

Vendor Management Policy

Vendor Onboarding

New vendors complete registration form with business information, tax ID, banking details, and insurance certificates.

Procurement conducts due diligence: Credit check, reference checks, background check for high-risk vendors. Approval takes 5-10 business days.

Vendor Categories

Strategic vendors: Critical to operations, high spend, long-term relationship. Preferred vendors: Qualified vendors with favorable terms.

Approved vendors: Completed onboarding, available for use. Restricted vendors: Do not use without special approval.

Vendor Agreements

Master service agreements (MSA) for ongoing relationships. Statements of work (SOW) for specific projects.

Agreements include: Scope, pricing, payment terms, deliverables, SLAs, confidentiality, liability, termination. Legal review required.

Vendor Performance Monitoring

Track vendor performance: Quality, timeliness, responsiveness, compliance. Conduct quarterly reviews for strategic vendors.

Performance issues addressed through corrective action plans. Persistent issues may result in vendor termination.

Vendor Risk Assessment

Assess vendor risk based on: Data access, criticality to operations, financial stability, geographic location, regulatory compliance.

High-risk vendors require additional due diligence and monitoring. Annual risk reassessment for strategic vendors.

Payment Terms

Standard payment terms: Net 30 days. Early payment discounts negotiated when beneficial. Payment via ACH or wire transfer.

Vendors submit invoices with PO number. Payment processed after 3-way match (PO, receiving, invoice).

Vendor Compliance

Vendors must comply with our policies: Security, data protection, code of conduct, anti-corruption.

Vendor audits conducted for high-risk vendors. Non-compliance may result in contract termination.

Vendor Insurance Requirements

General liability insurance: \$1M minimum. Professional liability: \$1M for service providers. Workers compensation: As required by law.

Cyber liability: \$2M for vendors with data access. Company named as additional insured on policies.

Vendor Data Protection

Vendors with access to company or customer data must sign data protection agreement (DPA).

DPA includes: Data handling requirements, security standards, breach notification, data retention, audit rights.

Vendor Offboarding

Terminating vendor relationships: Provide notice per contract terms. Ensure knowledge transfer and transition plan.

Revoke system access. Retrieve company property and data. Final invoice reconciliation. Update vendor status to inactive.

Vendor Diversity

We encourage vendor diversity including minority-owned, women-owned, veteran-owned, and small businesses.

Diversity considered in vendor selection alongside price, quality, and service. Report vendor diversity metrics annually.

Conflict of Interest

Employees must disclose relationships with vendors (family, financial interest, outside employment).

Disclosed conflicts reviewed by compliance. May require recusal from vendor selection or oversight.