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 aims to ensure that third-patty vendors adhere to the organization' s standards of 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 any individuals affiliated with the Archdiocese of Baltimore who engage with or have responsibilities related to third-party vendors.

1000.3 Vendor Selection:

3.1. Due Diligence

a. Prior to engaging a third-party vendor. a thorough evaluation will be conducted to assess their qualifications, capabilities, and reliability.

b. The due diligence process will include assessing the vendor's security practices, privacy policies, regulatory compliance, financial stability, and reputation.

3.2. Vendor Evaluation Criteria

a. Vendors must demonstrate a commitment to maintaining the highest

standards of security, privacy, and ethical conduct.

b. Criteria for evaluation may include vendor experience, references, certifications, security controls, disaster recovery plans, and insurance coverage.

1000.4 Contractual Requirements:

4.1. Security and Privacy Requirements

a. Contracts with third-patty vendors will 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 any sensitive information shared with them.

4.2. Data Handling and Processing

a. Vendors must agree to handle and process data in accordance with the Archdiocese of Baltimore’s data protection and privacy policies.

b. Data sharing, retention. and disposal requirements must be clearly defined in the contract.

4.3. Right to Audit

a. The organization reserves the right to conduct periodic audits or assessments of the vendor’s security controls, practices, and compliance.

b. Vendors must cooperate with any audit requests and provide necessary documentation and evidence of their security and privacy practices.

1000.5 Ongoing Vendor Management:

5.1. Vendor Performance Monitoring

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

b. Monitoring activities may include reviewing security incident repo1ts, service quality assessments, and feedback from internal stakeholders.

5.2. Incident Response and Business Continuity

a. Vendors must have appropriate incident response and business continuity plans in place to minimize disruptions and mitigate potential risks.

b. The organization and the vendor will establish procedures for reporting and managing security incidents and breaches.

1000.6 Termination and Transition:

Procedures will be established to ensure a smooth transition and secure retrieval of all organization-owned data and assets upon termination of the vendor relationship or contract expiration.

1000.7 Compliance and Consequences:

Failure to comply with the Third-Party Vendor Management Policy may result in contract te1111ination, legal action, or other appropriate consequences, depending on the severity and frequency of the non-compliance.

1000.8 Policy Review:

This Third-Party Vendor Management Policy will be periodically reviewed and updated to align with changing security risks, regulatory requirements, and organizational needs.