

Accel Comply Sample: Policy Excerpt

Redacted illustrative sample. Not a full pack.

Document: Information Security Policy (Excerpt, Redacted Sample)

Purpose: Define how the organisation protects information assets and demonstrates consistent controls to auditors and customer security reviewers.

Scope: Applies to all employees, contractors, and relevant third parties with access to company information and systems.

Policy statements (examples):

1. Ownership and accountability: The ISMS Owner is responsible for maintaining this policy, ensuring annual review, and coordinating updates after material changes.
2. Access control: Access to systems and data is granted on a least-privilege basis, approved by an authorised owner, and reviewed at least quarterly. (Redacted: specific tool configuration details.)
3. Logging and monitoring: Security-relevant events are logged and retained according to the log retention standard. Alerts are reviewed and escalated based on severity and impact.
4. Supplier security: Third parties with access to data must be assessed for security risk, contracted with appropriate clauses, and periodically reviewed.

Evidence cues (what an auditor will ask for): access review records, joiner/mover/leaver workflow evidence, log retention settings, supplier assessment records.

Document control: Versioning, owner field, approval date, next review date, and change log are maintained in the document header.