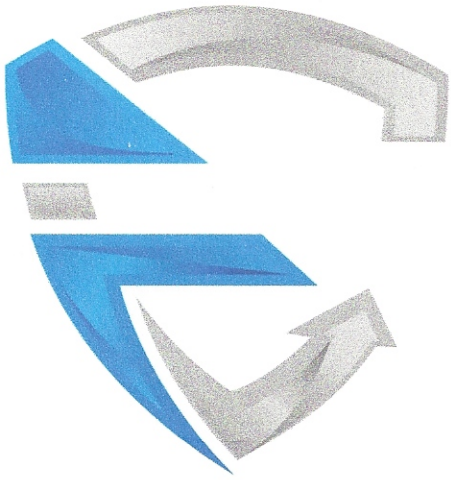

CYBER
FORWARD

Information Security Playbook

Table of Contents

Policy Documents

- ❑ Access Control
- ❑ Audit & Accountability
- ❑ Configuration Management
- ❑ Identification & Authentication
- ❑ Incident Response
- ❑ Maintenance
- ❑ Media Protection
- ❑ Personnel Security
- ❑ Physical & Environmental Security
- ❑ Risk Assessment
- ❑ Security Assessment
- ❑ Security Awareness & Training
- ❑ System & Information Security
- ❑ System & Communication Protection
- ❑ Acceptable Use

System Security Plan

Plan of Action & Milestones

CRAFTING YOUR CYBERSECURITY FUTURE

CYBER FORWARD™

Access Control Policy

Account Types
- ❑ Elevated Privilege
- ❑ Limited Privilege

Group Types
- ❑ CUI Access
- ❑ No CUI access

Information Types
- ❑ CUI
- ❑ Non-CUI

Role Types
- ❑ Administrator (*Elevated Privilege, No CUI Access*): builds, manages, maintains, secures & operates information technology.
  - ☑ Administrator accounts will be audited monthly and will only be used for administration activities
- ❑ Approver (*Limited Privilege*): authorizes account creation/termination, remote/wireless/mobile/ external-system access, placing information in publicly accessible locations and CUI access
  - ☑ Approver designation documented in formal document, which is updated (at least) monthly.
  - ☑ Approval authority must be appointed and not assumed.
- ❑ Auditor (*Limited Privilege*): reviews appropriate activities for compliance
- ❑ User (*Limited Privilege*): interacts with systems to access appropriate workplace applications
  - ☑ All user accounts will maintain least privilege required to perform essential work functions
- ❑ Process User: a restricted user account created specifically for a system or service process
  - ☑ Processes can only be run from a process user account
  - ☑ Process user accounts can only be used to run designated system or service processes

Information Flow Controls
- ❑ Outside traffic that claims to be from within the organization will be blocked at the boundary
- ❑ Web requests to the Internet will flow through monitored and controlled access points
  - ☑ Specific transaction may require exceptions
- ❑ CUI data will only be maintained or transferred within a secure environment using secure means
- ❑ Lateral movement should be limited to appropriate network resources (web, mail, DNS, NTP, etc.)

User Session Limitations
- ❑ Individuals must use user (rather than administrator) accounts to access CUI data
- ❑ Accounts locked after 5 unsuccessful attempts within 15 minutes & require administrator actions
- ❑ Screen savers set to initiate ≥ 30 minutes of inactivity and require password use to unlock
- ❑ Screen savers completely obfuscate any data on the screen
- ❑ Sessions terminated after 6 hours of inactivity and require users to log back into system

Remote Access
- ❑ Remote access restricted to recognized devices over TLS connections in VPN tunnels using multi-factor authentication traveling through managed access points
- ❑ Remote users must consent to same monitoring/auditing as local users
- ❑ Remote access must be appropriately authorized and travel through managed access control points
- ❑ Authorizes remote administration and monitoring of corporate devices and data
- ❑ Remotely accessed CUI must remain on managed devices

Wireless/Mobile Access
- ❑ Wireless access restricted to authorized users on specific devices using WPA2 encryption
- ❑ Mobile devices must use whole-device encryption mechanisms

External Systems
- ❑ External system access limited to read-only devices; exceptions require senior management approval
- ❑ Data exfiltration will occur through specified transaction types (company specific)

CYBER FORWARD™

Security Awareness and Training Policy

Note: Cyber Forward is responsible for all training material content.

Security Awareness Training

- ❑ All personnel will receive basic security awareness training as part of initial training and recurring annually thereafter.
- ❑ All personnel will be made aware of organizational cyber security policies.
- ❑ Topics include:
  - ☑ CUI identification & individual responsibilities
  - ☑ Insider Threat—how to recognize
  - ☑ Incident Response—how to recognize & who to call
  - ☑ Continuity of Operations—where to save files
  - ☑ Attack vectors (Social Engineering, Phishing, Malware, etc.)
  - ☑ Media Use (e.g. paragraph markings, storage, transportation & sanitation procedures)
  - ☑ Password complexity requirements
  - ☑ Multi-Factor Authentication Basics
  - ☑ Safe web surfing tips
  - ☑ Encryption Basics

Administrator Role-Based Security Training

- ❑ Focuses on procedures required to implement cyber security policies.
- ❑ Topics Include:
  - ☑ CUI Responsibilities
  - ☑ Insider Threat—measures to mitigate
  - ☑ Incident Response—what to do
  - ☑ Continuity of Operations—what to do
  - ☑ Configuration Management procedures
  - ☑ Network Monitoring Procedures
  - ☑ Digital Media sanitation procedures—reformatting media, etc.

Manager Role-Based Security Training

- ❑ Emphasizes senior leader cyber security considerations.
- ❑ Topics Include:
  - ☑ Employee authorizations requiring their approval
  - ☑ Insider threat detection
  - ☑ Incident Response considerations
  - ☑ Risk Management considerations
  - ☑ Audit report considerations
  - ☑ Patch management considerations
  - ☑ System Security Plan
  - ☑ Risk Assessment
  - ☑ Continuity of Operations—management
  - ☑ Supply Chain

Incident Response Personnel Role-Based Security Training

- ❑ Emphasizes individual's role in incident response.
- ❑ Topics Include:
  - ☑ Incident Response plan
  - ☑ Incident Response test plan
  - ☑ Reporting Requirements
  - ☑ Reporting Timelines
  - ☑ Requesting Incident Response assistance