Sample Information Security Policy

Version: 1.0 | Effective Date: January 1, 2024

1. Network Segmentation Requirements

1.1 All production systems shall be isolated from development environments.

1.2 Network micro-segmentation must be implemented to limit lateral movement.

1.3 Critical assets shall be placed in dedicated security zones with strict access controls.

2. Access Control Requirements

2.1 All network access shall follow the principle of least privilege.

2.2 Default deny policies must be enforced for all inter-zone traffic.

2.3 Administrative access shall require multi-factor authentication.

3. Monitoring Requirements

3.1 All network traffic shall be logged and monitored.

3.2 Security alerts must be generated for policy violations.

3.3 Flow data shall be retained for a minimum of 90 days.

4. Endpoint Security Requirements

4.1 All workloads must have security agents installed and reporting.

4.2 Workload enforcement status shall be monitored continuously.

4.3 Unmanaged devices should be quarantined from production networks.

5. Compliance Requirements

5.1 Security configurations must comply with CIS benchmarks.

5.2 Regular compliance audits shall be conducted quarterly.

5.3 Non-compliant systems should be remediated within 30 days.