



INFORMATION SECURITY
& CYBERSECURITY POLICY AND PROCEDURES MANUAL

- LIGHT EDITION -

TABLE OF CONTENTS

- Introduction..... 1
- Goals..... 1
- Information Systems Scope..... 1
- A Team Effort..... 2
- Access Rights..... 2
- Anti-Virus/Anti-Malware..... 4
- Assessing Online Threats..... 5
- Asset Inventory..... 6
- Audit Logs..... 7
- Awareness and Cyber Education..... 7
- Backups..... 8
- Business Continuity and Disaster Recovery..... 8
- Change Control..... 8
- Clean Desk..... 9
- Cloud Computing Essentials..... 9
- Computer Provisioning and Baseline Hardening..... 10
- Computer Monitoring..... 10
- Configuration Management..... 11
- Cyber Security..... 12
- Data Categorization for I.T. Systems..... 12
- Data Retention..... 13
- Data Security Breaches..... 14
- Email Best Practices..... 14
- Encryption Requirements..... 17
- Event Monitoring for I.T. Systems..... 18
- Have a Home Network? Secure it!..... 18
- Incident Response to Organizational Assets..... 19
- Insider Threats are Everywhere..... 19
- Internet Best Practices..... 20
- Internet Best Practices for Social Media Interaction..... 22
- Laptop Best Practices..... 25
- Managing Third-Parties..... 26
- Network Security..... 26
- Network and Server Patching Essentials..... 28
- Network Time Protocol..... 29
- Penetration Tests and Vulnerability Scans..... 29
- PII and PHI..... 30
- Physical Security Measures..... 31
- Remote User Access..... 31
- Securing and Updating Systems..... 32
- Securing Workstations..... 32

• Systems Development.....	34
• Software Use.....	35
• Terminating Users.....	36
• Vulnerability Management.....	37
• Wireless Environments.....	38
Appendix.....	40
• User Access Forms.....	41
• User Termination Forms.....	53
• Change Control Forms.....	60
• Remote Access Form.....	64
Terms of Use and Licensing.....	68