

Title	Supply Chain Management Policy
Document Reference	AEL-POL-013
Version	v010726
Effective Date:	January 2026
Next Review:	January 2027
Owner	Procurement Manager
Approved By	Managing Director

1. Purpose

This policy defines how Acorn selects, evaluates, manages, and develops suppliers and subcontractors to ensure product/service quality, legal and ethical compliance, protection of people and the environment, information security, and continuity of supply. It is part of our Integrated Management System (IMS).

2. Scope

Applies to all external providers (suppliers, subcontractors, logistics partners, and service providers) that affect Acorn products, services, or compliance obligations across all sites and business units.

3. Policy Commitments

Acorn will:

- Assure quality of purchased products/services through risk-based qualification, controls, and performance monitoring (ISO 9001).
- Protect the environment and prevent pollution by ensuring suppliers manage significant environmental aspects, waste, and resource use (ISO 14001).
- Protect health & safety by engaging suppliers who control risks, consult workers, and continually improve safety performance (ISO 45001).
- Safeguard information and personal data via proportionate security controls, GDPR compliance, and contractual protection (ISO 27001/GDPR).
- Uphold ethics and human rights: zero tolerance for bribery, corruption, forced or child labour; respect for fair working conditions and modern slavery legislation.
- Ensure resilience through business continuity and disaster recovery arrangements for critical goods and services.
- Continuously improve supply chain performance through audits, corrective actions, and supplier development.

4. Roles & Responsibilities

- Top Management: Approves policy; ensures resources; reviews supplier performance and risks.
- QHSE Manager (Policy Owner): Maintains this policy; defines standards and controls; oversees audits and performance reviews.

- Procurement: Executes sourcing process; embeds requirements in contracts/POs; maintains the Approved Supplier List (ASL).
- Information Security/Data Protection: Defines data security and privacy requirements; reviews DPAs; manages security incidents affecting suppliers.
- Budget Holders/Technical Owners: Define technical specs and criticality; participate in supplier evaluation and development actions.
- All Employees: Use only approved suppliers and follow this policy.

5. Supplier Life-Cycle Controls

5.1 Qualification & Onboarding

- Risk classification (criticality, complexity, regulatory/data exposure, HSE risk, sole source).
- Due diligence proportional to risk, e.g.:
 - Valid certification (ISO 9001/14001/45001/27001) where relevant, or equivalent evidence.
 - Legal and ethical checks: sanctions/export-control screening; anti-bribery; modern slavery/human rights; conflict minerals (where applicable).
 - HSE controls: risk assessments, training matrix, incident management, emergency preparedness.
 - Environmental controls: aspects & impacts, waste/licences, spill control, resource monitoring.
 - Information security & privacy: access control, encryption/backup posture, DPIAs/ROPA/retention (if processing personal data).
 - Continuity: BCP/DR for critical processes; single-source risk and alternates.
- Contractual requirements included via POs/Frameworks:
 - Conformance to specifications, standards, and flow-down of requirements to sub-suppliers.
 - Right of audit/access, non-conformance handling, CAPA, confidentiality/NDA, DPA (if applicable), and termination for non-compliance.

5.2 Performance Monitoring

- Maintain an Approved Supplier List (ASL) with status (Approved/Conditional/Suspended).
- Monitor KPIs (as applicable): OTIF, defect/PPM, complaints, non-conformities, incident rates, environmental incidents, data/security incidents, responsiveness to CAPA.
- Review frequency: risk-based (e.g., monthly for critical suppliers, quarterly/annually for others).
- Scorecards and audits: Apply remote/on-site audits to high-risk suppliers; track findings to closure.

5.3 Non-Conformance & Corrective Action

- Immediate containment for defects or service failures; protect customers and operations.
- Root-cause analysis (5-Whys/8D) and CAPA with due dates and verification of effectiveness.
- Escalation to Conditional or Suspended status if repeated failures or high risk.

5.4 Change & Configuration Control

- Suppliers must notify material changes (process, facility, key sub-suppliers, materials, certifications) before implementation.
- Re-qualification may be required for critical changes.

5.5 Documented Information

- Keep records of qualification, audits, scorecards, NCRs/CAPA, certificates, licences, DPAs, BCP tests in the IMS/DMS with revision and access control.
- Retention: Minimum [X years] or as required by law/contract.

6. Ethical, Legal & Human Rights Standards

- Zero tolerance for bribery/corruption; maintain gifts & hospitality registers where relevant.
- Suppliers must prohibit forced/child labour and ensure working hours, wages, and conditions meet legal standards; provide channels for grievances.
- Sanctions/export controls: comply with applicable laws and screen counterparties where required.
- Conflict minerals (if in scope): reasonable country-of-origin due diligence and declarations.

7. Environmental & H&S Expectations

- Environmental: Identify significant aspects; manage waste/hazardous materials; prevent pollution; comply with permits/licensing; pursue resource efficiency and carbon reduction consistent with [Company] objectives.
- Health & Safety: Maintain risk assessments (incl. COSHH where applicable), training/competence, incident reporting and learning, emergency preparedness (drills).

8. Information Security & Data Protection

- Apply proportionate controls to protect [Company] data and systems (access control, MFA for admin/remote access, patching, encryption, tested backups).
- For personal data: establish a Data Processing Agreement (DPA), lawful basis, ROPA, DPIA (for high risk), retention and secure destruction; notify data breaches without undue delay.

9. Business Continuity & Resilience

- Critical suppliers shall maintain and test Business Continuity/Disaster Recovery plans aligned to their risks (e.g., single-source, geopolitical, cyber, utilities, logistics).
- Suppliers must promptly notify disruptions with impact assessments and recovery timelines; [Company] may source alternates where necessary.

10. Communication & Training

- This policy is publicly available to suppliers and employees.
- Procurement, QHSE, and Technical teams receive periodic training on requirements, risk assessment, and supplier evaluation.

11. Performance Review & Improvement

- Management reviews supplier performance, risks, incidents, audit outcomes, and objectives/KPIs at least annually.
- Policy effectiveness is measured by trends (OTIF, defects/PPM, NCR closure times, incidents, audit findings) and is improved accordingly.

12. Non-Compliance

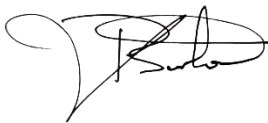
- Failure to comply can result in conditional approval, suspension, or termination. Severe breaches (safety, environment, ethics, data) trigger immediate escalation.

13. References

- ISO 9001 – Quality management; ISO 14001 – Environmental management; ISO 45001 – Occupational health & safety; ISO/IEC 27001 – Information security management.
- Applicable laws & regulations: data protection (e.g., GDPR), HSE legislation, environmental permits, sanctions/export controls, modern slavery/human rights laws relevant to the supplier's jurisdiction.

Policy Review

This policy will be reviewed regularly to ensure alignment with evolving sustainability standards, legislation, and organisational goals.



Jim Burton
Managing Director