Direct Costs	Products, Procedures, and Personnel	Allocated Security Control Costs
■ Development or maintenance of security reports ■ Contingency planning and testing ■ Physical and environmental controls for hardware and software ■ Auditing and monitoring ■ Computer security investigations and forensics ■ Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations ■ Privacy impact assessments		

4.2 Security Policy

Recall from Chapter 2 that an information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. It is helpful to distinguish four types of documents before proceeding:

- **Information security strategic plan:** Relates to the long-term goals for maintaining security for assets.
- **Security plan:** Relates to security controls in place and planned to meet strategic security objectives.
- **Security policy:** Relates to the rules and practices that enforce security.
- **Acceptable use policy:** Relates to how users are allowed to use assets.

Table 4.2 provides a more detailed description. All these documents should be approved by a CISO or comparable executive. The CISO may task an individual or a team with document preparation. With these distinctions in mind, this section addresses security policy.

TABLE 4.2 Security-Related Documents

Document Type	Description	Primary Audience
Information security strategic plan	A document used to communicate with the organization the organization's long-term goals with respect to information security, the actions needed to achieve those goals, and all the other critical elements developed during the planning exercise.	C-level executives
Security plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.	C-level executives, security managers, other managers
Security policy	A set of laws, rules, and practices that regulate how an organization manages and protects assets and the rules for distribution of sensitive information. It includes associated responsibilities and the information security principles to be followed by all relevant individuals.	All employees, especially those with some responsibility for an asset or assets
Acceptable use policy	A policy that defines for all parties the ranges of use that are approved for use of information, systems, and services within the organization.	All employees

The purpose of an information security policy is to ensure that all employees in an organization, especially those with responsibility of some sort for one or more assets, understand the security principles in use and their individual security-related responsibilities. Lack of clarity in information security policies can defeat the purpose of the security program and may result in significant losses. An information security policy is the means by which the organization provides management direction and support for information security across the organization. The security policy document defines what is expected from employees and possibly others who have roles in the organization, such as contractors, outside partners or vendors, and visitors.

Security Policy Categories

An organization may choose to use a single security policy document. For larger organizations, this may need to be a lengthy document. It is preferable to have a collection of policy documents so that employees and managers can consult only the relevant documents, as needed. Some of the security policies an organization may adopt include the following [INFO14]:

- **Access control policy:** How information is accessed
- **Contingency planning policy:** How availability of data is provided 24/7

- **Data classification policy:** How data are classified
- **Change control policy:** How changes are made to directories or the file server
- **Wireless policy:** How wireless infrastructure devices need to be configured
- **Incident response policy:** How incidents are reported and investigated
- **Termination of access policy:** How employee access to organization assets is handled during termination
- **Backup policy:** How data is backed up
- **Virus policy:** How virus infections need to be dealt with
- **Retention policy:** How data can be stored
- **Physical access policy:** How access to the physical area is obtained
- **Security awareness policy:** How security awareness is carried out
- **Audit trail policy:** How audit trails are analyzed
- **Firewall policy:** How firewalls are named, configured, and so on
- **Network security policy:** How network systems are secured
- **Encryption policy:** How data are encrypted, the encryption method used, and so on
- **BYOD policy:** What devices an employee may use both on premises and off to access organization assets
- **Cloud computing policy:** Security aspects of using cloud computing resources and service

Ultimately, a CISO and a security manager are responsible for developing these policies. Typically, a security analyst or team of analysts are tasked with the actual formulation of policy documents, which are then approved by higher management.

Security Policy Document Content

Whether a single document or a set of documents, each security policy document should include the following sections:

- **Overview:** Background information on what issue the policy addresses
- **Purpose:** Why the policy was created
- **Scope:** What areas the policy covers
- **Targeted audience:** To whom the policy is applicable

- **Policy:** A complete but concise description of the policy
- **Noncompliance:** Consequences for violating the policy
- **Definitions:** Technical terms used in the document
- **Version:** Version number to keep track of the changes made to the document

A good source of guidance for developing a policy document is the set of policy document templates provided by the SANS Institute. These have been made freely available as a public service. The complete set that is available is shown in Table 4.3.

SANS Institute Information Security Policy Templates https://www.sans.org/security-resources/policies/

TABLE 4.3 Security Policy Templates Provided by the SANS Institute

General	Network Security	Server Security	Application Security
Acceptable Encryption	Acquisition Assessment	Database Credentials	Web Application Security
Acceptable Use	Bluetooth Baseline Requirements	Technology Equipment Disposal	
Clean Desk	Remote Access	Information Logging Standard	
Data Breach Response	Remote Access Tools	Lab Security	
Disaster Recovery Plan	Router and Switch Security	Server Security	
Digital Signature Acceptance	Wireless Communication	Software Installation	
Email	Wireless Communication Standard	Workstation Security	
Ethics			
Pandemic Response Planning			
Password Construction Guidelines			
Password Protection			
Security Response Plan			
End User Encryption Key Protection			

As an example, the following sidebar shows one of the SANS Institute policy templates.

SANS Institute Router and Switch Security Policy

1. **PURPOSE**
   This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <Company Name>.
2. **SCOPE**
   All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.
3. **POLICY**
   Every router must meet the following configuration standards:
   1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
   2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
   3. The following services or features must be disabled: IP directed broadcasts; incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses; TCP small services; UDP small services; all source routing and switching; all web services running on router; cisco discovery protocol on Internet connected interfaces; Telnet, FTP, and HTTP services; Auto-configuration
   4. The following services should be disabled unless a business justification is provided: Cisco discovery protocol and other discovery protocols; dynamic trunking; scripting environments, such as the TCL shell
   5. The following services must be configured: password encryption; NTP configured to a corporate standard source
   6. All routing updates shall be done using secure routing updates.
   7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
   8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
   9. Access control lists for transiting the device are to be added as business needs arise.

10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including: IP access list accounting; device logging; incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped; router console and modem access must be restricted by additional security controls

4. **POLICY COMPLIANCE**

5.1 **Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 **EXCEPTIONS**

Any exception to the policy must be approved by the Infosec team in advance.

5.3 **NON-COMPLIANCE**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Management Guidelines for Security Policies

The SGP provides a useful set of guidelines for the creation, content, and use of security policy documents, which can be categorized as follows:

- **Responsibilities:** Identify the following:
  - Those responsible for ratifying policy document (for example, the board)
  - Responsibilities of all relevant individuals to comply with the policy
  - Individuals responsible for protecting specific assets
  - That all individuals must confirm the understanding of, acceptance of, and compliance with relevant policies and understand that disciplinary action will follow policy violation
- **Principles:** Specify the following:
  - All relevant assets to be identified and classified by value/importance
  - All assets protected with respect to CIA (confidentiality, integrity, and availability) and other security requirements
  - All laws, regulations, and standards complied with
- **Actions:** Specify the following:
  - That all individuals are made aware of the security policy and their responsibilities
  - That all assets are subject to risk assessment periodically and before a major change
  - That all breaches are reported in a systematic fashion
  - That auditing occurs periodically and as needed
  - That policy documents are reviewed regularly and as needed
- **Acceptable use:** Policies that include the following:
  - Documentation of what behaviors are required, acceptable, and prohibited with respect various assets
  - Responsibility for establishing, approving, and monitoring acceptable use policies

Monitoring the Policy

The CISO should designate an individual or a group responsible for monitoring the implementation of the security policy. The responsible entity should periodically

review policies and make any changes needed to reflect changes in the organization's environment, asset suite, or business procedures. A violation-reporting mechanism is needed to encourage employees to report.

4.3 Acceptable Use Policy

An acceptable use policy (AUP) is a type of security policy targeted at all employees who have access to one or more organization assets. It defines what behaviors are acceptable and what behaviors are not acceptable. The policy should be clear and concise, and it should be a condition of employment for each employee to sign a form indicating that he or she has read and understood the policy and agrees to abide by its conditions.

The MessageLabs white paper *Acceptable Use Policies—Why, What, and How* [NAYL09] suggests the following process for developing an AUP:

1. **Conduct a risk assessment to identify areas of concern.** As part of the risk assessment process, identify the elements that need to go into an AUP.
2. **Create the policy.** The policy should be tailored to the specific risks identified, including liability costs. For example, the organization is exposed to liability if customer data is exposed. If the failure to protect the data is due to an employee's action or inaction, and if this behavior violates the AUP, and if this policy is clear and enforced, then this may mitigate the liability of the organization.
3. **Distribute the AUP.** This includes educating employees on why an AUP is necessary.
4. **Monitor compliance.** A procedure is needed to monitor and report on AUP compliance.
5. **Enforce the policy.** The AUP must be enforced consistently and fairly when it is breached.

SANS Institute AUP Template https://www.sans.org/security-resources/policies/general#acceptable-use-policy

An example of a template for an AUP is provided by the SANS Institute. It has a similar structure to the security policy template shown in Section 4.1. The heart of the document is the policy section, which covers the following areas:

- **General use and ownership:** Key points in this section include:
  - Employees must ensure that proprietary information is protected.
  - Access to sensitive information is allowed only to the extent authorized and necessary to fulfill duties.
  - Employees must exercise good judgment regarding the reasonableness of personal use.

- **Security and proprietary information:** Key points in this section include:
  - Mobile devices must comply with the company's BYOD policies.
  - System- and user-level passwords must comply with the company's password policy.
  - Employees must use extreme caution when opening email attachments.
- **Unacceptable use—system and network activities:** Key points in this section include:
  - Unauthorized copying of copyrighted material
  - The prohibition against accessing data, a server, or an account for any purpose other than conducting company business, even with authorized access
  - Revealing your account password to others or allowing use of your account by others
  - Making statements about warranty unless it is a part of normal job duties
  - Circumventing user authentication or security of any host, network, or account
  - Providing information about, or lists of, company employees to outside parties
- **Unacceptable use—email and communication activities:** Key points in this section include:
  - Any form of harassment
  - Any form of spamming
  - Unauthorized use, or forging, of email header information
- **Unacceptable use—blogging and social media:** Key points in this section include:
  - Blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate company policy, is not detrimental to company's best interests, and does not interfere with an employee's regular work duties.
  - Any blogging that may harm or tarnish the image, reputation, and/or goodwill of company and/or any of its employees is prohibited.
  - Employees may not attribute personal statements, opinions, or beliefs to the company.

4.4 Security Management Best Practices

The SGP breaks down the best practices in the security management category into two areas and five topics and provides detailed checklists for each topic. The areas and topics are as follows:

- **Security policy management:** Discusses a specialist information security function, led by a sufficiently senior manager (e.g., a CISO), that is assigned adequate authority and resources to run information security-related projects; promote information security throughout the organization; and manage the implications of relevant laws, regulations and contracts.
  - **Information security policy:** Documents the governing body's direction on and commitment to information security and communicate it to all relevant individuals.
  - **Acceptable use policies:** Lists recommended actions for establishing AUPs, which define the organization's rules on how each individual (for example, an employee, a contractor) may use information and systems, including software, computer equipment, and connectivity.
- **Information security management:** Provides guidance for developing a comprehensive, approved information security policy (including supporting policies, standards, and procedures) and communicating it to all individuals who have access to the organization's information and systems.
  - **Information security function:** Ensures that good practice in information security is applied effectively and consistently throughout the organization.
  - **Information security projects:** Lists recommended actions for ensuring that all information security projects apply common project management practices, meet security requirements, and are aligned with the organization's business objectives.
  - **Legal and regulatory compliance:** Describes a process that should be established to identify and interpret the information security implications of relevant laws and regulations.

4.5 Key Terms and Review Questions

Key Terms

After completing this chapter, you should be able to define the following terms:

acceptable use policy (AUP)
capital planning
configuration management
information security strategic plan
security plan
security planning
security policy

Review Questions

Answers to the Review Questions can be found online in Appendix C, "Answers to Review Questions." Go to informit.com/title/9780134772806.

4.1 Define the security management function.

4.2 What are the two key individual roles in security management?

4.3 Explain key security program areas.

4.4 Describe the "select-control-evaluate" framework for capital planning.

4.5 Briefly explain the need of an effective information security policy. Also list different documents related to security.

4.6 Describe some common security policies of an organization.

4.7 What can be an effective structure of a security document?

4.8 What are the key aspects of security policy document?

4.9 What functions does information security management perform?

4.10 What do you understand by "acceptable use policy"?

4.6 References

INFO14: INFOSEC Institute, *Information Security Policies.* April 16, 2014. http://resources.infosecinstitute.com/information-security-policies/

GAO04: Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*. GAO-04-394G, March 2004.

NAYL09: Naylor, J., *Acceptable Use Policies—Why, What, and How*. MessageLabs White Paper, 2009. http://esafety.ccceducation.org/upload/file/Policy/AUP%20Legal%20advice.pdf

OMB10: Office of Management and Budget, NIST, and Federal Chief Information Officers Council, *Federal Enterprise Architecture Security and Privacy Profile.* 2010.