

**POLICY:**

A policy is a guiding or governing principle that mandates or constrains action.

**STANDARD:**

A standard is a level of quality that requires conformity.

**GUIDELINE:**

A guideline is recommended but optional behavior.

**PROCEDURE:**

A procedure is a series of interrelated steps that are taken to help implement a policy, standard or guideline. Instructions and forms facilitate completing the procedures.

From University of Minnesota

---

A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.

A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to harden a Windows NT workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows NT workstation on an external network segment.

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

From SANS