TYPES OF POLICY

Management must define three types of security policy according to the National Institute of Standards and Technology's special publication 800-14.

General or security program policies.
Issue-specific security policies
Systems-specific security policies.

General or Security Program Policy Enterprise Information Security Policy (EISP)

A security program policy (SPP) or EISP is also known as

- A general security policy
- IT security policy
- Information security policy

EISP

- The EISP is based on and directly supports the mission, vision, and direction of the organization and Sets the strategic direction, scope, and tone for all security efforts within the organization
- The EISP is an executive-level document, usually drafted by or with, the Chief Information Officer (CIO) of the organization and is usually 2 to 10 pages long.
- The EISP does not usually require continuous modification, unless there is a change in the strategic direction of the organization.
- The EISP guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework.
- It defines then purpose, scope, constraints, and applicability of the security program in the organization.
- It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users.
- Finally, it addresses legal compliance.
- According to NIST, the EISP typically addresses compliance in two areas:
  - General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components and
  - The use of specified penalties and disciplinary action.

Issue-Specific Security Policy (ISSP)

- As various technologies and processes are implemented, certain guidelines are needed to use them properly
- The ISSP:
  - addresses specific areas of technology like
    - Electronic mail
    - Use of the Internet

- Specific minimum configurations of computers to defend against worms and viruses.
- Prohibitions against hacking or testing organization security controls.
- Home use of company-owned computer equipment.
- Use of personal equipment on company networks
- Use of telecommunications technologies (FAX and Phone)
- Use of photocopy equipment.

requires frequent updates
contains an issue statement on the organization's position on an issue

- There are a number of approaches to take when creating and managing ISSPs within an organization.
- Three approaches:

Independent ISSP documents, each tailored to a specific issue.
A single comprehensive ISSP document covering all issues.
A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue‘s requirements.

- The independent document approach to take when creating and managing ISSPs typically has a scattershot effect.
- Each department responsible for a particular application of technology creates a policy governing its use, management, and control.
- This approach to creating ISSPs may fail to cover all of the necessary issues, and can lead to poor policy distribution, management, and enforcement.

- The single comprehensive policy approach is centrally managed and controlled.
- With formal procedures for the management of ISSPs in place , the comprehensive policy approach establishes guidelines for overall coverage of necessary issues and clearly identifies processes for the dissemination, enforcement, and review of these guidelines.
- Usually, these policies are developed by those responsible for managing the information technology resources.

- The optimal balance between the independent and comprehensive ISSP approaches is the modular approach.

- It is also certainly managed and controlled but tailored to the individual technology issues.
- The modular approach provides a balance between issue orientation and policy management.
- The policies created with this approach comprise individual modules, each created and updated by individuals responsible for the issues addressed.
- These individuals report to a central policy administration group that incorporates specific issues into an overall comprehensive policy.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf