13.1.4 Security Policy Facts

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

- Planned: Good security is the result of good planning.
- Maintained: A good security plan must be constantly evaluated and modified as needs change.
- Used: The most common failure of a security policy is the lack of user awareness. The most effective way of improving security is to implement user education and training.

There are several security-related policies that should be implemented within your organization:

Policy	Description
Organizational Security Policy	An Organizational Security Policy is a high-level overview of the organization's security program. The Organizational Security Policy is usually written by security professionals, but must be supported and endorsed by senior management. This policy usually identifies: - Roles and responsibilities to support and maintain the elements of the security program - What is acceptable and unacceptable regarding security management - The rules and responsibilities for enforcement of the policy
Acceptable Use Policy (AUP)	An Acceptable Use Policy (AUP) defines an employee's rights to use company property, such as: - Using computer equipment - Accessing data stored on company computers - Using the company's network - Accessing the internet through the organization's network For example, the AUP may identify whether users are allowed to: - Connect their personally-owned mobile devices to the organization's wireless network. If they are, it may also specify rules for what internet resources they are allowed to access using those devices. - Use company-owned computers for personal uses, such as shopping for personal items on ecommerce websites. The AUP should also set expectations for user privacy when using company resources. Privacy is the right of individuals to keep personal information from unauthorized exposure or disclosure. However, when using company-owned resources, organizations may need to monitor and record employee actions. To protect against potential legal issues, the AUP should disclose when employees may expect such monitoring to occur. For example, the AUP should: - Clearly communicate that monitoring may occur. - Define the types of activities that will be monitored. It is common 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. - Comply with all legal requirements for privacy. For example, personal medical information is protected and cannot be shared without prior authorization.

Password Policy	An organization's Password Policy identifies the requirements for passwords used to authenticate to company-owned systems. For example, this policy may specify:
	- Accounts should be disabled or locked out after a certain number of failed login attempts.
	- Users should be required to change their passwords within a certain time frame.
	- Users may not reuse old passwords.
	- Users must use strong passwords. Strong passwords should contain:
	  - Multiple character types, including uppercase letters, lowercase letters, numbers, and symbols.
	  - A minimum of eight characters. (More is better.)
	- User passwords should never contain:
	  - Words found in the dictionary.
	  - Personally-identifiable information, such as an employee's spouse's name, child's name, birth date, favorite sports teams, etc.
	  - Part of a username or email address

User Education and Awareness Policy	The strongest technological security measures can be quickly defeated if employees engage in unsafe behaviors, such as: ▪ Clicking links in a phishing email. ▪ Visiting malicious websites. ▪ Responding to social engineering attempts. ▪ Downloading and installing unauthorized software. Employee awareness is the key to prevent these behaviors. The User Education and Awareness Policy is designed to: ▪ Familiarize employees with the organization's security policy. ▪ Communicate standards, procedures, and baselines that apply to the employee's job. ▪ Facilitate employee ownership and recognition of security responsibilities. ▪ Explain how to respond to security events. ▪ Establish reporting procedures for suspected security violations.
Code of Ethics	Many organization's implement a code of ethics to prevent user-facilitated security issues. A code of ethics is a set of rules or standards that define ethical behavior. Because the issues involved in different situations may vary and can be quite complex, the code of ethics does not prescribe actions for every situation. Instead, it identifies general principles of ethical behavior that can be applied to various situations. For example, a company's code of ethics may require that everyone: ▪ 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 the organization. ▪ Appropriately report activity related to the profession that they believe to be unlawful. ▪ Openly cooperate with ongoing investigations.