					[Insert Registered Legal Entity Name Here]							
Document number: P1S					Document Title: **Information Security Policy**							
Version: 1.0		Effective Date:			Document Owner: IT							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 5.1, 5.2, 5.3, 6.1, 6.2, 8.1	
ISO/IEC 27002:2022	Controls 5.1–5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	

					[Insert Registered Legal Entity Name Here]									
Document number: P1S					Document Title: **Information Security Policy**									
Version: 1.0		Effective Date:			Document Owner: IT									
X	Policy		Standard		Procedure		Form		Register		Other			

Purpose

1.1. This policy demonstrates **our organization's** commitment to protecting customer and business information by clearly defining responsibilities and practical security measures, suitable for organizations without dedicated IT teams.

1.2. It ensures that all employees, contractors, and service providers follow enforceable rules, enabling full compliance with ISO/IEC 27001 certification requirements.

1.3. This policy enables **our organization** to build customer trust by clearly demonstrating how we protect their information through defined responsibilities, structured processes, and strong accountability.

2. Scope

2.1. This policy applies to all individuals who access or manage the organization's data and systems, including:

2.1.1. Business owners and general managers

2.1.2. Employees, contractors, interns

2.1.3. External IT service providers or consultants

2.2. It covers all types of information, systems, and services, including:

2.2.1. Business records, customer data, passwords, and emails

2.2.2. IT hardware such as laptops and phones

2.2.3. Cloud services used for file storage, communication, or finance

2.2.4. Physical documents stored in office locations

2.3. The policy applies across all work environments—office-based, remote, and cloud-based—and includes all devices and software used to process or store business information.

3. Objectives

3.1. **Assign Clear Responsibility:** Ensure that someone is always accountable for information security. Typically, this is the General Manager or the person they formally assign.

3.2. **Protect Customer and Business Information:** Provide reliable and consistent safeguards to prevent misuse, loss, or theft of sensitive data, including customer and financial records.

3.3. **Support ISO/IEC 27001 Certification:** Enable the organization to demonstrate full compliance with ISO/IEC 27001 requirements, making it audit-ready and certification-eligible without requiring complex infrastructure.

3.4. **Embed Security in Business Operations:** Integrate information security into daily tasks and decisions across the organization.

3.5. **Build Security Awareness and Culture:** Encourage every employee to understand and uphold security practices, such as using strong passwords and reporting suspicious activity.

4. Roles and Responsibilities

4.1. **General Manager or Business Owner**

4.1.1. Holds full accountability for information security.

4.1.2. Approves and maintains this policy.

4.1.3. Ensures all key security tasks are either handled directly or delegated in writing.

4.1.4. Verifies that any delegated security tasks (such as managing access or responding to incidents) are carried out effectively.

4.1.5. Serves as the default contact for all internal and external security matters, including audits and customer inquiries.

4.1.6. Is monitoring progress against these objectives during the annual review. Objectives should be measurable where possible (e.g., % of staff trained, number of incidents reported, etc.) and revised based on security findings and changes in risk.

4.2. **Designated Employee (if applicable)**

4.2.1. May assist the General Manager by managing day-to-day tasks, such as creating user accounts, removing access for leavers, or coordinating with the IT provider.

4.2.2. Must be officially assigned and have enough authority and tools to carry out the tasks.

4.2.3. Reports any issues back to the General Manager.

4.3. **External IT Service Provider (if used)**

4.3.1. Implements and maintains technical protections like firewalls, antivirus software, backups, and secure access.

4.3.2. Provides advice to the General Manager on IT risks and issues.

4.3.3. Must act promptly on identified security risks and report them immediately to the General Manager.

4.3.4. Must follow the organization's security requirements and be bound by contract or written agreement.

4.4. **All Staff, Contractors, and Temporary Workers**

4.4.1. Must follow all security instructions, including:

4.4.1.1. Using systems only for authorized purposes

4.4.1.2. [……..]