CONNSTEP
a CBIA affiliate

CMMC PREPARATION Webinars: How to Develop & Implement Effective CMMC Policies & Procedures

CONNSTEP
4/6/2023

CMMC PREPARATION Webinars

CONNSTEP
a CBIA affiliate

Four Webinar Series

3/9 – 6/1

12 noon – 1 pm

March 9th	Understanding CMMC Timeline & Steps to Compliance
April 6th	How to Develop & Implement Effective CMMC Policies & Procedures
May 4th	How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance
June 1st	Steps to Take in Preparation for a CMMC Audit

Webinar #2 Agenda

How to Develop & Implement Effective CMMC Policies & Procedures:

- The Importance of Policies and Procedures
- CUI Definition
- Policies & Procedures Scope
- General Recommendations and Tips
- Policies and Procedures Team
- Implementation, Training, and Risk Management
- Success Factors

CONNSTEP
a CBIA affiliate

Presenters:

Anna Mumford
Cybersecurity Consultant

860.305.8880
amumford@connstep.org

Jeffrey Orszak
Director, Business Technology and Innovation

860.539.4905
jorszak@connstep.org

Guidance

Nothing in this presentation (written, spoken, expressed, or implied) is legal advice.

Nothing in this presentation (written, spoken, expressed or implied) should be construed as an endorsement of any solution, product, service, or methodology.

Poll

Policies versus Procedures

Policy	Procedure
General	Specific
WHAT to do	HOW to do it
The Goal	The steps to Execute it
Changes Infrequently	Changes Overtime

Why Policies & Procedures are Important

1. Security Policies and Procedures will protect your business

Human Errors
lead to over 80% of all Security Incidents

Best Defense Method?

Policies
&
Procedures

Why Policies & Procedures are Important

2. Security Policies and Procedures are a critical step in CMMC compliance

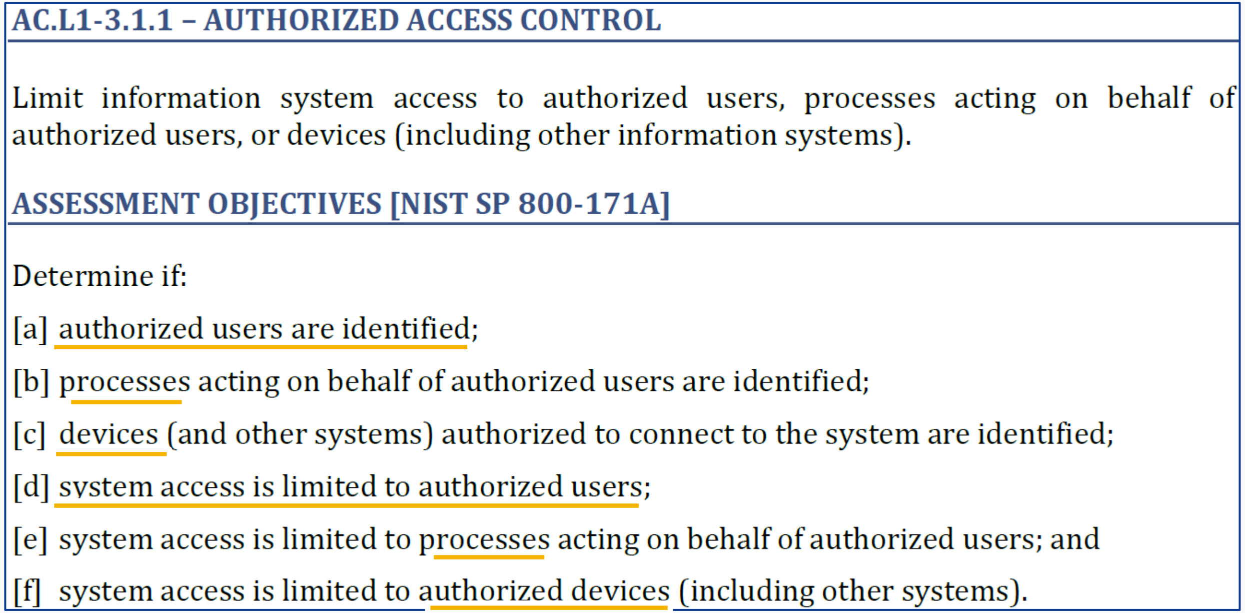
- Need **policies** to enforce the NIST SP 800-171 controls
- Create **procedures** to operationalize the policies

Note: CMMC auditors will examine policies and procedures for evidence of **organizational maturity**

Why Policies & Procedures are Important

3. Implementation of security Policies and Procedures will generate evidence of compliance

From CMMC Level 2 Assessment Guide:



AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Access Control Policy

- list of authorized accounts and the name of the individual associated with each account

- list of devices and systems authorized to connect to organizational systems

Account Management Procedure:

- access authorization records
- notifications or records of recently transferred, separated, or terminated employees
- list of conditions for group and role membership
- list of recently disabled system accounts along with the name of the individual associated with each account
- account management compliance reviews (system monitoring records; system audit logs and records)

Policy Standard Format

No required format

However, there are adopted policy standards:

Purpose:

Scope:

Policy:

Responsible Role:

Procedure:

Revision History:

CUI and CDI

Controlled Unclassified Information (CUI)

Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended

Covered Defense Information (CDI)

Unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DOD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract;

AND…

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) Critical information

(iii) Export control

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information)

Distribution Statements on Technical Documents

Example of Marking for Distribution Statement D

Distribution authorized to Department of Defense and U.S. DoD contractors only; Proprietary Information; 15 Apr 2017. Other requests for this document shall be referred to AFRL/VSSE, 3550 Aberdeen Ave. SE, Kirtland AFB, NM 87117-5776. REL TO UK

Example of Marking for Export Control Warning

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.2

CUI Resources

CUI TRAINING:

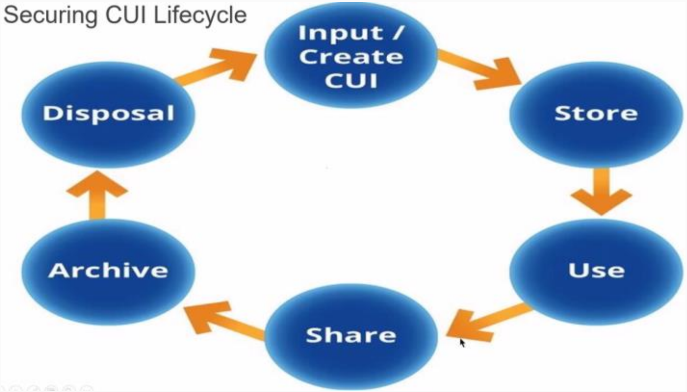
- **CUI Training.** Cover how to designate CUI, CUI categories and subcategories, the CUI registry, markings, as well as how to appropriately safeguard, disseminate, and decontrol CUI.
- Free training that satisfies this requirement is offered by the government at DoD Mandatory Controlled Unclassified Information (CUI) Training (usalearning.gov)

- **CUI Marking**
  - https://dtcglobal.us/blog/f/nist-800-171-marking-and-labeling-cui
  - https://www.archives.gov/files/cui/documents/marking-introduction-20170906.pdf
  - https://www.dodcui.mil/Portals/109/Documents/Desktop%20Aid%20Docs/20-S-2093%20cleared%20training%20guide-13_oct-20.pdf

Scope for CMMC Policy Requirements

The **SCOPE** of Policies & Procedures:

- Any asset that provides security or stores, transmits, or processes CUI
- Includes:
  - ✓ People
  - ✓ Information Technology
  - ✓ Operations Technology
  - ✓ Physical Security



- ➢ Map CUI flow throughout the organization
- ➢ Consider CUI data lifecycle

Implement ***Company-wide*** *Cybersecurity Policies & Procedures*

Other Compliance & Security Demands:

What to protect?

- CUI
- Intellectual Property (IP)
- Financial Data
- Critical and Sensitive Operations Information
- Personally Identifiable Information (PII)
- Customer Proprietary Information (as specified by state legislation, such as CCPA)
- GDPR - General Data Protection Regulation
- PCI - Payment Card Industry Data Security Standard
- Privacy and Personnel Records
- And more…

Actions to Take

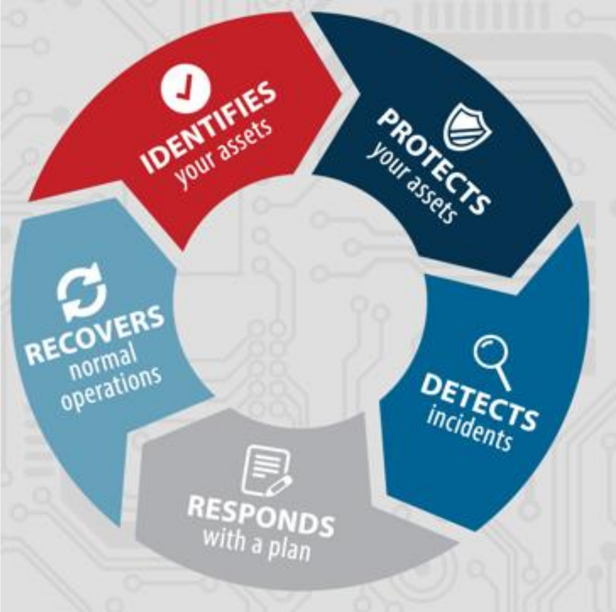
1. Create a **CUI Data Flow Diagram** and review how CUI flows through your organization. [Attach this to your System Security Plan!]
2. Attend DOD CUI training
3. Acquire Policies and Procedures template
4. Identify the scope of your company's Policies and Procedures

Three Foundational Principles – Include in Policy

CONNSTEP
a CBIA affiliate

Three foundational principles in the Framework and NIST 800-171 requirements:

- Least Functionality
- Separation of Duties
- Unique Traceability



General Recommendations

Policies and Procedures tips:

- Always include: who requests, who approves, who executes and if relevant, who reports

  'Who" = role: design based on ***role***, not on an individual.

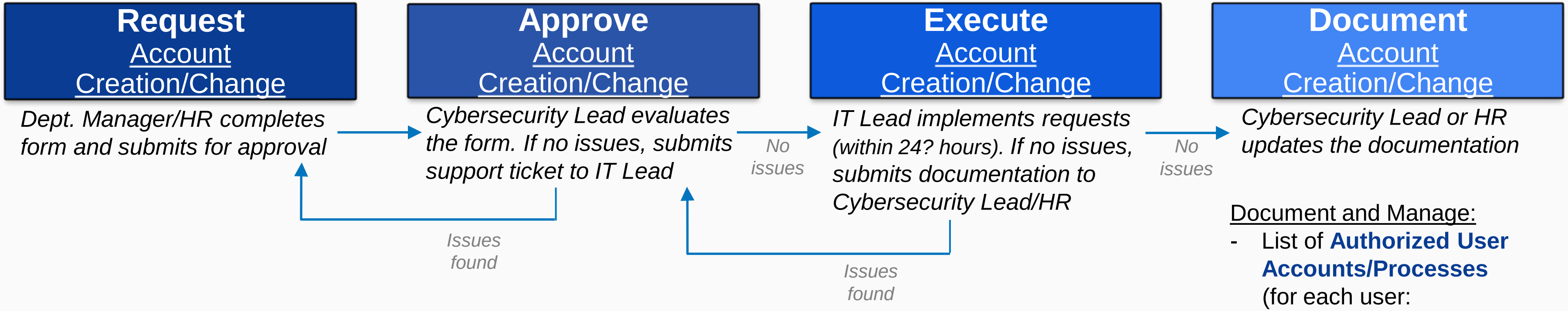
- Include timing and iterations:

ex: Password must be changed every 30 days and cannot be reused for 5 generations.

- Include required documentation (visitor log, system inventory, etc.)
- Identify "Acceptable Use Policies" and necessary employee training
- Include Version Control/Revision section – and keep current
- Review and update periodically.

Example of Account Creation/Role Change Procedure

Process Owner: ___________



Request Account Creation/Change

Dept. Manager/HR completes form and submits for approval

Approve Account Creation/Change

Cybersecurity Lead evaluates the form. If no issues, submits support ticket to IT Lead

Execute Account Creation/Change

IT Lead implements requests (within 24? hours). If no issues, submits documentation to Cybersecurity Lead/HR

Document Account Creation/Change

Cybersecurity Lead or HR updates the documentation

Document and Manage:

- List of **Authorized User Accounts/Processes** (for each user:
  - hire date/role change,
  - user role, acct type, approved devices, approver/date)
- List of **Authorized Devices (inventory)**
  - (device type and detail, assigned user)
- **Account Creation/Change Form**

Account Creation/Change Form:
Identify: **User Acct/Device/Process**
-hire date
-end date (vendor, temp contractor)
User **Role**: (based on the type of work performed)
Assigning approved **devices**:

Before you start: Team Roles & Responsibilities

Decide on your **cybersecurity team roles and responsibilities**:

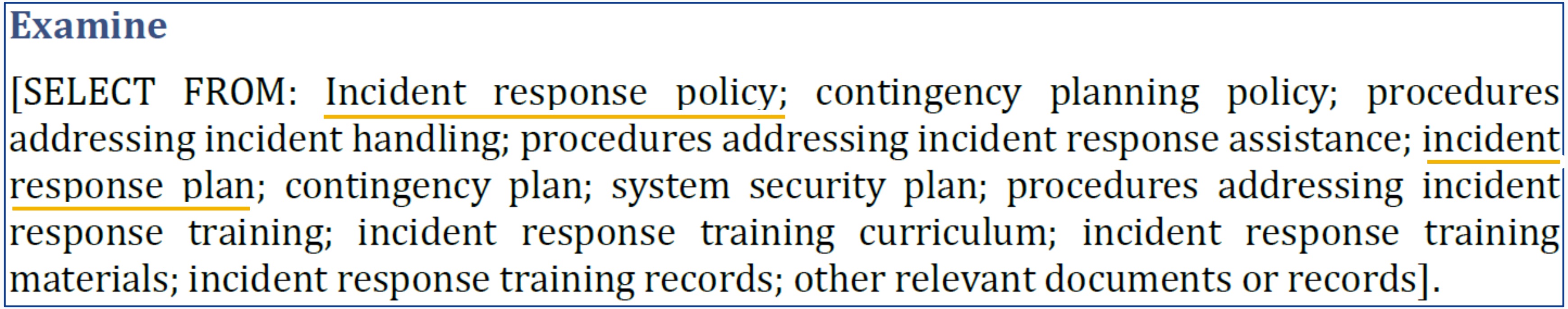
- Create a roles & responsibilities matrix outlining duties
- Think of who would be requesting and who would be authorized to approve system access and system changes
- Include MSP roles if all or some IT functions are outsourced

Incident Response - EXAMPLE

NIST SP 800-171 3.6.1: Establish an **operational incident-handling capability** for organizational information systems that includes adequate **preparation**, **detection analysis**, **containment**, **recovery** and **user response** activities

This includes creating
an Incident Response **POLICY** as well as a **PLAN**

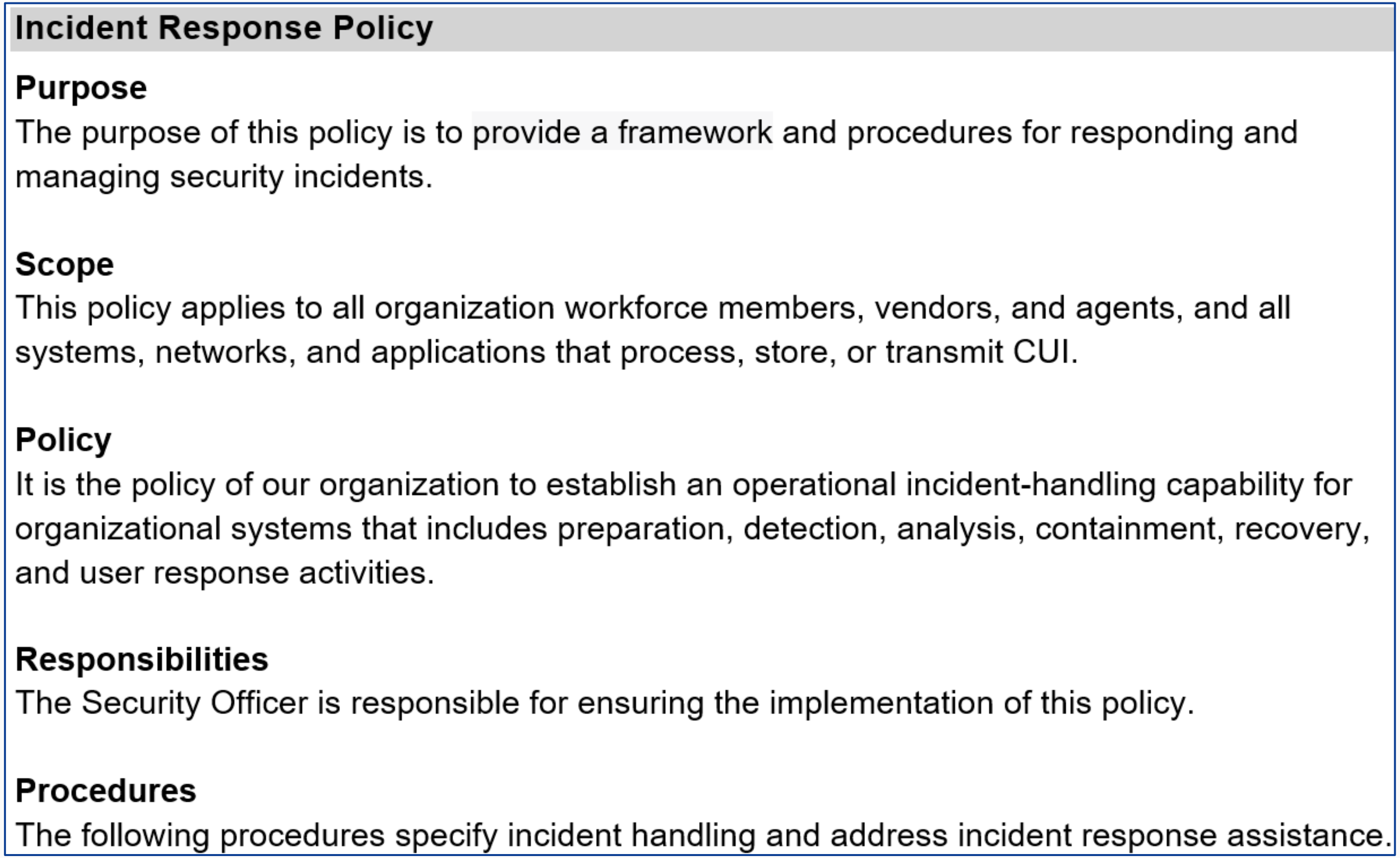
From CMMC Level 2 Assessment Guide:



Examine

[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records].

Incident Response POLICY (example)



Incident Response Policy

Purpose
The purpose of this policy is to provide a framework and procedures for responding and managing security incidents.

Scope
This policy applies to all organization workforce members, vendors, and agents, and all systems, networks, and applications that process, store, or transmit CUI.

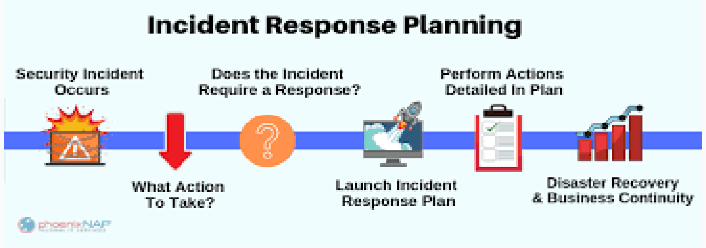
Policy
It is the policy of our organization to establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Procedures
The following procedures specify incident handling and address incident response assistance.

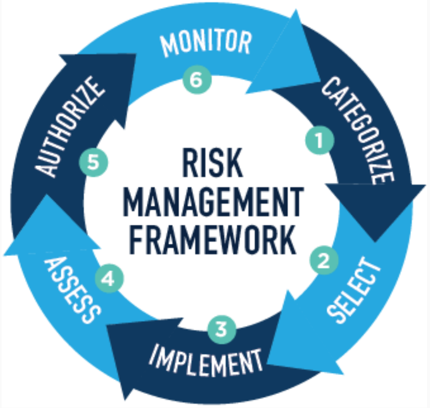
Incident Response PLAN

- **Procedures** for incident handling and reporting
    - Preparation: create internal capability to handle security incidents (team, process)
    - Detection analysis (incident classification and severity)
    - Containment
    - Recovery
    - Post Incident Activities
- **Communication** within organization and outside stakeholders about the incident & status
- **Incident Response Team** roles and responsibilities
- **Incident Reporting**


Incident Response Planning
Security Incident Occurs
What Action To Take?
Does the Incident Require a Response?
Launch Incident Response Plan
Perform Actions Detailed In Plan
Disaster Recovery & Business Continuity
phoenixNAP

Risk Management Process

Cybersecurity = Managing the Risks to your Organization



1. Identify and categorize critical assets
2. CONTINUALLY assess, analyze, prioritize, improve, authorize, and monitor the risks

Results:

- Improving the confidence of security controls effectiveness
- maintaining policies and procedures

Actions to Take

1. Decide on your cybersecurity roles and responsibilities and assign individuals to each role
2. Develop Incident Response Plan and create inter-departmental Incident Response Team
3. Integrate cybersecurity into your periodic management review

P&P Implementation Phases

- Develop
- Document
- Implement
- Train
- Monitor
- Manage Risk
- Maintain

IMPLEMENT Policies & Procedures

Human Errors lead to over 80% of overall security incidents

-> Policies and Procedures are a crucial protection method for minimizing the human factor

- <u>Technical vs Acceptable Use Policies</u>

Issue-specific type of policies that all employees need to comply with (rules, procedures, and guidelines for the company’s employees to comply with).

- <u>Common pitfalls of implementing P&P</u>:

- insufficient employee training
- compensating through investment in strong technology
- ineffective change management

TRAIN, MONITOR, and MANAGE RISK

Perform effective training on the Acceptable Use Policies

Monitor and manage risk areas

- understand human behavior that expose the company to security threats
- develop risk profile and build mitigation capability
- Understand, track, and manage risks

Implement effective change management:

- **Create a sense of urgency**
- **Communicate cybersecurity strategy**
- **Enlist a volunteer army**
- **Enable action by removing barriers**
- **Generate short-term wins**
- **Sustain acceleration**
- **Institute change**

Implementing Culture of Change Management

- Create an environment of employee engagement and collaboration where everyone is informed, has an important part to play, and is actively engaged in managing the company’s risks
- Leadership team needs to go through a cultural and philosophical change to effect such changes throughout the whole company

MAINTAIN Policies & Procedures

Maintain the procedures

- Over time employees may start to bend the rules in favor of productivity, convenience, or lack of non-compliance consequences

- Maintenance tactics
  - emphasize to employees the risks of non-compliance
  - ask for commitment to the rules through a signature
  - Revise and improve procedures to increase compliance
  - post policies in easily accessible areas for reference
  - affirm policies understanding with annual training

Implementation Techniques

Compliance implementation techniques:

Not Effective:

- penalties or punishments for non-compliance,
- being unclear in policies objectives and approach,
- creating policies that do not appeal to employee's unique characteristics

Effective, proven to promote employee policies compliance:

- training that builds employee with skills and confidence to combat threats,
- employee guidance on suspicious threat response and reporting,
- providing understanding how compliance benefits the entire company,
- hiring employees with a positive attitude towards cybersecurity, and
- supporting organization's commitment to security

Success Factors

1. Don't get it right: get it written! You don't have to get it 100% perfect and complete. Just make a start...

2. Use Risk Management Framework

3. Periodically review and continually improve:
   - Annual gap assessment – improving confidentiality
   - After a security incident – after action activities
   - After annual employee training – P&P
   - As needed

4. Management commitment and engagement

Actions to Take

After P&P documentation is competed

1. Train employees
2. Monitor effectiveness
3. Continually improve

State Funding Available

State funding is available for

Connecticut Manufacturing SIRI and CYBER Assistance Program (SAC)

for manufacturing companies or allied service providers located in Connecticut.

The SAC Program is Funded by:

The Connecticut Department of Economic and Community Development

"Strengthening Connecticut's Competitive Position"

Connecticut

Department of Economic and
Community Development

https://ctsac.ccat.us/

CONNSTEP
a CBIA affiliate

Questions?

CONNSTEP
350 Church St., Hartford, CT 06103 | 800.266.6672
CBIA & Affiliates | cbia.com | connstep.org | readyct.org

PART OF THE MEP National Network™

Connecticut Department of Economic and Community Development

Glossary

CMMC – Cybersecurity Maturity Model Certification

CUI - Controlled Unclassified Information

DFARS - Defense Federal Acquisition Regulation Supplement

DIB – Defense Industrial Base

DIBCAC – Defense Industrial Base Cybersecurity Assessment Center

DCMA – Defense Contract Management Agency

IRP – Incident Response Plan

IT – Information Technology

MEP - Hollings Manufacturing Extension Partnership

MSP – Managed Service Provider

MSSP – Managed Security Service Provider

NIST – National Institute of Standards and Technology

NIST SP 800-171 – NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

POAM – Plan of Action and Milestones

SPRS – Supplier Performance Risk System

SSP – System Security Plan