

# Acceptable Use Policy

## Document Metadata

**Company:** Atlas Systems Group

**Headquarters:** Gilbert, AZ

**Document ID:** ASG-POL-ACC-9932

**Policy Owner (Department):** IT

**Policy Owner (Role):** IT Operations Manager

**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.

# Acceptable Use Policy — Section 1.0

## 1.1 Topic: Permitted business use of systems

**Purpose.** This section defines expectations for permitted business use of systems 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: Password Length:** Passwords must be at least 12 characters (legacy systems) and never reused across accounts.

- 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 *permitted business use of systems*. 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.

# Acceptable Use Policy — Section 2.0

## 2.1 Topic: Personal use boundaries and prohibited conduct

**Purpose.** This section defines expectations for personal use boundaries and prohibited conduct 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 *personal use boundaries and prohibited conduct*. 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.

# Acceptable Use Policy — Section 3.0

## 3.1 Topic: Email, messaging, and collaboration standards

**Purpose.** This section defines expectations for email, messaging, and collaboration standards 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: Password Length:** Passwords must be at least 12 characters (legacy systems) and never reused across accounts.

- 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 *email, messaging, and collaboration standards*. 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.

# Acceptable Use Policy — Section 4.0

## 4.1 Topic: Software installation and licensing

**Purpose.** This section defines expectations for software installation and licensing 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

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.

## 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 *software installation and licensing*. 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.

# Acceptable Use Policy — Section 5.0

## 5.1 Topic: Monitoring notice and privacy expectations

**Purpose.** This section defines expectations for monitoring notice and privacy expectations 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: Password Length:** Passwords must be at least 12 characters (legacy systems) and never reused across accounts.

- 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 *monitoring notice and privacy expectations*. 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.

# Acceptable Use Policy — Section 6.0

## 6.1 Topic: Password basics and account hygiene (legacy)

**Purpose.** This section defines expectations for password basics and account hygiene (legacy) 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

Users must maintain strong passwords (minimum 12 characters for legacy compatibility) and must not reuse passwords across accounts.

Credential sharing is prohibited. Accounts are assigned to individuals and are auditable.

If another policy sets a stricter password requirement, the stricter requirement applies; see Corporate Governance Policy for precedence guidance.

## 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 *password basics and account hygiene (legacy)*. 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.

# Acceptable Use Policy — Section 7.0

## 7.1 Topic: Data handling in everyday work

**Purpose.** This section defines expectations for data handling in everyday work 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 *data handling in everyday work*. 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.

# Acceptable Use Policy — Section 8.0

## 8.1 Topic: Mobile device and BYOD rules

**Purpose.** This section defines expectations for mobile device and byod rules 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 *mobile device and byod rules*. 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.

# Acceptable Use Policy — Section 9.0

## 9.1 Topic: Examples, violations, and enforcement

**Purpose.** This section defines expectations for examples, violations, and enforcement 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 *examples, violations, and enforcement*. 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.