

Code of Ethics and Security Policies

AUSOURCE INDUSTRIES LLC · EIN 86-3945528

AUS POL 01 | Version 1.2 | Prepared May 11, 2026

Effective from the approval date stated at the end of this document.

This document sets out the conduct rules and controls for Ausource commercial and logistics operations. It applies to managers, personnel and contractors according to their duties. Relevant requirements must be communicated to the suppliers and service providers involved in each transaction.

1 Responsibilities and decisions

Management approves this document, assigns a responsible officer and an alternate, and provides the necessary access and resources. The officer retains records, coordinates reviews and handles incidents. The alternate assumes these duties during the officer's absence, within the authority granted. Appointments must be documented in company records.

2 Integrity and business conduct

Bribery, facilitation payments, fraud, document falsification and the use of operations for money laundering, smuggling, terrorist financing or other unlawful activities are prohibited. Records must reflect actual transactions and preserve traceability.

No gifts, commissions or benefits intended to influence decisions may be offered or accepted. Conflicts of interest must be disclosed before participating in a decision; another manager without a conflict must review and approve it. If both managers have a conflict, the decision must be suspended until a documented independent review has been completed.

Statements about origin, metal content or certification must be supported by the documents for each transaction. No one may promise deliveries, certifications or conditions that have not been verified.

3 Good faith reporting

Irregularities must be reported to the responsible officer or alternate through an approved company channel. If the report concerns the officer, it must be directed to the other manager. Information must be kept confidential on a need-to-know basis, and retaliation for good faith reports is prohibited. Facts, supporting evidence, decisions and follow-up actions must be retained.

4 Counterparty due diligence and review

Before approving a business relationship, record the person's identity or company name, tax identification, business registration where applicable, activity, contact details, role in the transaction and payment information. Request ownership or beneficial ownership information when warranted by risk. Confirm that the activity, product, origin and destination are consistent.

Consult relevant national and international sources and restricted-party lists applicable to the counterparty and transaction. Record the exact sources, date, identity checked, results and reviewer. A name match requires verification of additional identifiers and is not conclusive on its own.

If documents are inconsistent, origin is unexplained, instructions are unusual or matches remain unresolved, suspend approval and the affected payment or shipment. The officer obtains clarification, and management documents whether to proceed, impose controls or reject the transaction. Third-party payments and bank account changes require independent verification through a previously known contact.

Review critical suppliers every two years and earlier if material changes or alerts arise. Upon approving this policy, management must set risk-based review frequencies for personnel, contractors and other counterparties. Each record must include the next review date.

5 Personnel and subcontracting

Verify identity, experience and suitability for assigned duties. Perform relevant background checks at onboarding, when duties change and at the approved intervals, subject to applicable privacy and authorization requirements. Retain the results and decision with restricted access.

Record authorized access rights. When a relationship ends, revoke access, recover assets and information, and document completion. Promptly inform the client of changes to assigned personnel and their replacements where applicable.

Obtain prior client authorization for subcontracting when required. Communicate applicable controls to the third party, review its capabilities and supporting documents, and retain evidence of acceptance. Engaging a service provider does not remove Ausource coordination and oversight responsibilities.

6 Traceability and cargo security

Maintain a file for each transaction linking the order, supplier, product, quantity, batch where applicable, invoice, origin or certification documents, transportation and delivery. Verify identity and quantity at each custody transfer using the operator's records. Record discrepancies before proceeding.

Use carriers suitable for the goods. Before dispatch, confirm product acceptance, security arrangements, insurance, packaging and documentation. For dangerous goods, use personnel and operators trained and authorized for the activity; do not change products, routes or packaging without verifying acceptance. Ausource has a contracted emergency response hotline to support incidents involving dangerous goods. Keep its contact details verified in a separate operational directory, confirm service coverage for the products and routes, and provide the contact information to operators where appropriate.

7 Information and records protection

Assign individual access rights according to duties; do not share passwords. Enable multifactor authentication where available, keep equipment updated and verify recipients before sending sensitive information. Restrict access to physical and digital files and use approved company channels.

Keep documents in an approved company repository. Define and record the backup frequency, responsible person and location. Maintain a recoverable copy protected against the same incident that could affect the original. Synchronization alone does not demonstrate recovery capability. Conduct an initial recovery test and repeat it at approved intervals and after material changes.

Management must approve a retention schedule by document type, taking applicable contractual and legal obligations into account. Do not delete information related to open audits, claims or investigations. At the end of the retention period, authorize and record secure disposal.

8 Incidents and stakeholder coordination

In an incident, protect people, contain the impact within available capabilities, preserve evidence and immediately notify the responsible officer or alternate. Record the facts, transaction, date, participants, actions and communications. Do not alter or delete supporting evidence.

Where appropriate, the officer promptly informs the client's authorized contact of irregularities or unlawful, unusual or suspicious activities linked to the transaction. Distinguish confirmed facts from suspicions and retain communications. Coordinate reports to the competent authorities and activation of the contingency plan.

9 Monitoring and improvement

Cooperate with previously coordinated audits and organize supporting records to respond to requests from clients, authorities and other authorized parties within applicable contractual or legal deadlines. Record each recommendation, assigned owner, deadline and evidence of closure.

Review this document at least annually and after material incidents or changes. Communicate updates to the relevant parties and retain acknowledgments. Management must assess noncompliance and determine measures according to its severity, the contractual relationship and applicable rules.

10 Implementation evidence

Retain approvals and communication records, counterparty checks, access and offboarding records, transaction files, backup tests, incident records and corrective actions. Issuing this document does not replace these records.

Approval

Luis Romero

Luis Helder Romero Bonilla

Manager

Ausource Industries LLC

Approval date: 05-11-2026