

Written Information Security Policy

Does your organization have a Written Information Security Policy? Why Does my Company need one? A Written Information Security Policy (WISP) is a documented statement of rules and guidelines that need to be followed by people accessing company data, assets, systems and other IT resources. **Let KiZAN create one for you.**

WHAT ARE THE BENEFITS OF A WRITTEN INFORMATION SECURITY POLICY?

1. Defines Roles and Responsibilities by indicating who is authorized to perform various tasks and associated responsibilities.
2. Defines Accountability by having to be acknowledged and signed by employees and outlines the consequences of not adhering to the policy.
3. Increased employee cybersecurity awareness with education documents and can teach employees about cybersecurity best practices.
4. Addresses threats by including actions to be performed, recover from a breach or cyber-attach and ways to mitigation vulnerabilities.
5. Complies with Regulations such as PCI, GDPR, HIPAA, CCPA, or ISO/IEC 27002

WHY IS A WRITTEN INFORMATION SECURITY POLICY IMPORTANT TO MY COMPANY?

Depending on industry, noncompliance could lead to fines, lawsuits and loss of reputation.

What Does a Written Information Security Plan Typically Include?

- ✓ Purpose of Policy
- ✓ Scope of the Policy
- ✓ Sanctions
- ✓ Exceptions
- ✓ User Agreement

Regardless of the size of your organization, a Written Information Security Policy is vital in protecting company data, IT resources and increasing employee cyber awareness. Written Information Security Policies help companies remain competitive and earn (and retain) the trust of their clients or customers.

Kizan understands the importance of a Written Information Security Policy. Whether you have a plan already in place that needs updating or you need help getting started, let our experts guide you through the process.

Contact Us



KiZAN Technologies
www.kizan.com
(877) 775-7159