## **Information Security Policy Template for Small Business Restaurant**

### **1. Purpose**

The purpose of this Information Security Policy is to establish guidelines for protecting the information assets of [Restaurant Name], ensuring the confidentiality, integrity, and availability of sensitive data.

### **2. Scope**

This policy applies to all employees, contractors, and third-party service providers who access [Restaurant Name]'s information systems and data.

### **3. Data Classification**

#### **3.1 Classification Levels**

* **Confidential Data**: Includes customer payment information, employee records, and supplier contracts.
* **Internal Use**: Business operation documents, schedules, and internal communications.
* **Public Data**: Menu information, promotional materials, and press releases.

### **4. Access Control**

#### **4.1 User Access Management**

* Access to confidential data is restricted to authorized personnel based on job roles.
* Employees must use unique usernames and strong passwords that meet the following criteria:
  + Minimum of 12 characters
  + Includes uppercase and lowercase letters, numbers, and special characters
* Passwords must be changed every 90 days.

#### **4.2 Authentication**

* Multi-factor authentication (MFA) is required for access to sensitive systems.

### **5. Data Protection**

#### **5.1 Data Encryption**

* All sensitive data must be encrypted in transit and at rest using industry-standard encryption methods.

#### **5.2 Payment Card Industry Data Security Standard (PCI-DSS)**

* Customer payment information must be processed using PCI-DSS compliant systems.

#### **5.3 Data Retention**

* Confidential data must be retained only as long as necessary for business or legal purposes and securely disposed of when no longer needed.

### **6. Incident Response**

#### **6.1 Incident Reporting**

* Employees must report any security incidents, including breaches, suspicious activities, or data loss, to management immediately.

#### **6.2 Incident Management**

* An incident response team will investigate reported incidents and document findings, including impact assessment and remedial actions taken.

### **7. Training and Awareness**

#### **7.1 Security Training**

* All employees must complete mandatory information security training upon hiring and annually thereafter.

#### **7.2 Security Awareness**

* Regular security awareness communications, including phishing simulations and reminders, will be provided to staff.

### **8. Policy Compliance**

#### **8.1 Compliance Monitoring**

* Regular audits will be conducted to ensure adherence to this policy and identify areas for improvement.

#### **8.2 Violations**

* Any violation of this policy may result in disciplinary action, up to and including termination of employment.

### **9. Policy Review**

This policy will be reviewed annually and updated as necessary to reflect changes in regulatory requirements, industry standards, and emerging threats.