**Cybersecurity Program Charter Template for Small Businesses**

**1. Introduction**

**Purpose**

This document outlines the cybersecurity program for [Company Name], aiming to protect our information assets against cyber threats, ensuring the confidentiality, integrity, and availability of data across all operations.

**Scope**

This charter applies to all employees, contractors, and third-party service providers of [Company Name], encompassing all digital and physical assets, systems, and data owned or managed by the organization.

**2. Objectives**

* To implement and maintain a robust cybersecurity posture that protects against unauthorized access, data breaches, and other cyber threats.
* To ensure compliance with [List Relevant Regulations] and other legal obligations related to information security.
* To foster a culture of security awareness and best practices among all employees and stakeholders.

**3. Governance**

**Steering Committee (if applicable)**

* **Members:** [Names or Titles of Committee Members]
* **Responsibilities:** Provide strategic direction, approve cybersecurity policies, and oversee program implementation and effectiveness.

**Roles and Responsibilities**

* **CISO/Security Lead:** [Name/Title, Responsibilities]
* **IT Department:** [Responsibilities]
* **Employees:** [Responsibilities]

**4. Program Components**

**Risk Management**

* **Process:** Identify, assess, and prioritize cybersecurity risks. Implement measures to mitigate significant risks to an acceptable level.

**Incident Response**

* **Plan:** Outline steps for detecting, responding to, and recovering from security incidents. Include contact information for key personnel and external partners (e.g., law enforcement).

**Asset Management**

* **Inventory Process:** Maintain an up-to-date inventory of all information assets and classify them according to their sensitivity and value to the business.

**Access Control**

* **Policies:** Define user access levels and implement controls (e.g., multi-factor authentication) to ensure that access to sensitive information is restricted and monitored.

**Training and Awareness**

* **Programs:** Conduct regular training sessions and awareness campaigns to educate employees about cybersecurity threats and safe practices.

**5. Compliance and Legal Requirements**

* **Regulations:** [List of Applicable Regulations]
* **Compliance Strategy:** Outline the approach for achieving and maintaining compliance with the identified regulations.

**6. Performance Measurement and Reporting**

**Metrics**

* **KPIs:** [List Key Performance Indicators]
* **Measurement Frequency:** [e.g., Quarterly]

**Reporting**

* **Report Recipients:** [List Stakeholders]
* **Frequency:** [e.g., Bi-annually]

**7. Budget and Resources**

* **Annual Budget:** [$ Amount]
* **Resource Allocation:** Detail the distribution of the budget across technology, personnel, training, and other essential resources.

**8. Review and Update Process**

* **Frequency:** [e.g., Annually]
* **Procedure:** Describe the process for reviewing and updating the cybersecurity program and this charter.

**9. Approval and Endorsement**

This charter is approved and endorsed by the undersigned stakeholders, signifying their commitment to the successful implementation and maintenance of the cybersecurity program for [Company Name].

* **[Name, Title]:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_
* **[Name, Title]:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_

(Additional signatures as required)

**Note:** This template is a starting point. Customize it to fit the specific needs, risks, and structure of your small business. Regular reviews and updates are essential to adapt to new threats and regulatory changes.