

# Data Privacy and Retention

## Document Metadata

**Company:** Atlas Systems Group

**Headquarters:** Gilbert, AZ

**Document ID:** ASG-POL-DAT-2076

**Policy Owner (Department):** Privacy

**Policy Owner (Role):** Data Protection Officer

**Revision:** 1.0

**Effective Date:** December 20, 2025

**Next Review Date:** December 20, 2026

**Approved By:** Executive Leadership Team (ELT)

**Applies To:** All employees, contractors, and temporary workers unless stated otherwise

**Policy Precedence:** Corporate Governance Policy governs conflicts; stricter control applies unless an exception is approved

Note for AI ingestion: Sections are numbered consistently; key terms are repeated with controlled variation to support semantic retrieval with sentence-transformer embeddings. Exceptions and conflicts are explicit to enable benchmarking of conflict resolution behaviors.

# Data Privacy and Retention — Section 1.0

## 1.1 Topic: Privacy principles and lawful processing

**Purpose.** This section defines expectations for privacy principles and lawful processing within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 1.2 Responsibilities

- **Employees:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 1.3 Controls and Procedures

Control level is **Low**. Required actions must be completed within 5 business days. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 1.4 Conflicts, Exceptions, and Edge Cases

**Policy Interaction: HR Retention:** Routine HR support tickets are retained for 3 years unless required longer.

**Exception: Legal Holds:** Legal holds and statutory requirements override deletion schedules.

- If a customer contract requires stronger controls than this policy, the contract requirement applies and must be recorded as a contractual obligation.

- If local law conflicts with this policy, Legal & Compliance determines the compliant path and records the decision.

## 1.5 Example Scenario

Scenario 1: A manager requests an action related to *privacy principles and lawful processing*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 2.0

## 2.1 Topic: PII handling, minimization, and access

**Purpose.** This section defines expectations for pii handling, minimization, and access within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 2.2 Responsibilities

- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Finance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 2.3 Controls and Procedures

Control level is **Medium**. Required actions must be completed within 2 business days. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 2.4 Conflicts, Exceptions, and Edge Cases

- If local law conflicts with this policy, Legal & Compliance determines the compliant path and records the decision.
- If an employee requires an accommodation, People Ops coordinates an interactive process; documentation is limited to what is necessary.

## 2.5 Example Scenario

Scenario 2: A manager requests an action related to *pii handling, minimization, and access*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 3.0

## 3.1 Topic: Consent, notices, and data subject requests

**Purpose.** This section defines expectations for consent, notices, and data subject requests within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 3.2 Responsibilities

- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Finance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Legal & Compliance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 3.3 Controls and Procedures

Control level is **High**. Required actions must be completed within 24 hours. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 3.4 Conflicts, Exceptions, and Edge Cases

**Policy Interaction: HR Retention:** Routine HR support tickets are retained for 3 years unless required longer.

**Exception: Legal Holds:** Legal holds and statutory requirements override deletion schedules.

- If an employee requires an accommodation, People Ops coordinates an interactive process; documentation is limited to what is necessary.

- If systems are unavailable, follow the manual fallback procedure and document actions retroactively within 1 business day.

### 3.5 Example Scenario

Scenario 3: A manager requests an action related to *consent, notices, and data subject requests*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 4.0

## 4.1 Topic: Retention schedules (core categories)

**Purpose.** This section defines expectations for retention schedules (core categories) within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 4.2 Responsibilities

- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Finance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Legal & Compliance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Managers:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 4.3 Controls and Procedures

Retention schedules exist to minimize risk and comply with statutory requirements. Data must not be retained indefinitely 'just in case.'

Routine HR support tickets are retained for 3 years. Personnel records are handled under Records Management schedules and may be longer.

Legal holds override standard deletion; when a hold is issued, deletion and auto-purge must be suspended for in-scope systems.

## 4.4 Conflicts, Exceptions, and Edge Cases

- If systems are unavailable, follow the manual fallback procedure and document actions retroactively within 1 business day.
- If a customer contract requires stronger controls than this policy, the contract requirement applies and must be recorded as a contractual obligation.

## 4.5 Example Scenario



Scenario 4: A manager requests an action related to *retention schedules (core categories)*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 5.0

## 5.1 Topic: Deletion and secure disposal procedures

**Purpose.** This section defines expectations for deletion and secure disposal procedures within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 5.2 Responsibilities

- **Finance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Legal & Compliance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Managers:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Employees:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 5.3 Controls and Procedures

Control level is **Low**. Required actions must be completed within 5 business days. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 5.4 Conflicts, Exceptions, and Edge Cases

**Policy Interaction: HR Retention:** Routine HR support tickets are retained for 3 years unless required longer.

**Exception: Legal Holds:** Legal holds and statutory requirements override deletion schedules.

- If a customer contract requires stronger controls than this policy, the contract requirement applies and must be recorded as a contractual obligation.

- If local law conflicts with this policy, Legal & Compliance determines the compliant path and records the decision.

## 5.5 Example Scenario

Scenario 5: A manager requests an action related to *deletion and secure disposal procedures*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 6.0

## 6.1 Topic: Legal holds and litigation readiness

**Purpose.** This section defines expectations for legal holds and litigation readiness within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 6.2 Responsibilities

- **Legal & Compliance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Managers:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Employees:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 6.3 Controls and Procedures

Control level is **Medium**. Required actions must be completed within 2 business days. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 6.4 Conflicts, Exceptions, and Edge Cases

- If local law conflicts with this policy, Legal & Compliance determines the compliant path and records the decision.
- If an employee requires an accommodation, People Ops coordinates an interactive process; documentation is limited to what is necessary.

## 6.5 Example Scenario

Scenario 6: A manager requests an action related to *legal holds and litigation readiness*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 7.0

## 7.1 Topic: Third-party sharing and DPAs

**Purpose.** This section defines expectations for third-party sharing and dpas within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 7.2 Responsibilities

- **Managers:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Employees:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 7.3 Controls and Procedures

Control level is **High**. Required actions must be completed within 24 hours. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 7.4 Conflicts, Exceptions, and Edge Cases

- If an employee requires an accommodation, People Ops coordinates an interactive process; documentation is limited to what is necessary.
- If systems are unavailable, follow the manual fallback procedure and document actions retroactively within 1 business day.

## 7.5 Example Scenario

Scenario 7: A manager requests an action related to *third-party sharing and dpas*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 8.0

## 8.1 Topic: Cross-border transfers and remote access

**Purpose.** This section defines expectations for cross-border transfers and remote access within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 8.2 Responsibilities

- **Employees:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 8.3 Controls and Procedures

Control level is **Critical**. Required actions must be completed immediately ( $\leq 1$  hour). Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 8.4 Conflicts, Exceptions, and Edge Cases

- If systems are unavailable, follow the manual fallback procedure and document actions retroactively within 1 business day.
- If a customer contract requires stronger controls than this policy, the contract requirement applies and must be recorded as a contractual obligation.

## 8.5 Example Scenario



Scenario 8: A manager requests an action related to *cross-border transfers and remote access*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.

# Data Privacy and Retention — Section 9.0

## 9.1 Topic: Exceptions, audits, and accountability

**Purpose.** This section defines expectations for exceptions, audits, and accountability within Atlas Systems Group. It aims to reduce operational risk, improve consistency, and clarify approvals, responsibilities, and timelines.

**Scope.** Unless a narrower scope is stated, this section applies to employees and contractors using company systems, data, facilities, or representing the company in any capacity.

## 9.2 Responsibilities

- **People Ops:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **IT:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Security:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.
- **Finance:** Must follow documented procedures, report issues within required timelines, and retain evidence when needed.

## 9.3 Controls and Procedures

Control level is **Low**. Required actions must be completed within 5 business days. Evidence should be stored in the approved repository for auditability.

Approvals must be obtained before the action is taken when spend, access, or people-impact thresholds are met. Use the standard request form and include business justification, risks, and alternatives considered.

Exceptions are allowed only when documented and time-bounded. Compensating controls must reduce residual risk to an acceptable level.

## 9.4 Conflicts, Exceptions, and Edge Cases

- If a customer contract requires stronger controls than this policy, the contract requirement applies and must be recorded as a contractual obligation.
- If local law conflicts with this policy, Legal & Compliance determines the compliant path and records the decision.

## 9.5 Example Scenario

Scenario 9: A manager requests an action related to *exceptions, audits, and accountability*. The requester provides incomplete justification. The approver rejects the request, asks for risk analysis, and records the decision. If the request is urgent, a time-bounded exception is created with compensating controls and a review date.