3.1.4 Security Documentation Facts

A comprehensive security policy is not just one document, but rather a collection of documents, each one detailing the policies for a specific area of concern. The following table lists several types of security policy documents:

Policy	Function
Acceptable Use	An *acceptable use policy* (AUP) identifies the employees' 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 against 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 might be of a personal nature. ▪ Clearly communicate all monitoring activities. Users should know that monitoring is being performed. ▪ Apply monitoring to all employees. Targeting specific employees could be grounds for discrimination. ▪ 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 the various systems of the organization.
Configuration Management	A *configuration management policy* provides a structured approach to securing company assets and making changes. Configuration management: ▪ Establishes hardware, software, and infrastructure configurations that are to be 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 Escrow Agreement	A *code escrow agreement* is documentation of the storage and conditions of release of source code. For example, a code escrow agreement could specify that you can obtain the source code from a vendor if the vendor went out of business.
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 to take for every situation. Rather, it identifies general principles of ethical behavior that can be applied to various situations. The code of ethics requires that everyone associated with the security policy: ▪ 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	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 to be implemented when terminating employees. For example, the termination policy might specify that:
	  ▪ Network access and user accounts are disabled immediately
	  ▪ Exit interviews are conducted
	  ▪ 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 actions taken by the employee and provide a passage of time where problems caused by misconduct could become evident.

Organizational Security	The *organizational security policy* is a high-level overview of the corporate security program. The organizational security policy: ▪ Is usually written by the security professionals, but must be wholly supported and endorsed by senior management ▪ Identifies roles and responsibilities to support and maintain the elements of the security program ▪ Identifies what is acceptable and unacceptable regarding security management ▪ Identifies the rules and responsibilities of the enforcement of the policy

Password	*Password policies* detail the requirements for passwords for the organization. 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 use a rotation policy.
	▪ A strong password policy should be enforced. Strong passwords:
	  ▪ Contain multiple character types (uppercase, lowercase, numbers, and symbols).
	  ▪ Are a minimum length of eight characters or more.
	  ▪ 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. It is the responsibility of security professionals to become aware of and adhere to all of the laws that apply to their respective organizations.
	▪ The Health Insurance Portability and Accountability Act (HIPAA) defines security guidelines that enforce the protection of privacy. Specifically, HIPAA protects the privacy of medical records, including the transmission of these records.
	▪ The 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.
	▪ The Gramm-Leach-Bliley Act (GLBA) requires all banks and financial institutions to implement the following:
	  ▪ Financial Privacy Rule - requires banks and financial institutions to alert customers to their policies and practices in disclosing customer information.
	  ▪ 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.
	  ▪ Pretexting Protection - requires banks and financial institutions to train their staff how to recognize social engineering exploits.
	▪ The USA Patriot Act mandates organizations to 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. An example is the California Database Security Breach Act.
	▪ 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's participation without the need to disclose more personal information than is reasonably necessary to participate.
	▪ A Privacy Threshold Assessment (PTA) is a required document that serves as the official determination by the Department of Homeland Security (DHS) as to whether a department program or system has privacy implications and whether additional privacy compliance documentation is required, such as a Privacy Impact Assessment (PIA) and System of Records Notice (SORN). The PTA is built into departmental processes for technology investments and security. PTAs expire and must be reviewed and re-certified every three years. The purpose of a PTA is to:
	  ▪ Identify programs and systems that are privacy-sensitive
	  ▪ Demonstrate the inclusion of privacy considerations during the review of a program or system
	  ▪ Provide a record of the program or system and its privacy requirements at the DHS's Privacy Office
	  ▪ Demonstrate compliance with privacy laws and regulations
	▪ A Privacy Impact Assessment (PIA) is a process that assists organizations in identifying and minimizing the privacy risks of new projects or policies.

Resource Allocation	A *resource allocation policy* outlines how resources are allocated. Resources could include: ▪ Staffing ▪ Technology

	▪ Budgets
Service Level Agreement (SLA)	Service Level Agreements (SLAs), sometimes called maintenance contracts, guarantee the quality of a network service provider's care to a subscriber. SLAs often include descriptions for the following: ▪ The mean time between failures (MTBF) identifies the average lifetime of a system or component. Components should be replaced about the time that the MTBF is reached. ▪ The mean time to repair (MTTR) identifies the average amount of time necessary to repair a failed component or to restore operations. SLAs can include guarantees for: ▪ Turn-around times ▪ Average response times ▪ Number of online users ▪ System utilization rates ▪ System uptimes ▪ Volume of transactions ▪ Production problems Keep in mind the following recommendations for SLAs: ▪ SLAs should define, in sufficient detail, any penalties incurred if the level of service is not maintained. ▪ In the information security realm, it is also vital that the provider's role in disaster recovery operations and continuity planning is clearly defined. ▪ Industry standard templates are frequently used as a starting point for SLA design, but must be tailored to the specific project or relationship to be effective. ▪ If you depend on an SLA for mission-critical code, you should consider a *code escrow* arrangement. Code escrow is a storage facility hosted by a trusted third party which will ensure access to the mission critical code even if the development company, the company with whom you have the SLA, goes out of business.
User Education and Awareness Training	Security awareness and 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. Role-based security awareness training which should be tailored for the role of the employee (role-based awareness training) ▪ Data owner ▪ System Administrator ▪ System owner ▪ User ▪ Privileged user ▪ Executive user When an updated version of a security plan is produced, the most critical activity to prevent is public release of older versions of the document. Even an out of date plan can provide sufficient information to 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