NPTEL ASSIGNMENT
WEEK:-5

1. The primary function of a cybersecurity policy within an organization is to:

a. Define a rigid set of penalties for security violations.
b. Eliminate the need for ongoing security awareness training programs.
c. Dictate specific technical security controls for implementation.
d. Establish a comprehensive reference point for organizational cybersecurity practices.

2. Which type of policy is related to an organization's strategic purpose, mission, and vision?

a. Issue-specific information security policies (ISSP)
b. Systems-specific information security policies (SysSP)
c. Enterprise information security policy (EISP)
d. Technical implementation policy

3. True or False: Standards are broad, abstract documents that provide detailed procedures for employees to comply with policies.

a. True
b. False

4. Which of the following reflects the hierarchical top-down order of information security policies?

a. Enterprise > Issue-Specific > Systems-Specific
b. Systems-Specific > Issue-Specific > Enterprise
c. Issue-Specific > Enterprise > Systems-Specific
d. All three policy types are independent and unconnect

5. Which of the following components is typically included in the Enterprise Information Security Policy (EISP)?

a. Incident response procedures
b. Statement of purpose
c. Software development guidelines
d. Employee performance evaluations

6. True or False: Systems-specific security policies (SysSPs) can be separated into two general groups, managerial guidance SysSPs and technical specifications SysSPs

a. True
b. False

7. _____ consists of details about user access and use permissions and privileges for an organizational asset or resource.

a. Access Control Lists
b. Configuration rules
c. Authorized access and usage of equipment

d. Authorization rules

8. True or False: Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the lowest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments.

a. True
b. False

9. _____ are nonmandatory recommendations the employee may use as a reference in complying with a policy.
a. Practices
b. Procedures
c. Standards
d. Guidelines

10. Creating "air gaps" to isolate critical systems is a cyber hygiene practice that focuses on:
a. Installing the latest security patches.
b. Strengthening user authentication.
c. Segmenting networks for improved security
d. Keeping complex passwords up-to-date.