



MANAGING YOUR RISK AS AN ORGANIZATION REQUIRES COMPREHENSIVE TECHNOLOGY POLICIES

Creation and management of the following policies can be provided by our team.

| | |
|--------------------------------------|--|
| Acceptable Use | Governs use of computing information technology resources in a responsible manner, respecting the rights and privacy of others and complying with applicable laws and the Firm's policies and standards. |
| Access Control | Governs granting access to the Firm's sensitive information, limiting access only to those who need it. |
| Backup | Provides a consistent framework to ensure backups are available and useful when needed, providing the last line of defense against data loss from a hardware failure, data corruption, or a security incident. |
| Breach Notification | Governs the Firm's legal and/or ethical obligations to report, mitigate, or otherwise respond to any loss or inadvertent disclosure of confidential or protected information related to the client, its work, or its personnel. |
| Business Continuity | Protects the welfare of staff, visitors, and clients by providing for the continued delivery of products and services at acceptable, predefined levels following a disruptive incident. |
| BYOD | Specifies Firm standards for the use and security of mobile devices to protect the integrity and confidentiality of the Firm's data and the security of the network; applies to company data as it relates to mobile devices that can store such data, including but not limited to laptops, notebooks, PDAs, smartphones, and USB drives. |
| Change Control | Provides a managed and orderly method in which changes to the information technology environment are requested, tested, and approved prior to installation or implementation. |
| Clean Desk | A corporate directive that specifies how employees should leave their workstations whenever they leave the office or their workspace. |
| Client Technology | Governs the usage of the Firm's IT resources and communication systems and all use of such resources and systems when accessed using an employee's own resources. |
| Cloud Computing Security | Ensures that cloud services are not used for firm or client business without appropriate management knowledge and approval. |
| Cybersecurity | Establishes guidelines and provisions for preserving the security of the Firm's data and technology infrastructure through security controls and preventive measures. |
| Cybersecurity Threat Response | Defines the Firm's responsibility in responding to security threats affecting the confidentiality, integrity, and/or availability of information technology resources. |



| | |
|--|---|
| Data Classification | Governs information resources by providing a system for classification, storage and processing, and management for information handling, retention, and destruction. |
| Encryption | Establishes the types of devices and media that need to be encrypted, defines when encryption must be used, and sets the minimum standards for the level of encryption. |
| HIPAA | Governs the Firm's obligations for the security and privacy of a variety of clients' privileged and confidential information pursuant to applicable Federal and State consumer protection laws. |
| Identity Theft | Defines the Firm's standards for identifying and protecting against an imposter using a Firm employee's identity - or someone else's identity - to obtain services or information from the Firm. |
| Information Governance | Provides for the review, classification, retention, and destruction of both paper and electronic records received or created by the Firm. |
| Password | Establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of required password changes. |
| Personnel Security | Ensures that adequate checks are established to determine and/or confirm, within appropriate legal and professional limits, the qualifications and suitability of a job candidate for roles within the Firm. |
| Physical Security | Governs the safety and protection of computers, routers, cables, and other devices essential for business. |
| Remote Access | Provides a framework for secure remote access to Firm resources; defines standards for accessing corporate information technology resources from outside the network. |
| Security Awareness & Training | Governs the implementation of ongoing security awareness and training programs for all members of the Firm's workforce. |
| Social Media | Governs employee use of social media as relates to the Firm; protects the Firm, its employees, clients, vendors, and business associates from damages and potential criminal liability resulting from improper or unlawful use of social media. |
| Third-party Vendor | Identifies vendors that pose the greatest risk to the organization and defines controls for the Firm to implement to mitigate this risk. |
| Vulnerability Management | Defines standards to develop and implement procedures to prevent, detect, contain, and correct security violations utilizing automated tools to scan systems, computing and network devices, and web applications and application codes. |

Book your free 15-minute discovery call.

rizetechnologies.com ● (954) 204-0212 ● info@rizetechnologies.com