**ChannelPro Written Information Security Policy Template**

A Written Information Security Program (WISP) is a crucial component for any organization that handles sensitive data. All businesses, including MSPs themselves, should have a WISP. By working on a WISP collaboratively with your client, you can educate them on the dangers of inaction and the importance of an ongoing financial commitment to security measures.

This template is a general guide and starting point. It should be heavily customized to meet the business’ individual needs.\*

**Written Information Security Policy**

**Effective Date: [Date]**

### **Introduction**

This Written Information Security Program ("WISP") is established by [Company Name] to protect the security, confidentiality, integrity, and availability of Personally Identifiable Information (PII) and other sensitive data it collects, stores, transmits, and processes. This document outlines the administrative, technical, and physical safeguards implemented to ensure data protection in compliance with applicable laws and industry standards.

### **Scope**

This WISP applies to all employees, contractors, and third-party service providers of [Company Name] who have access to PII and other sensitive information within the organization’s network and physical premises.

This policy encompasses all systems, automated and manual, for which the organization has administrative responsibility, including systems managed or hosted by third parties on the organization’s behalf.

### **Roles and Responsibilities**

Specify what each group/person is responsible for:

* Executive Management
* Information Security Officer (ISO)
* IT Management
* Employees
* Contractors

### **Risk Assessment and Management**

[Company Name] conducts regular risk assessments to identify, evaluate, and manage risks to its information assets. This section details the risk assessment methodology and frequency.

### **Security Measures**

[Elaborate upon each of these bulletpoints:]

* **Access Control**: Measures to ensure that access to sensitive information is appropriately controlled.
* **Data Encryption**: Standards for encrypting data at rest and in transit.
* **Systems Security:** Systems include but are not limited to servers, platforms, networks, communications, databases and software applications. Account for testing, maintenance, and decommissioning in accordance with the lifecycle of the hardware or software.
* **Physical Security**: Safeguards to protect physical locations and assets.
* **Incident Response Plan**: Procedures for responding to security breaches or incidents.
* **Employee Training**: Requirements for ongoing education on information security and privacy.

### **Third-Party Service Providers**

List requirements and standards for third-party service providers handling [Company Name]'s sensitive information, including compliance with this WISP.

### **Incident Response and Notification**

List procedures for identifying, responding to, and recovering from security incidents, including notification processes for affected individuals and authorities.

### **Monitoring and Review**

[Company Name] will regularly monitor compliance with this WISP and review the program annually or in response to significant changes in the business or threat landscape.

### **Acknowledgment**

This policy shall take effect upon publication. Employees, contractors, and third parties must acknowledge they have read and understood the WISP and agree to comply with its provisions. Non-compliance may result in disciplinary action, including termination of employment, as well as legal action.

### **Contact Information**

Submit all inquiries and requests for future enhancements to: [contact information]

### **Amendments & Revision History**

This WISP may be amended or revised by [Company Name] at any time to improve security practices or comply with new regulations.

### This document shall be subject to periodic review to ensure relevancy.

|  |  |  |
| --- | --- | --- |
| **Date**  | **Description of Change**  | **Reviewer** |
|  |  |  |

\*The ChannelPro Network, its parent company, or subsidiaries are not liable for any claim, damage, or loss of any kind caused by the use or misuse of this template.