3.1.3 Security Policy Facts

A security *policy* defines the overall security goals and processes 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 through user awareness.

When creating security policies, be aware of some other types of documents:

Document	Description
Regulation	A *regulation* (or law) is a requirement published by a government or other licensing body that must be followed. While you are not responsible for writing regulations, you are responsible for knowing which regulations apply to your organization and making sure that those regulations are understood and adhered to. Policies are often written in response to regulations.
Procedure	A *procedure* is a step-by-step process that outlines how to implement a specific action. The design of a procedure is guided by goals defined in a policy, but go beyond the policy by identifying specific steps that are to be implemented. The use of consistent procedures ensures that the goals defined in a policy are met and that the actions of multiple administrators are consistent.
Baseline	A *baseline* dictates the settings and security mechanisms that must be imposed on a system in order to comply with required security standards. Baselines are mandatory standards with which all systems must comply.
Guideline	A *guideline* is a recommendation for use when a specific standard or procedure does not exist. Guidelines are considered non-compulsory and flexible.

Under the direction of senior management, security professionals establish specific policies and plans related to the organization's security implementation. The purpose of these plans and policies is twofold: they protect the organization's assets and protect the organization from liability and exposure. Security planning must include:

- Complying with legal and regulatory compliance issues.
- Demonstrating ethical practices.
- Practicing *due care* in the development of security policy and procedures. Due care means that security has been examined and reasonable security measures have been put in place. Due care eliminates an organization's burden of negligence in case of a security breach.
- Practicing *due diligence* by ensuring that approved security measures have been implemented and continue to be effective.
- Implementing *due process* by adhering to laws regarding evidence and fairness to protect individuals' rights. Due process ensures that any party charged with a crime is fully aware of the charges held against them and has the opportunity to fully defend themselves.

The exercise of due care and due diligence, also called the *prudent man rule*, demonstrates that management has taken reasonable actions to ensure safety standards according to accepted best practices. The ability to demonstrate due care and due diligence protects the organization and its staff from accusations of negligence or incompetence in security-related issues.

Security policies need not to be created in a bubble. There are security frameworks, best practices and secure configuration guides that can help when creating secure architectures and systems.

- Security professionals have created industry-standard frameworks which describe the activities that will achieve specific security outcomes. In addition, security reference architectures can be used as templates when building a secure environment. In some cases, such as when creating government systems, a security framework or reference architecture may be mandated by government regulations. These frameworks and architectures can be customized for specific industries or may be customized for a specific nation. They can be generalized for organizations with international interests.
- Benchmarks and secure configuration guides can be used to harden computers, networks and vendor-specific devices. There are general purpose guides and guides that are platform specific or vendor specific. For example, there are secure configuration guides to harden web servers, operating systems, application servers and network infrastructure devices.