response (ATX-TEC-04, ATX-RES-01). Atlastix does not operate a staffed 24x7 security operations centre.

11. Supplier management

Q68: Do you assess the security of your suppliers? A: Atlastix maintains a supplier-risk process and controlled supplier register. The process risk-tiers suppliers according to service, data access and criticality and requires due diligence, contractual review and periodic review proportionate to tier (ATX-PPL-05, ATX-PPL-07).

Q69: Do you maintain a supplier register? A: Yes. ATX-PPL-07 records supplier service, data access, risk and review information internally. ATX-SOC-07 is the public processor, AI-provider and hosting view across Atlastix activities and includes a current Device Intelligence customer annex.

Q70: Which subservice organisations and subprocessors underpin your services? A: Microsoft Entra ID, AWS, GitHub, Microsoft 365, Slack, Atlassian, Vercel, EmailJS and Xero support identity, development, build, website, enquiry, delivery, support or corporate functions as detailed in ATX-SOC-07. Product- and deployment-specific hosting and processing suppliers depend on configuration and agreement. Customer AI providers or cloud-native services remain under the customer's arrangement; Atlastix has no AI model-provider account receiving customer workflow content. For current Device Intelligence extracts and uploads, Microsoft Azure Australia East is the approved processor; the MSP's cloud provider and customer's AI provider are their suppliers, not Atlastix-managed subprocessors.

Q71: Will you notify us of material changes to your subprocessors or subservice organisations? A: Notice and objection rights, if any, follow the applicable data-processing or customer agreement. ATX-SOC-07 is updated before a newly approved Atlastix-managed subprocessor begins production processing.

12. Support, availability and contractual commitments

Q72: What availability do you commit to? **A:** Availability responsibilities and commitments follow the product or custom solution architecture and applicable agreement. For current in-tenancy delivery, the customer or MSP generally operates availability, capacity, backup and recovery. For the current Device Intelligence deployment, the MSP performs those functions and Atlastix does not publish an uptime figure.

Q73: What are your support hours, and how are service-affecting matters communicated? **A:** Support coverage, response targets, escalation and service-affecting communications follow the applicable customer agreement. support@atlastix.io is the monitored public contact and creates Jira Service Management tickets. Release and advisory notifications use release notes, nominated customer email contacts and Jira Service Management where applicable. Atlastix does not publish a universal support or response service level.

Q74: Do you offer a data processing agreement (DPA)? **A:** Data-processing terms are addressed in customer contracting where required and may cover confidentiality, security, incidents, subprocessors, location, retention and deletion (ATX-PPL-05, ATX-PPL-06).

Q75: What security commitments will you make contractually? **A:** Applicable agreements may address shipped-software security, customisation change control, approved engagement-data handling and deletion, temporary support access, incident coordination, vulnerability handling, AI-provider responsibility and supplier transparency. ATX-SOC-08 lists the public commitments; the executed customer agreement controls binding commitments and timing.

Q76: Do we have a right to audit or review your security? **A:** Review and audit rights are determined by the applicable agreement. A management-led questionnaire response and control walkthrough may be arranged under confidentiality, subject to legal, security, contractual and customer restrictions. Raw internal records, on-site audits and future external reports are not promised unless the applicable agreement provides for them.

Q77: How can we verify your answers? **A:** Contact support@atlastix.io to request a management-led walkthrough or due diligence response. ATX-SOC-03 through ATX-SOC-08 are public. Atlastix will update its public assurance status if an independent penetration test, SOC 2 report or ISO/IEC 27001 certification is completed; none is currently available.

Revision history

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