Cybersecurity Policies

May 2021

Cybersecurity Policies

CIAS-ISA
COMMUNITY CYBERSECURITY PROGRAMS

This webinar was developed by
the Center for Infrastructure Assurance and Security
at the University of Texas at San Antonio

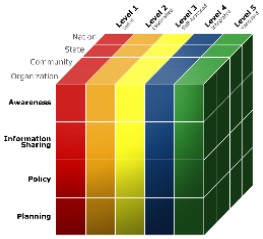
The CIAS has been working with communities to improve their cybersecurity posture since 2002.

Core competencies include cybersecurity training, exercises, competitions, game development, culture of security initiatives, information sharing and cybersecurity community programs.

UTSA

About the CIAS-ISAO

- An initiative of the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio
- Focus Areas: Outreach & Grassroots Security
  - Cybersecurity Professional Training & Exercises
  - Cyber Competition Programs
  - Cybersecurity Educational Games
  - Culture of Cybersecurity
  - Information Sharing and Analysis Initiatives
  - National Cybersecurity Preparedness Consortium (NCPC)



Membership Resources

- Educational Content
- Quick Access to National Resources
- Access to Customized Training
- Recorded Webinars
- Discount on Cybersecurity Prep Courses & Workshops
- Roadmap to Establishing an ISAO
- Assessments
- Your CIAS-ISAO Support Team!

Membership Benefits (Levels 2 & 3)

- **Discount on CIAS Prep Courses**: CISSP, CompTIA A+, CompTIA Security+
- Access to **Customized Training** Resources
- Customized **Consultations**
- **Discount on book** "Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)"
- **Discount on Panoply**, a virtual cyber defense event
- Personalized **Roadmap** to Establishing an ISAO

Upcoming Events

CIAS-ISAO Webinars:

- Look for new webinars
- Let us know what you need

Instructor-Led (Virtual) Courses:

- CompTIA A+: September 4, 2021
- $(ISC)^2$ CISSP: July 31, 2021
- CompTIA Security+: Coming Summer/Fall 2021

How to Develop Effective Cybersecurity Policies

Natalie Sjelin
Director of Training
CIAS-ISAO

Agenda

- Developing effective policies
- Overcome implementation challenges
- Critical cybersecurity policies
- When you should review, update and add new policies

Cybersecurity Policies

Organizations are exposed to new cybersecurity risks every day. Cyberattacks and data breaches impact all organizations, large and small, which means you want to make sure everyone associated with your business understands their role in protecting the organization's IT assets, sensitive information, and reputation.

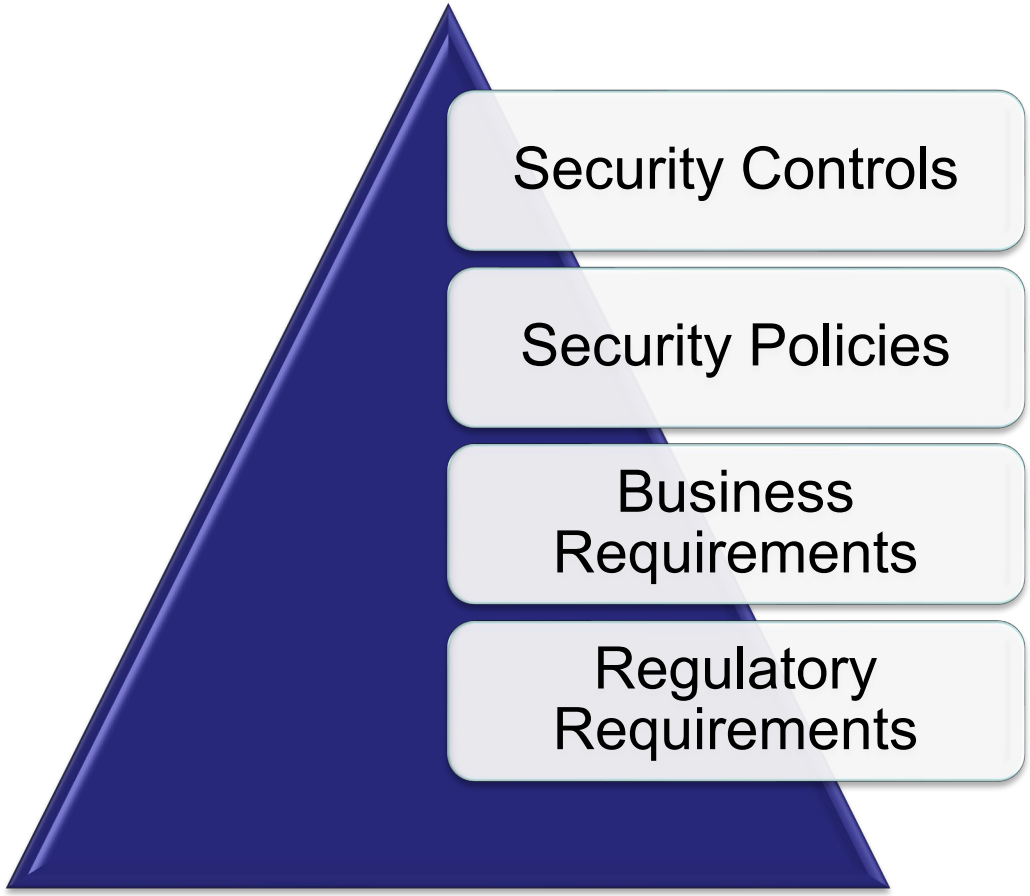
Cybersecurity policies explain how employees, consultants, partners, board members and other end-users can assist in defending the organization from cyber incidents.

Role of Policy

The role of policy is to:

- Categorize guiding principles
- Shape behavior
- Provide guidance for future decisions
- Ensures compliance with legal and regulatory requirements
- Serve as an implementation roadmap

Relationship Between Security Controls and Policy



Policy Development

Six Key Tasks

- Planning
- Research
- Writing
- Vetting
- Approving
- Authorizing

Successful policies include representatives of those who must comply with and enforce the policy.

Development Tasks

- **Planning**
  - Identify the need for the policy
- **Research**
  - Ensures all laws, obligations, and customs have been taken into consideration.
- **Writing**
  - Identify the target audience for the policy
  - Use language they will understand

Development Tasks

- **Vetting**
  - Ensures the policy has properly been scrutinized
  - Examples of those who may wish to engage
    - Legal counsel
    - Human resources
    - Compliance personnel
    - Cybersecurity and technology professionals
    - Auditors and regulators
    - Employees that will be required to follow the policy
    - Contractors and partners required to follow the policy

Development Tasks

- **Approving**
  - Building support and acceptance to all affected departments and employees
- **Authorizing**
  - Process for executive management to agree and approve the policy
  - Certain regulations require cybersecurity policies to be written and approved

Policy Design Structure

- Title
- Introduction
- Goals/Objectives
- Scope
- Standards
- Procedures
- Guidelines
- Exceptions
- Enforcement

Policy Title

- Reflects what the policy is
- The more specific the better
- Makes the policy easy to find

Policy Introduction

- Frames the document
- Reflects the core values of the organization
- Identify regulatory and contractual obligations

Policy Goals and Objectives

- Conveys the intent of the policy
  - ❑ Demonstrate our commitment to information security
  - ❑ Define organizational roles and responsibilities
  - ❑ Provide the framework for effective risk management and continuous assessment
  - ❑ Meet regulatory requirements
- Aligns with the organization's goals for security or compliance

Policy Scope

- Defines what elements are covered in the policy
  - ✓ IT assets
  - ✓ Organization-owned assets
  - ✓ Whom it covers

Policy Standards

- Identifies standards that all users must comply with:
  - ✓ Hardware
  - ✓ Software
  - ✓ Configuration
- Explain the relationship of this policy with these standards
- Could include both technical and user requirements

Policy Procedures and Guidelines

- **Procedures**
  - Explain how you intend to implement and deliver the policy to all those who must follow the policy
- **Guidelines**
  - Explain the roadblocks or implementation issues that must be addressed
  - Describe how you intend to overcome them

Policy Exceptions and Enforcement

- **Exceptions**
  - Identify the waiver process to request deviations or exceptions to the policy
- **Enforcement**
  - Explain what can happen if the policy is not followed

❖ **Policy enforcement is critical**

Implementation Challenges

- Weak strategy
- Ineffective training
- Lack of resources
- Lack of communication
- Lack of follow through

Implementation Strategies

- Effective communication is one of the most important best practices
- Clearly communicate the expected results of the investment in security policies
- Obtain executive support early
- Keep expectations realistic
- Keep security policies flexible

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Acceptable Use Policy**
  - Addresses the constraints and practices that a user must agree to access the corporate network or the internet.
- **Incident Response Policy**
  - The policy should include information about the incident response team, personnel responsible for testing to the policy, the role of each team member, and actions, means, and resources used to identify and recover compromised data.

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Network Security Policy**
  - Ensures the confidentiality, integrity, and availability of data on company's systems.
  - Ensures systems have appropriate hardware, software, or procedural auditing mechanisms.
  - Requires logging items include anomalies in the firewalls, activity over routers and switches, and devices added or removed from the network.
  - State applicable actions taken during an auditable event and who is responsible for what

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Password Policy**
  - Provides guidance on developing, implementing, and reviewing a documented process for appropriately creating, changing, and safeguarding strong and secure passwords used to verify user identities and obtain access for company systems or information.

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Remote Access Policy**
  - The remote access policy is designed to minimize potential exposure from damages that may result from unauthorized use of resources.
  - Directed to all employees and should include provisions for sending or receiving emails and intranet resources.
  - Include requirements for VPN access and disk encryption.

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Security Awareness and Training**
  - Goals should include education about the security policy and help develop an understanding on how the policy protects the business, employees, and customers.
  - Should be administered to all workforce members, so they can properly carry out their functions while appropriately safeguarding company information.
  - Highlight personnel that are responsible for creating and maintaining the training.

Cybersecurity Policies Needed

Based on your organizations security controls and security needs

- **Also consider these topic areas:**
  - Mobile Device Security
  - Data Backup
  - Personnel Security
  - Physical Security
  - Records Retention
  - Confidential Data
  - Disaster recovery
  - Software
  - Technology disposal
  - Vendor Management

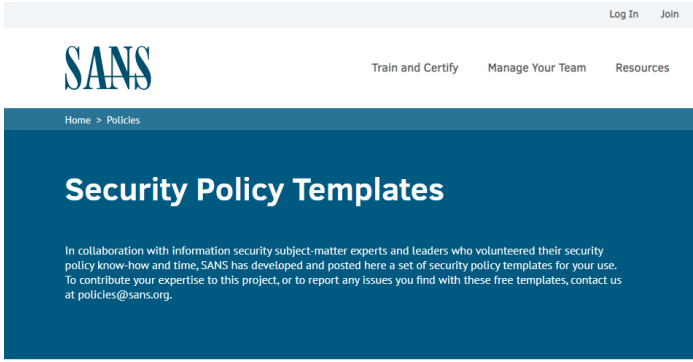
When to Review, Update and Add Policies

- Adapting new technologies
- Cybersecurity incident
- Operational and workforce changes
- Changes in compliance, legal requirements and contracts
- Annual review

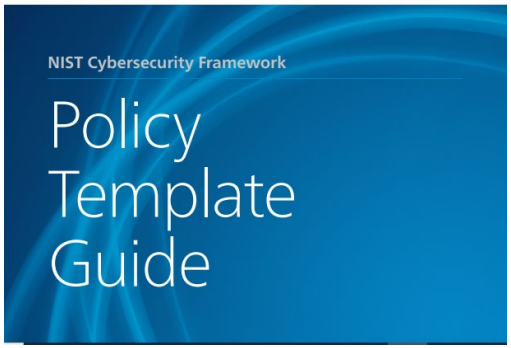
Policy Templates

Policy Templates – Don't recreate the wheel!

- SANS
  - 50 security templates
  - Various common security topics
- NIST
  - Templates are organized around
    - Identify, Protect, Detect, Respond, Recover
- CIAS-ISAO
  - Cybersecurity templates repository
  - Customization available to Level II and III Membership



https://www.sans.org/information-security-policy/



NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf

How to Suck At Security Policies

- Create a security policy just to mark a checkbox
- Assume that if the policies worked for you last year, they'll be valid for the next year

Cheat sheet of common mistakes, so you can avoid them!

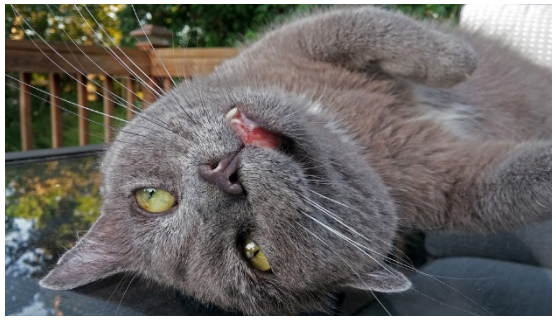
Lenny Zeltser with contributions from SANS Internet Storm Center handlers.

How to Suck At Security Policies

- Create security policies you cannot enforce
- Assume that policies don't apply to executives
- Use security templates without customizing them.

Cheat sheet of common mistakes, so you can avoid them!

Lenny Zeltser with contributions from SANS Internet Storm Center handlers.



How to Suck At Security Policies

- Assume the users will read the security policy because you've asked them to

Cheat sheet of common mistakes, so you can avoid them!

Lenny Zeltser with contributions from SANS Internet Storm Center handlers.

Thank you!

In addition to today's webinar, we can help you with:

- Training & Exercises
- Implementing a Culture of Cybersecurity & K-12 Educational Cybersecurity Program
- Customized Cybersecurity Competitions
- Assessments
- Access to Educational Content
- ISAO Support for Communities
- Establishing and Growing a Program (CCSMM)

Questions?

Natalie Sjelin
Director of Training
Natalie.Sjelin@utsa.edu

Julina Macy
Director of Communications
Julina.Macy@utsa.edu

CIASISAO.org