IJEZIE
RISK ADVISORY

THIRD-PARTY INFORMATION SECURITY POLICY

Governing Security Expectations for External Vendors and Service Providers

Ifeanyi Ijezie

Ijezie Risk Advisory | https://github.com/ijeziermf

Third-Party Information Security policy

Version: 1.0

Effective Date: _____

Policy Owner: Information Security

Review Frequency: Annual

1. Purpose

The purpose of this policy is to establish security requirements and governance expectations for third-party vendors that access, process, store, or transmit organizational data or systems. This policy is intended to reduce cybersecurity, operational, and regulatory risk introduced by external parties by ensuring that third-party relationships are managed in a consistent and risk-based manner.

2. Scope

This policy applies to all third-party vendors, service providers, contractors, and business partners that have access to organizational systems, networks, applications, or data. It covers all vendor relationships regardless of engagement type, including cloud service providers, payment processors, software vendors, managed service providers, and other external entities.

3. Policy Statements

3.1 Third-Party Risk Management Principles

- Third-party security risk shall be identified, assessed, and managed prior to onboarding and throughout the vendor relationship.
- Vendors shall be evaluated based on the level of risk they pose to the organization, including the sensitivity of data accessed and the criticality of services provided.
- Security requirements for third parties shall be proportionate to the level of risk presented.
- Vendors may be categorized into risk tiers (e.g., high, medium, low) to determine the depth and frequency of security assessment activities.

3.2 Vendor Due Diligence and Onboarding

- Security due diligence shall be conducted prior to engaging a third-party vendor.
- Due diligence may include security questionnaires, attestations, certifications, or other evidence of security controls.
- Vendors with access to sensitive or regulated data shall undergo enhanced security review prior to approval.
- Identified security risks shall be documented and addressed prior to onboarding or formally accepted by management.

3.3 Contractual Security Requirements

- Contracts with third-party vendors shall include security requirements appropriate to the level of risk.
- Security requirements may include data protection obligations, access controls, incident notification timelines, and audit rights.
- Vendors shall be required to notify the organization of security incidents that may affect organizational data or systems within a defined timeframe.
- Contracts shall define vendor responsibilities for incident response, remediation, and cooperation with investigations.

3.4 Access and Data Handling

- Vendor access to organizational systems and data shall be limited to the minimum necessary to perform contracted services.
- Access shall be provisioned in accordance with organizational access control requirements and revoked promptly upon contract termination.
- Vendors shall handle organizational data in accordance with applicable data protection and privacy requirements.
- Data shared with vendors shall be classified and protected based on sensitivity.

3.5 Ongoing Monitoring and Reassessment

- Third-party security risk shall be reassessed periodically based on risk level, changes in service scope, or significant security events.
- High-risk vendors shall be reviewed at least annually or more frequently as required.
- Identified security issues shall be tracked and remediated in a timely manner.
- Continued use of a vendor shall be contingent upon acceptable risk posture.

3.6 Incident Notification and Response

- Vendors shall promptly report security incidents that impact or may impact organizational data or systems.
- Incident notifications shall include sufficient detail to support organizational response and regulatory obligations.
- Vendors shall cooperate with the organization during incident investigation, containment, and remediation activities.

3.7 Exceptions

- Exceptions to this policy must be formally documented and approved by Information Security and appropriate business owners.
- Exceptions shall include documented business justification, compensating controls, and defined review periods.
- Approved exceptions shall be reviewed periodically and revoked when no longer necessary.

4. Roles and Responsibilities

Information Security

- Defines third-party security requirements, conducts risk assessments, and monitors compliance with this policy.

Procurement and Vendor Management

- Ensures security requirements are incorporated into vendor selection and contracting processes.

Business Owners

- Identify third-party relationships, support risk assessments, and ensure vendors comply with security expectations.

Third-party Vendors

- Comply with contractual security requirements and promptly report security incidents.

5. Enforcement

Failure to comply with this policy may result in suspension or termination of vendor access, contract termination, or other corrective actions. Violations may also result in legal, regulatory, or contractual consequences. Non-compliant vendors may be subject to remediation requirements or disengagement.

6. Review and Maintenance

This policy shall be reviewed at least annually or upon significant changes to vendor relationships, regulatory requirements, or organizational risk posture. Updates shall be approved by appropriate governance authorities and communicated to relevant stakeholders.

7. Framework Alignment Reference

- NIST Cybersecurity Framework: ID.SC
- NIST SP 800-53: SR (Supply Chain Risk Management), RA (Risk Assessment)
- ISO/IEC 27001: Supplier Relations (Annex A)

This policy is intended to support organizational governance and third-party cyber risk management and may be adapted to align with specific operational, regulatory, or business requirements.

Document Control

Document ID	IRA-TPR-001
Approved By	_____
Classification	Internal
Next Review Date	_____