CYBERATOS
SMART STRATEGY
STRONG SECURITY

How to Develop a Cybersecurity Policy:

A practical Guide for CISOs and ISOs

Learn More

cyberatos.com

HOW TO DEVELOP A CYBERSECURITY POLICY:

A PRACTICAL GUIDE FOR CISOs AND INFORMATION SECURITY OFFICERS (ISOs).

INTRODUCTION

In the modern digital age, the security of an organization's information assets is paramount. Cyber threats are constantly evolving, demanding a proactive and structured approach to safeguarding sensitive data and maintaining operational integrity. At the heart of this approach lies a set of well-defined and rigorously enforced cybersecurity policies. For Chief Information Security Officers (CISOs) and IT leaders, the responsibility of crafting these policies is not merely a task, but a strategic imperative.

This guide, developed by ***Cyberatos***®, is designed to serve as a comprehensive roadmap for developing and implementing robust cybersecurity policies. It transcends the mere compilation of rules, focusing on creating a dynamic framework that aligns with organizational goals, complies with regulatory mandates, and fosters a culture of security awareness. We will navigate through the essential steps, from understanding your unique organizational landscape to establishing a solid policy framework, ensuring alignment with industry standards, and implementing effective enforcement mechanisms. By following these guidelines, you will be equipped to build a formidable defense against evolving cyber threats, ensuring the resilience and security of your organization's digital ecosystem.

STRUCTURE OF THE ORGANIZATIONAL CYBERSECURITY POLICY FRAMEWORK

When developing cybersecurity policies, organizations often ask whether to create a single, overarching security policy with all other topic-specific policies underneath it, or to maintain multiple separate policies of equal standing. Best practices and standards strongly favor a hierarchical policy framework. In this model, a high-level master cybersecurity (or information security) policy sets the overall direction and principles, and it is supported by a suite of subordinate policies addressing specific domains (e.g. access control, data protection, incident response).

Organizations are advised to establish a **tiered policy structure**. At the top, define a single overarching **Cybersecurity or Information Security Policy** approved by senior management. This high-level policy should set the tone and direction: e.g. affirm leadership's commitment to security, outline the security objectives and principles (like confidentiality, integrity, availability), describe the scope (which assets and data are covered), and assign high-level responsibilities for security governance.

Under this umbrella, develop a **suite of focused policies** for key domains of cybersecurity. Each domain policy should address a specific area such as access control, data protection, network security, incident response, acceptable use, vendor/third-party security, etc., with enough detail to guide that aspect of operations. These subordinate policies are effectively **components of the overall security program**. They should be consistent with the overarching policy's principles and with each other, but they spell out requirements in their domain (for instance, an Incident Response Policy will align with the overall goal of resiliency stated in the master policy, while providing the detailed mandate to maintain incident handling procedures). This approach mirrors the requirement in ISO 27001 to have "topic-specific policies" alongside the main policy and reflects NIST's concept of issue-specific policies under a program policy.

Example: Consider an enterprise that sets an overarching Information Security Policy stating that the company *"will protect information assets commensurate with risk and in compliance with laws, assigning appropriate roles to enforce security."* This high-level policy references more detailed policies for enforcement. Under it, an **Access Control Policy** mandates user authentication, unique IDs and least privilege for systems (mapping to ISO/NIST access control controls).

A **Data Protection Policy** covers data classification, encryption, and handling of personal data (mapping to privacy regulations and encryption controls). An **Incident Response Policy** requires maintaining incident handling procedures and defines incident severity levels and reporting timelines (mapping to NIST's respond/recover functions).

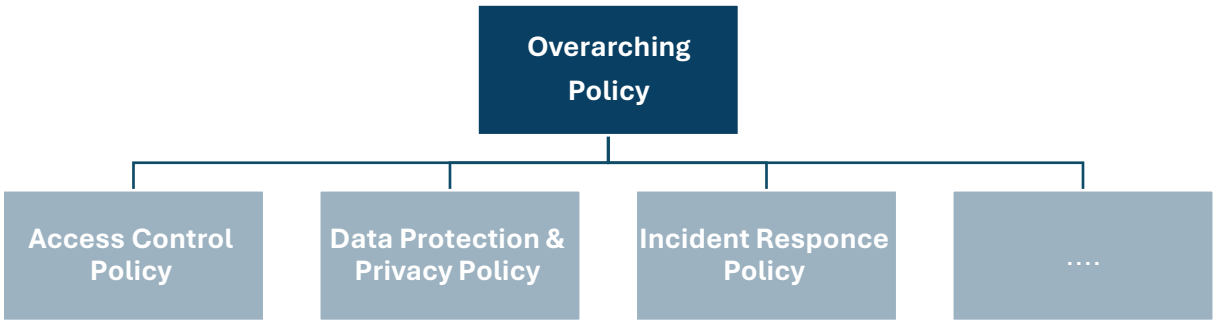
All these policies are separate documents on equal tier with each other (each approved by management and published to staff), but all are subordinate to the principles of the master policy. In day-to-day operation, this means each team knows where to look: if there's a security incident, staff follow the Incident Response Policy procedures, while understanding that this fulfills the organization's overall commitment to resiliency as stated in the top policy. If a new threat arises (say a new malware), the Incident Response Procedure can be updated quickly (no board approval needed, since it's a lower-level document referenced by the policy), and the Incident Response Policy might be reviewed annually by the security committee for effectiveness.

Throughout, the **governance chain** is intact – the board sees and approves the top-level policy and is confident that subordinate policies exist to implement it, and those subordinate policies are regularly maintained by security management. This hierarchical setup thereby provides both **strategic oversight and operational agility**.

Begin with a clearly structured policy hierarchy to organize cybersecurity policies effectively. Start with an overarching **Information Security Policy**, which defines the organization's high-level security objectives, responsibilities, and core principles. Beneath this overarching policy, establish domain-specific subordinate policies addressing various security aspects, such as:

- Access Control Policy
- Data Protection and Privacy Policy
- Acceptable Use Policy
- Incident Response Policy
- Network Security Policy
- Mobile Device and Remote Work Policy

All subordinate policies should align with and support the overarching policy.



Structure of the Organization's Cybersecurity Polices Framework

STEPS TO DEVELOP CYBERSECURITY POLICIES

1. Understand Your Organization's Unique Landscape:

Before you begin writing, a deep understanding of your organization is essential.

- **Risk Assessment:**
    - Conduct a comprehensive risk assessment to identify:
        - Critical assets (data, systems, facilities)
        - Potential threats (internal and external)
        - Vulnerabilities (weaknesses in systems or processes)
        - Impact of potential breaches (financial, reputational, legal)
    - Use risk assessment outcomes to inform policy decisions and ensure each policy addresses realistic, prioritized risks effectively
    - Use frameworks like NIST Risk Management Framework (RMF) or ISO 27005 for guidance.
- **Regulatory Compliance:**

- Identify all applicable legal and regulatory requirements:
    - Industry-specific regulations (e.g., HIPAA for healthcare, PCI DSS for payment card industry, CSF-CBJ for Banking in Jordan, NCA-ECC for entities in KSA). Also other sectors, such as Electricity and Aviation, need to comply with respective national and international regulations.
    - Data privacy laws (e.g., GDPR, CCPA, Jordan's PDPL)
    - National and international laws (e.g., Cybersecurity Law in Jordan)
- Ensure policies are designed to meet or exceed these requirements.
- Adhering to these frameworks strengthens your organization's security posture and compliance position.

- **Business Objectives:**
    - Align cybersecurity policies with the organization's strategic goals:
        - Support business operations and innovation
        - Protect business continuity
        - Maintain customer trust
    - Avoid policies that hinder legitimate business activities.
- **Organizational Culture:**
    - Consider the organization's culture and communication style:
        - Tailor language and tone for employee understanding
        - Promote security awareness and buy-in
        - Address potential resistance to change

2. Establish Policy Framework and Structure:

A well-defined framework is crucial for organization and maintainability.

- **Policy Hierarchy:**
    - Implement a hierarchical structure:
        - **Overarching Cybersecurity Policy:**
            - High-level principles and objectives
            - Governance and responsibilities
            - Enforcement and compliance
        - **Specific Policies:**

        - Detailed rules and requirements for specific areas
        - Examples: Access Control Policy, Data Protection Policy, Incident Response Policy
    - **Procedures and Guidelines:**
        - Support policies with detailed operational documents such as procedures, guidelines, and technical standards. These documents guide practical implementation and reinforce the policies' applicability to daily operations. They represent step-by-step instructions for implementing policies.
        - Examples: Password Reset Procedure, Data Backup Procedure

- **Policy Template:**
    - Develop a consistent template for all policies:
        - Policy Name and Number
        - Version and Revision Date
        - Purpose and Scope
        - Definitions
        - Roles and Responsibilities
        - Policy Statements
        - Compliance and Enforcement
        - Exceptions
        - Review Cycle

3. Map to Industry Standards and Regulations:

Leverage established standards for best practices.

- **Industry Standards:**
    - Incorporate relevant standards:
        - NIST Cybersecurity Framework: Provides a comprehensive framework for managing cybersecurity risk.
        - ISO 27001/27002: International standards for information security management systems (ISMS).
        - CIS Benchmarks: Configuration security guidelines for various systems.

- **Regulatory Requirements:**
    - Map policy requirements to specific regulatory obligations:
        - Document how each policy statement helps achieve compliance.
        - Maintain up-to-date knowledge of regulatory changes.

4. Craft Clear and Actionable Policy Statements:

Policy statements must be unambiguous and enforceable.

- **Use Clear Language:**
    - Avoid jargon and technical terms.
    - Use simple, direct sentences.
    - Define acronyms and abbreviations.
- **Be Specific:**
    - Provide concrete instructions.
    - Specify actions that are required or prohibited.
    - Include measurable criteria where possible.
- **Define Responsibilities:**
    - Clearly assign roles and responsibilities to individuals or groups.
    - Use job titles or functional roles rather than names.
- **Provide Examples:**
    - Use real-world examples to illustrate policy statements.
    - Show "good" and "bad" practices.
- **Prioritize Key Areas:**
    - Address critical areas based on risk assessment and compliance needs:
        - Access Control Policy
        - Data Protection Policy
        - Incident Response Policy
        - Password Policy
        - Mobile Device Security Policy
        - Email and Internet Usage Policy
        - Software and Hardware Management Policy

        - Acceptable Use Policy

5. Ensure Policy Enforcement and Compliance:

Policies are ineffective without proper enforcement.

- **Communication and Training:**
    - Communicate policies effectively to all employees:
        - Multiple channels (email, intranet, presentations)
        - Tailored communication for different roles
        - Regular security awareness training
    - Provide training on specific policy requirements.
- **Monitoring and Auditing:**
    - Implement mechanisms to monitor compliance:
        - Automated tools (e.g., security information and event management - SIEM)
        - Regular audits of systems and processes
    - Document audit findings and track remediation efforts.
- **Disciplinary Actions:**
    - Define clear consequences for policy violations:
        - Escalating levels of disciplinary action
        - Consistent application of penalties
        - Legal review of disciplinary procedures
- **Enforcement Technology:**
    - Leverage technology to enforce policies where possible:
        - Access control systems
        - Data loss prevention (DLP) tools
        - Endpoint detection and response (EDR)

6. The Policy Development Lifecycle:

Manage policies as living documents.

- **Gather Information:**
    - Collect input from stakeholders:

        - IT staff
        - Legal counsel
        - Human resources
        - Business units
    - Review existing policies and documentation.
- **Draft the Policy:**
    - Write the initial draft using the policy template.
    - Focus on clarity, accuracy, and completeness.
- **Review and Feedback:**
    - Circulate the draft for review and feedback.
    - Incorporate feedback and address concerns.
- **Revise and Finalize:**
    - Make necessary revisions and finalize the document.
    - Obtain legal review if needed.
- **Approval:**
    - Secure formal approval from senior management.
    - Document the approval process.
- **Distribution:**
    - Publish the policy in an accessible location (e.g., intranet).
    - Communicate the policy to all employees.

7. Maintain and Update Policies:

Regular updates are essential.

- **Regular Reviews:**
    - Establish a schedule for reviewing policies (e.g., annually, semi-annually).
    - Review policies more frequently after significant changes or incidents.
- **Change Management:**
    - Implement a formal change management process for policy updates.
    - Document all changes and their rationale.
- **Version Control:**

    - Use version control to track policy revisions.
    - Maintain an archive of previous versions.
- **Incident Response:**
    - Review and update policies based on lessons learned from security incidents.
- **Technology Updates:**
    - Adapt policies to reflect changes in technology and the threat landscape.

CONCLUSION

Developing and implementing effective cybersecurity policies is not a one-time endeavor, but a continuous journey. As we've outlined in this guide, it involves a meticulous process of understanding your organization's unique needs, establishing a robust framework, aligning with industry standards, and ensuring consistent enforcement. However, the work doesn't stop there.

By embracing the principles and steps outlined in this guide, CISOs and IT leaders can build a strong foundation for their organization's cybersecurity posture. This foundation will not only protect valuable assets but also cultivate a culture of security awareness, empowering every employee to play a role in safeguarding the organization's digital future. Remember, cybersecurity is a shared responsibility, and well-crafted policies are the essential tools that enable us to navigate the complexities of the digital age with confidence and resilience.

At Cyberatos, we specialize in assisting organizations with the development and implementation of comprehensive cybersecurity programs, including the creation of robust policy frameworks. Our team provides tailored solutions and ongoing guidance to ensure your organization's security posture remains strong and resilient against evolving threats.

About Cyberatos

Cyberatos is a professional services company that helps organizations in different industries to be ready for the next cyber-attack. We offer many different business services, including cybersecurity Strategy and Policy planning, cybersecurity assessment, cybersecurity GAP recommendations, reports and policy and procedure templates, mentoring with high-level executives, and many more. Do you have a specific need that's not mentioned on our website? Contact us today with your details and we'll match you up with one of our highly trained and experienced professional consultants. If you wish to reach out, please visit us at https://cyberatos.com

Disclaimer:

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.