**[Business Name]**

**Written Information Security Policy (WISP)**

**Effective Date:** [Insert Date]  
**Last Reviewed:** [Insert Date]  
**Version:** [Insert Version Number]

**1. Purpose**

The purpose of this Written Information Security Policy (WISP) is to establish a formal, documented framework to protect the confidentiality, integrity, and availability of sensitive information handled by [Business Name]. This policy ensures appropriate security measures are implemented to protect personal, financial, and confidential data from unauthorized access, disclosure, or loss.

**2. Scope**

This policy applies to all employees, contractors, vendors, and other individuals or entities with access to [Business Name]'s information systems and data. It covers all physical and digital information, including:

* **Customer information** (e.g., personal data, financial information)
* **Employee information**
* **Company proprietary information**
* **Vendor and partner information**
* **Any other sensitive business data**

**3. Roles and Responsibilities**

3.1. **Information Security Officer (ISO):**

* Oversees the development, implementation, and management of the company’s information security strategy.
* Ensures compliance with policies, regulatory requirements, and conducts audits.

3.2. **Employees:**

* Must adhere to the security practices outlined in this policy.
* Complete regular security training and report any suspicious activities or security incidents within **24 hours** to the ISO or IT department.

3.3. **IT Department:**

* Implements and maintains technical controls (e.g., firewalls, encryption tools).
* Monitors for security incidents and mitigates risks to software, hardware, and networks.

3.4. **Third Parties:**

* Vendors and contractors with access to company systems and data must comply with this policy and relevant security protocols outlined in vendor agreements.

**4. Data Classification and Handling**

4.1. **Public Information:**  
Non-sensitive data intended for public dissemination.

4.2. **Internal Use Only:**  
Information not for public release but not highly sensitive.

4.3. **Confidential Information:**  
Sensitive information requiring protection (e.g., personally identifiable information, financial data).

4.4. **Restricted Information:**  
Highly sensitive data, where disclosure could cause significant harm to the company (e.g., financial records, intellectual property).

**Handling Requirements:**

* Confidential and Restricted Information must be **encrypted** both at rest and in transit using AES-256 encryption or higher.
* Physical documents containing sensitive data must be stored in **locked cabinets or rooms** with restricted access.
* All employees must securely **shred** physical documents containing Confidential or Restricted Information after use.

**5. Access Control**

5.1. **Role-Based Access Control:**  
Access to systems and data is granted based on **job roles** and responsibilities. Employees receive only the access necessary to perform their job functions (principle of **least privilege**).

5.2. **Authentication:**  
All users must authenticate with **strong passwords** and multi-factor authentication (MFA) where applicable.  
Password Requirements:

* **Minimum of 12 characters**
* **Must include** uppercase, lowercase, numbers, and special characters
* **Changed every** [Insert Period, e.g., 90 days]

5.3. **Account Monitoring and Management:**

* The IT department will **monitor user accounts** and permissions on a regular basis.
* Unused or inactive accounts will be **disabled after [Insert Number of Days]**.

**6. Data Protection**

6.1. **Encryption:**

* Sensitive data must be encrypted using **industry-standard algorithms** (e.g., AES-256).
* Encryption applies to:
  + **Data at rest** (stored data)
  + **Data in transit** (transmitted data)

6.2. **Backups:**

* Regular data backups must be performed, with backup copies securely stored in **offsite or cloud locations**.
* All backups must be encrypted and periodically **tested for integrity** to ensure recovery capability.

6.3. **Remote Access:**

* Remote access to company systems must be secured via **VPNs or secure channels**.
* Remote workers must comply with the same security standards as those working on-premises.

**7. Incident Response**

7.1. **Incident Detection:**

* Employees are required to report **suspicious activities or potential breaches within 24 hours** to the ISO or IT department.

7.2. **Incident Handling:**  
The **Incident Response Team (IRT)** will follow the **Incident Response Plan**, which includes:

* **Identification** of the threat
* **Containment and mitigation** of the incident
* **Investigation and documentation** of the cause
* **Restoration** of affected systems
* **Notification to affected parties** within [Insert Period] if required by law or regulation

**8. Training and Awareness**

* **All employees** must complete **annual security awareness training**, covering:
  + Recognizing **cybersecurity threats** (e.g., phishing, ransomware)
  + **Safe computing practices** (e.g., password management, device security)
  + Company-specific security policies and procedures
* **New employees** must undergo mandatory information security training during onboarding.

**9. Physical Security**

9.1. **Secure Areas:**

* Areas where sensitive data is stored must be **physically secured** with access restricted to **authorized personnel only**.

9.2. **Device Security:**

* Laptops, mobile devices, and other equipment must be physically secured at all times.
* Employees must **lock screens** when leaving their devices unattended.

**10. Compliance and Audits**

10.1. **Legal and Regulatory Compliance:**  
[Business Name] will ensure compliance with **all applicable laws, regulations, and standards** (e.g., **GDPR, HIPAA, CCPA**) concerning data security.

10.2. **Audits and Reviews:**

* The ISO will conduct **regular audits** and **policy reviews** to ensure continued compliance with evolving security standards and legal requirements.
* **Third-party audits** may be conducted as necessary to validate compliance.

**11. Policy Enforcement**

* **Violations** of this policy will result in disciplinary action, up to and including **termination of employment**.
* Vendors and contractors found in violation may have their **contracts terminated** or face **legal action** as appropriate.

**12. Policy Review**

* This WISP will be reviewed **annually** or **after any significant security incident**.
* Changes will be communicated to all employees and relevant stakeholders promptly.

**13. Approved by:**

**[Name]**, [Title]  
**Date:** [Insert Date]

**14. Acknowledgment and Acceptance**

I, **[Employee/Contractor/Vendor Name]**, have read, understood, and agree to comply with the terms of this Written Information Security Policy (WISP). I acknowledge that failure to adhere to these policies may result in disciplinary action or termination of agreements, as applicable.

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Disclaimer:**

This template is provided as a **sample policy** for general guidance. It should be **reviewed by your IT and Legal teams** to ensure it aligns with **specific governmental, regulatory, and industry compliance requirements** relevant to your business.