Program Charter – Small Business Cybersecurity Program

1. Scope Statement

The Cybersecurity Program applies to all information systems, devices, data, and processes used by the business, regardless of whether they are formally managed by IT.

Because the organization does not maintain a dedicated IT or cybersecurity department, the scope includes:

- Employee-owned and company-owned devices used for work (laptops, desktops, mobile phones)
- Internet access, Wi-Fi, and basic network equipment
- Cloud-based and SaaS services (email, file storage, accounting, CRM, payment platforms)
- User accounts, passwords, and access privileges
- Customer, financial, and internal business data
- Backup and data recovery processes
- Incident reporting and response
- Third-party service providers and vendors
- Basic security awareness and safe-use practices

Any system or tool used to conduct business is considered in scope.

---

2. Business Purpose

The purpose of this Cybersecurity Program is to reduce business risk in a practical and cost-effective way while allowing staff to perform their duties efficiently.

The program supports business objectives by:

- Protecting customer information and maintaining trust
- Reducing the likelihood and impact of ransomware, fraud, and data loss
- Minimizing downtime that could disrupt daily operations
- Supporting insurance, contractual, and basic regulatory expectations

- Enabling safe use of cloud services and remote work

Cybersecurity is treated as a shared responsibility across the business, supported by clear expectations and simple controls.

---

3. Statement of Authority

The **Business Owner** holds ultimate authority and accountability for the cybersecurity program.

Due to the size of the organization, the Business Owner:

- Sets cybersecurity expectations
- Approves policies and risk decisions
- Assigns cybersecurity-related tasks to staff as part of their normal duties

The Business Owner may designate one staff member as a **Cybersecurity Coordinator** to assist with organization and oversight but retains final responsibility.

---

4. Roles & Responsibilities

Business Owner

- Provides overall accountability for cybersecurity
- Approves policies and major risk decisions
- Ensures staff have time and basic resources to meet security expectations

Cybersecurity Coordinator (Designated Staff Member)

- Maintains basic security documentation
- Coordinates updates, reviews, and audits
- Acts as the main point of contact for security issues
- Escalates significant risks or incidents to the Business Owner

All Employees

- Follow cybersecurity policies and safe-use guidelines
- Use strong passwords and approved security tools

- Protect devices and business information
- Report suspicious emails, incidents, or data loss immediately

External IT or Service Providers (if used)

- Support technical security controls as contracted
- Notify the business of security incidents affecting services
- Follow agreed security requirements

---

5. Governance Structure & Processes

Cybersecurity governance is lightweight and integrated into normal business operations.

Key governance practices include:

- Written but concise cybersecurity policies
- Annual review of risks, systems, and vendors
- Periodic review of user access and accounts
- Informal check-ins between the Business Owner and Cybersecurity Coordinator
- Clear incident reporting and decision escalation paths

Decisions prioritize business impact, practicality, and risk reduction rather than complexity.

---

6. Program Documentation Procedures

Cybersecurity documentation is stored in a simple, centralized, access-controlled location (such as a shared cloud folder).

Documentation includes:

- Cybersecurity policies and guidelines
- Inventory of key systems and accounts
- Incident reports and lessons learned
- Backup and recovery procedures
- Vendor and service provider information

Documentation is:

- Kept simple and readable
- Reviewed at least annually
- Updated when major changes or incidents occur

---

7. Enforcement Mechanisms

Cybersecurity requirements apply to all staff.

Enforcement focuses on prevention, awareness, and correction rather than punishment.

Mechanisms include:

- Required acknowledgment of policies
- Basic technical controls (password managers, MFA, backups)
- Periodic checks of compliance with security practices

Repeated or serious non-compliance may result in:

- Removal of system access
- Reassignment of responsibilities
- Disciplinary action as appropriate

Vendors may face contract termination for security failures.

---

8. Review Process

The Cybersecurity Program is reviewed to ensure it remains effective and appropriate for the size of the business.

Reviews include:

- Annual self-assessment or simple audit and gap analysis
- Review following major technology or business changes
- Immediate review after any security incident or data loss

Improvements are documented and implemented as part of normal operations.

---

9. Approval Statement

This Cybersecurity Program Charter is approved and enforced under the authority of the Business Owner.

By approving this charter, leadership affirms that cybersecurity is a shared responsibility and a necessary part of protecting the business, employees, and customers.

Approved by: _____
Title: Business Owner
Date: _____