12.3.2 Security Policy Facts

A *security policy* defines the overall security outlook for an organization. To be effective, the security policy must be:

- Planned. Effective security is the result of good planning.
- Maintained. An effective security plan is constantly evaluated and modified as needs change.
- Used. The most common failure of a security policy is the lack of user awareness.

A comprehensive security policy is not just one document but rather a collection of documents, with each one detailing the policies for a specific area of concern.

Security Policy Documents

The following table lists several types of security policy documents that are commonly used by organizations.

Policy	Function
Acceptable Use	An acceptable use policy (AUP) identifies whether employees have rights to use company property, such as internet access and computer equipment, for personal use. The acceptable use agreement might set expectations for user privacy when using company resources. *Privacy* is the right of individuals to keep personal information from unauthorized exposure or disclosure. In a business environment, businesses might need to be able to monitor and record actions taken by employees. Such monitoring might be viewed as a violation of individual privacy. To protect your organization from legal issues: ▪ Define the types of actions and communications that will be monitored. For instance, it is typical for a business to reserve the right to monitor all activities performed on company computers, even if those activities are of a personal nature. ▪ Clearly communicate all monitoring activities. Users should know that monitoring is being performed. ▪ Monitor all employees. If you target specific employees, you could create grounds for discrimination charges. ▪ Comply with all legal requirements for privacy. For example, personal medical information is protected and cannot be shared without prior authorization.
Authorized Access	An authorized access policy documents access control to company resources and information. This policy specifies who is allowed to access an organization's various systems.
Remote Access	A *remote access* policy is a document that outlines and defines remote connections methods that are accepted by a company. Companies might have employees or contractors that work remotely, so networks are not only dispersed, but also potentially unsecure or unmanaged. The remote access policy helps secure assets and information that belongs to the company. The policy should cover all available methods to remotely access internal resources such as dial-in (SLIP, PPP), ISDN/Frame Relay, Telnet access from internet, and cable modem.
Privileged User Account	It's important to have a privileged user account policy. A *privileged user account* is any account that gives full access to the system. These accounts give users the ability to access and modify critical system settings, view restricted data, and so on. Some types of privilege user accounts include personal privileged account, administrative accounts, service accounts, and emergency accounts. The most common privileged users are system administrators, network engineers, database administrators, and upper management. Although these users are typically highly trusted in a company, they can also be the most dangerous threat to the company and its assets. A privilege user account policy helps protect the company against any users with privilege access who might try to cause harm.
Change and Configuration Management	A change and configuration management policy provides a structured approach to securing company assets and making process changes. Change management: ▪ Establishes hardware, software, and infrastructure configurations that are deployed universally throughout the corporation. ▪ Tracks and documents significant changes to the infrastructure. ▪ Assesses the risk of implementing new processes, hardware, or software. ▪ Ensures that proper testing and approval processes are followed before changes are allowed.
Code of Ethics	A *code of ethics* is a set of rules or standards that help you to act ethically in various situations. Because issues involved in various situations can be complex, the code of ethics does not prescribe actions for every situation. Rather, it identifies general principles of ethical behavior that can be applied to various situations. The code of ethics requires that employees associated with the security policy should: ▪ Conduct themselves in accordance with the highest standards of moral, ethical, and legal behavior. ▪ Not commit or be a party to any unlawful or unethical act that may negatively affect their professional reputation or the reputation of their profession.

	▪ Appropriately report activity related to the profession that they believe to be unlawful and cooperate with resulting investigations.

Human Resource Policies	*Human resource* policies related to security might include the following:
	▪ Hiring policies identify processes to follow before hiring. For example, the policy might specify that pre-employment screening include:
	  ▪ Employment, reference, and education history checks.
	  ▪ Drug screening.
	  ▪ A background investigation or credit rating check.
	▪ Termination policies and procedures identify processes for terminating employees. For example, the termination policy might specify that:
	  ▪ Network access and user accounts are disabled immediately.
	  ▪ Employees are escorted at all times following termination.
	  ▪ All company property is returned.
	  ▪ Appropriate documents are signed.
	▪ A requirement for job rotation cross-trains individuals and rotates users between positions on a regular basis. Job rotation helps to catch irregularities that could arise when one person is unsupervised over an area of responsibility.
	▪ A requirement for mandatory vacations requires employees to take vacations of specified length. These vacations can be used to audit employees' actions and provide a passage of time where problems caused by misconduct can surface.

Password	*Password policies* detail the requirements for passwords. This can include the following:
	▪ The same password should never be used for different systems.
	▪ Accounts should be disabled or locked out after a specified amount of failed login attempts.
	▪ Passwords should never contain words, slang, or acronyms.
	▪ Users should be required to change their passwords within a certain time frame and to use a rotation policy.
	▪ A strong password policy should be enforced. Strong passwords:
	  ▪ Contain multiple character types, uppercase and lowercase letters, numbers, and symbols.
	  ▪ Are a minimum length of eight characters.
	  ▪ Use no part of a user name or email address.

Privacy	A *privacy policy* outlines how the organization will secure private information for employees, clients, and customers. The privacy policy outlines how *Personally Identifiable Information* (PII) can be used and how it is protected from disclosure. PII items could include:
	▪ Full name
	▪ Address
	▪ Telephone number
	▪ Driver's license
	▪ National identification number
	▪ Credit card numbers
	▪ Email address
	Various laws govern privacy and the organization's responsibility to protect private information. A few of the high profile laws are identified below. As a network professional, it is your responsibility to become aware of and adhere to all of the laws that apply to your organization.
	▪ Health Insurance Portability and Accountability Act (HIPAA) defines security guidelines that enforce the privacy of medical records, including the transmission of records.
	▪ Sarbanes-Oxley Act (SARBOX) requires publicly traded companies to adhere to stringent reporting requirements and internal controls on electronic financial reporting systems. A key aspect of the law is the requirement for retaining copies of business records, including email, for a specified period of time.
	▪ Gramm-Leach-Bliley Act (GLBA) requires all banks and financial institutions to implement the following policies:
	  ▪ The Financial Privacy Rule requires banks and financial institutions to alert customers to their policies and practices in disclosing customer information.
	  ▪ The Safeguards Rule requires banks and financial institutions to develop a written information security plan detailing how they plan to protect electronic and paper files containing personally identifiable financial information.
	  ▪ The Pretexting Protection Rule requires banks and financial institutions to train their staff how to recognize social engineering exploits.
	▪ The USA Patriot Act mandates that organizations provide information, including records and documents, to law enforcement agencies under the authority of a valid court order, subpoena, or other authorized agency.
	▪ Many states mandate that when a security incident involving privacy occurs, organizations are obligated to inform users that their information could have been compromised.
	▪ The Children's Online Privacy Protection Act (COPPA) requires online services or websites designed for children under the age of 13 to:
	  ▪ Obtain parental consent prior to the collection, use, disclosure, or display of a child's personal information.

	▪ Allow children to participate without disclosing more personal information than is reasonably necessary to participate.
User Education and Awareness Training	User education and awareness training is designed to: ▪ Familiarize employees with the security policy. ▪ Communicate standards, procedures, and baselines that apply to the employee's job. ▪ Facilitate employee ownership and recognition of security responsibilities. ▪ Establish reporting procedures for suspected security violations. When an updated version of a security plan is produced, it is critical to prevent the public release of older versions of the document. Even an out-of-date plan can provide sufficient information for attackers to perform serious security intrusions. When the security plan is updated, users should be made aware of the changes, the document should be distributed internally to appropriate parties, and all old versions should be destroyed.
User Management	*User management* policies identify actions that must take place when employee status changes. The administrator of a network for an organization needs to be aware of new employees, employee advancements and transfers, and terminated employees to ensure the security of the system. All of these activities could result in changes to: ▪ Network access ▪ Equipment configuration ▪ Software configuration Failure to properly manage users can create a security risk known as creeping privileges. Creeping privileges is a form of privilege escalation that occurs when users are promoted or transferred to different departments and their previous position's privileges are not removed. As a result, the user accumulates privileges over time that are not necessary for their current work tasks.