1000 Third-Party Vendor Management Policy v2

1000 THIRD-PARTY VENDOR MANAGEMENT POLICY

1000.1 Purpose:

The purpose of this Third-Party Vendor Management Policy is to establish guidelines and procedures for the selection, engagement, and ongoing management of third-party vendors by the Archdiocese of Baltimore.

This policy ensures that all third-party vendors adhere to the Archdiocese's standards for **security, privacy, and compliance** to safeguard sensitive information and maintain the organization's reputation.

1000.2 Scope:

This policy applies to all **employees, volunteers, contractors, and affiliates** of the Archdiocese of Baltimore who engage with or hold responsibilities related to third-party vendors.

1000.3 Vendor Selection:

1000.3.1 Due Diligence

a. Prior to engaging any third-party vendor, a thorough evaluation shall be conducted to assess qualifications, capabilities, and reliability.
b. The due diligence process must include assessment of the vendor's **security practices, privacy policies, regulatory compliance, financial stability, and reputation**.

1000.3.2 Vendor Evaluation Criteria

a. Vendors must demonstrate a commitment to maintaining the highest standards of **security, privacy, and ethical conduct**.
b. Evaluation criteria may include **experience, references, certifications, security controls, disaster recovery plans, and insurance coverage**.

1000.4 Contractual Requirements:

1000.4.1 Security and Privacy Requirements

a. Contracts with third-party vendors shall include provisions requiring compliance with applicable **security standards, regulations, and data protection laws**.
b. Vendors must agree to protect the **confidentiality, integrity, and availability** of all sensitive information shared with them.

1000.4.2 Data Handling and Processing

a. Vendors must handle and process data in accordance with the Archdiocese's **data protection and privacy policies**.
b. Data sharing, retention, and disposal requirements must be clearly defined within the contract.

1000.4.3 Right to Audit

a. The Archdiocese reserves the right to conduct **periodic audits or assessments** of the vendor's security controls, practices, and compliance.
b. Vendors must cooperate fully with audit requests and provide necessary documentation or evidence upon request.

1000.5 Ongoing Vendor Management:

1000.5.1 Vendor Performance Monitoring

a. Regular performance evaluations shall be conducted to assess the vendor’s adherence to contractual obligations and service level agreements (SLAs).

b. Monitoring activities may include reviewing **security incident reports, service quality metrics, and feedback** from internal stakeholders.

1000.5.2 Incident Response and Business Continuity

a. Vendors must maintain **incident response and business continuity plans** to minimize disruption and mitigate risks.

b. Procedures for reporting and managing **security incidents or breaches** must be jointly established between the vendor and the Archdiocese.

1000.6 Use of Third-Party Applications in Microsoft Azure:

1000.6.1 Policy Requirement

Only **Microsoft-certified applications** may be integrated or utilized within the Archdiocese’s Microsoft Azure Enterprise environment. Use of non-Microsoft-certified third-party applications is prohibited unless a formal exception is granted per section 1000.6.4.

1000.6.2 Security & Compliance Rationale

a. Microsoft-certified applications undergo **rigorous testing, validation, and ongoing review** to ensure compliance with security, privacy, and reliability standards.

b. Non-certified applications pose risks such as uncontrolled updates, inadequate encryption, hidden vulnerabilities, and regulatory non-compliance.

c. Restricting Azure integrations to certified apps helps maintain governance, reduce the attack surface, and ensure consistency in support and incident response.

1000.6.3 Operational Enforcement

a. All requests to integrate or enable third-party applications in Azure must be submitted to the **IT/Security Team** for review.
b. Only applications listed in Microsoft's official **Certified Azure Enterprise Applications Catalog** shall be approved.
c. Approved applications will be documented and monitored in the organization's **vendor/integration register**.
d. Periodic audits shall confirm continued compliance with certification, security updates, and enterprise alignment.

1000.6.4 Exceptions & Risk Assessment

a. Exceptions may be considered only with **written approval** from the CIO/CTO or Head of IT Security.
b. Exception requests must include a full **security and compliance risk assessment**, including threat modeling, encryption review, and vendor support evaluation.
c. Documented mitigation strategies must be approved and monitored for the duration of the exception.

1000.6.5 Non-Compliance

a. Use of non-certified applications without approval constitutes a **violation** of this policy.
b. Violations may trigger revocation of access, removal of the application, contract review, or disciplinary action per section 1000.9.
c. If a certified application loses certification or becomes deprecated, IT must evaluate alternatives or plan a controlled decommission.

1000.7 Domain Name Registration and Management:

1000.7.1 Policy Requirement

All Archdiocesan **parishes, schools, and affiliated centers** must have their registered internet domain names managed within the Archdiocese's **centralized Cloudflare account**. No entity shall independently register or manage domains outside of this centralized environment.

1000.7.2 Purpose and Rationale

a. Centralized management ensures **security, operational consistency, and business continuity** across all Archdiocesan entities.
b. Cloudflare provides **enterprise-level protection** including DNS security, redundancy, DDoS mitigation, and SSL management.
c. Decentralized or independently managed domains pose significant risks—such as **domain expiration, hijacking, DNS misconfiguration, lack of monitoring, or delayed incident response**.

1000.7.3 Implementation Requirements

a. All new or existing domains must be **registered, transferred, or delegated** into the official Archdiocese Cloudflare account under the Technology Department’s management.
b. IT will maintain an **authoritative domain inventory**, documenting ownership, expiration, DNS records, and associated services.
c. Any vendor or hosting provider supporting Archdiocesan domains must coordinate with the Technology Department to ensure compliance.
d. All DNS updates and configuration changes must be performed or approved by **authorized Technology Department staff**.

1000.7.4 Exceptions and Transitional Provisions

a. Legacy domains under separate management must be **reviewed and transitioned** during the next renewal cycle or as otherwise directed.
b. The Technology Department will assist all entities through the migration and validation process.

1000.8 Termination and Transition:

Procedures will be established to ensure a **secure and orderly transition** and retrieval of all Archdiocese-owned data and assets upon vendor contract termination or expiration.

1000.9 Compliance and Consequences:

Failure to comply with this Third-Party Vendor Management Policy may result in **contract termination, legal action, or disciplinary measures**, depending on the severity and frequency of non-compliance.

1000.10 Policy Review:

This policy will be **periodically reviewed and updated** by the Technology Department to ensure continued alignment with evolving security risks, regulatory requirements, and organizational needs.