Written Information Security Program

Written Information Security Policies created by MergerTree for MMCA clients cover all categories of the NIST framework. Policies create a blueprint for information security from identifying information assets, to protecting those assets, detecting any threat to those assets, responding to threats, and recovering any information assets compromised in a security event. Creating and managing these policies establishes a full Written Information Security Program.

- Information Classification and Handling Policies/ Identify
    - Identify the confidentiality, integrity and availability requirements of corporate data. Establish standard restrictions and requirements for copying, printing, distribution, storage, disposal, logging and retention of each data classification.
- Information Asset Management Policies/ Identify and Protect
    - Create inventory of all information assets. Establish life cycle standards from acquisition to disposal of all assets. Establish mobile device management policies.
- Access Control Policies/ protect
    - Network, Physical, and Remote Access Control Policies
    - Establish role based access controls using least privilege principle. Create standards for all user authorization, enrollment and suspension of access. Establish password management policy.
- IT Vendor Management Policy/ Protect
    - Vendor questionnaire
- Acceptable Use Policies/ Protect
    - Establish Clean Desk policy and corporate standards and restrictions for email and all social media use.
- Encryption Policies / Protect
    - Establish data protection requirements for data in transit and data at rest. Define guidelines for removable media use. Define standards for cryptography.
- Information Security Management Policy/ Protect
- Network Security Policies/ Protect
    - Network security including Router, Switch Firewall and wireless access security.
- Change Management Policy/ Protect
    - Establish change management procedure for all software, hardware and network changes.
- Applications Development and Application Acquisition Policy/ Protect
- Security Logging and Monitoring Policies/ Detect
    - Include continuous threat monitoring. Include network activity monitoring. Establish threat response plan. Define parameters for monitoring and logging of network activity.
- Security Incident Response Policy/ Respond
    - Security incident event identification, reporting, monitoring, management and historical recording.
- IT Business Continuity and Disaster Recovery Policies/ Recover
- Update and Assessment Policy/ Recover

MergerTree Solutions – All Rights Reserved