## 

### ***Disclaimer***

*This draft foundational document was prepared by a certified cybersecurity/GRC professional and is provided for general information only.* ***It is not legal advice.*** *Obtain independent legal review before adopting or relying on this policy.*

## 

### **General Vendor Information**

* **Vendor Name & Service Provided**
* **Primary Contact for Security & Privacy Concerns**

### **Data Processing & Privacy**

* **Review and sign Data Processing Agreement (DPA)**:  
  + Clearly defines responsibilities and confidentiality.
  + Specifies processing purpose and data retention rules.
* **List Sub-processors** (third parties that the vendor engages):  
  + Confirm vendor's approval process for new sub-processors.
  + Notification policy when sub-processors change.
* **Clarify Cross-border Data Transfer**:  
  + Document exact locations (countries/regions) where data is stored and processed.
  + Ensure transparency to users (privacy policy must reflect cross-border transfers clearly).

### **Encryption & Data Security**

* **Encryption of Data**:  
  + Encryption at rest (AES 256 recommended).
  + Encryption in transit (TLS 1.2 or higher).
* **Payment Data Protection (for Payment Gateways)**:  
  + Confirm vendor maintains current PCI-DSS compliance.
  + Verify cardholder data is never stored without proper tokenization/encryption.

### **Access & Authentication**

* **Support for Multi-Factor Authentication (MFA)**:  
  + Verify MFA is available and mandatory for account administrators.
* **User Access Management**:  
  + Ability to clearly assign role-based permissions.
  + Easy and secure onboarding/offboarding processes.

### **Security Practices & Compliance**

* **Vendor Security Certifications & Compliance**:  
  + NIST, OWASP, ISO 27001, or equivalent preferred.
  + Regular third-party security assessments or penetration tests.
* **Incident Response & Notification**:  
  + Confirm clear timelines for notifying your charity in case of a breach (ideally within 72 hours).
  + Clear process for incident reporting and support.

### **Audit & Transparency**

* **Request Vendor Security Documentation**:  
  + Vendor’s latest security audit summaries, if available.
  + Recent history of breaches/incidents (last 2-3 years).
* **Right to Audit or Review Vendor Controls** (optional but valuable):  
  + Clarify ability to request evidence of security practices.

### **Termination & Data Retrieval**

* **Clarify Exit Strategy**:  
  + Process and timelines for retrieving/deleting your data after service termination.
  + Guarantee of complete data deletion after the contract ends.

### **Insurance & Liability**

* **Vendor Liability & Insurance Coverage**:  
  + Review vendor’s liability clauses related to data breaches or losses.
  + Confirm adequate insurance coverage for cyber incidents.

### **Documentation**

* **Store Completed Vendor Security Reviews Centrally**:  
  + Maintain records accessible for future reference or regulatory inquiries.

**Implementation Tips:**

* Prioritize critical vendors (payment processors, email providers, cloud databases).
* Ensure responses are documented clearly and maintained securely.