Vendor Policy Suite

Supplier Security Policy

Purpose: This policy defines the minimum security expectations required for all third-party suppliers.

Scope: Applies to every vendor that stores, processes, or transmits company data.

Roles and Responsibilities: Business owners submit vendor requests. Security reviews evidence. Vendors provide accurate documentation.

Requirements: Vendors must maintain strong access control, multi-factor authentication, encryption, monitoring, and vulnerability management.

Monitoring and Reporting: High-risk vendors must provide updated SOC 2 or ISO 27001 evidence annually.

Exceptions: Any exception requires written approval from Security leadership.

Enforcement: Vendors that do not meet requirements may be suspended or removed from service.

Third-Party Risk Management Policy

Purpose: Establish a structured process for assessing third-party security risk.

Scope: Applies to all vendors with access to company systems, data, or operational workflows.

Roles and Responsibilities: Security performs due diligence. Legal reviews contracts. Procurement manages onboarding.

Requirements: Includes tiering, evidence collection, security questionnaires, SOC 2 or ISO review, and risk scoring.

Monitoring and Reporting: High-risk vendors require continuous monitoring and periodic evidence updates.

Exceptions: Must be formally documented with an expiration date.

Enforcement: Vendors that fail remediation requirements may be denied approval.

Data Handling Policy

Purpose: Ensure all vendors manage company data securely.

Scope: Applies to any supplier that stores, processes, or transmits information.

Roles and Responsibilities: Vendors follow classification, handling, retention, and destruction guidelines.

Requirements: Encryption in transit and at rest, secure disposal, limited access, and proper data lifecycle management.

Monitoring and Reporting: Vendors must immediately notify Security of any data incident.

Exceptions: Reviewed individually and approved by Security leadership.

Enforcement: Violations may result in termination of the vendor relationship.

Access Control Policy

Purpose: Define access governance expectations for external users.

Scope: Applies to all external accounts accessing company systems.

Roles and Responsibilities: Security enforces multi-factor authentication. Business owners conduct quarterly access reviews.

Requirements: Least privilege access, documented onboarding and offboarding, privileged access monitoring, and time-bound exceptions.

Monitoring and Reporting: Privileged access is monitored continuously for unusual activity.

Exceptions: Granted only for specific operational needs and must be time-limited.

Enforcement: Unauthorized access results in immediate revocation and investigation.