



**Insert company
logo here**

Information Security Policy and Procedures Manual



Information Security Policy and Procedures Manual Table of Contents

• Overview.....	3
• Purposes.....	3
• Scope.....	3
• Policy.....	4
• Roles and Responsibilities.....	4
○ Chief Technology Officer Chief Information Officer.....	4
○ Director of Information Technology Senior Information Security Officer.....	4
○ Network Engineer Systems Administrator.....	4
○ Software Developers Coders.....	5
○ Change Management Change Control Personnel.....	6
○ End Users.....	6
○ Vendors, Contractors, Other Third-Party Entities.....	6
• Information Security Solutions.....	7
• Defense-in-Depth.....	7
• Layered Security.....	8
• Cyber Security.....	8
• Cloud Computing.....	9
• Email Guidelines, Responsibilities and Acceptable Use.....	9
• The CAN-SPAM ACT.....	12
• Internet Guidelines, Responsibilities and Acceptable Use.....	13
• Network Guidelines, Responsibilities and Acceptable Use.....	15
• Social Media Guidelines, Responsibilities and Acceptable Use.....	17
• Identity Theft.....	20
• Securing Your Home Network.....	21
• Online Security and Mobile Computing.....	23
• Online Shopping.....	24
• Other Important Security Considerations.....	25
• Helpful Security Resources.....	29
• Security Updates.....	33
• Workstation Security.....	34
• Laptop Security.....	36
• Software Licensing and Usage.....	37
• Internal Threats.....	38
• Clean Desk Policy.....	39
• Data Security Breaches.....	40
• Data and Information Classification.....	41
• Security Categorization.....	42
• Asset Inventory.....	42

[Insert Company Logo]

• Personally Identifiable Information (PII)	43
• Protected Health Information (PHI)	44
• Personally Identifiable Financial Information (PIFI)	44
• Physical Security and Environmental Security	45
• Personnel	45
• Security Awareness Training	46
• Provisioning and Hardening	46
• Reference Material	47
• Time Synchronization	47
• Access Rights	48
• Methods of Authentication	48
• Password Parameters	49
• De-Provisioning Off-boarding Process	50
• Remote Access	51
• Wireless Security	51
• Malware	53
• Change Control Change Management	53
• Software Development Life Cycle (SDLC)	54
• Patch Management	56
• Vulnerability Management	57
• Configuration Management	58
• Vendor Management	58
• Backup and Storage	59
• Encryption	60
• Event Monitoring	61
• Configuration and Change Monitoring	61
• Performance and Utilization Monitoring	62
• Logging and Reporting	62
• Data Retention and Disposal	63
• Incident Response	63
• Performance and Security Testing	64
• Disaster Recovery	64
• Authorization Form for User Access New Employees	67
• Authorization Form for User Access Vendors	71
• Authorization Form for User Access Guests	75
• User De-provisioning Off-boarding Form All Users (Employee, Guest, Vendor, Other)	79
• Employee Separation Form	82
• Change Management Request Form (CMRF)	85
• Change Management Logging System (CMLS)	87
• Remote Access Request Form	88
• Incident Response Plan Form	91
• Security Awareness Training Instructional Guide	92
• Wireless Security Checklist	101

[Company name Information Security Policy and Supporting Procedures]