1. Explain the acronym CIA and the meaning of the terms that it stands for in Computer Security.

2. Explain and distinguish the meanings of the following terms: “Virus”, “Trojan Horse”, and “Worm”.

3. Standards, guidelines, and procedures are used to implement policies. Explain the meaning of these terms.

4. What are the two main benefits of increasing user awareness, user training, and user education? Explain each in a sentence or less.

5. Give the main technical possibilities for identification and authentication. You can group your answers by the four “W”: “What you know?”; “What you have?”; “What you are?”; and “Where you are?”.

6. The Computer System Life Cycle is broken into the following stages: Initiation, Development or Acquisition, Implementation, Operation/Maintenance, and Disposal. Explain the security activities in each cycle in at most two sentences each.

7. Explain the following risk mitigation options in a sentence or less: Risk assumption, risk avoidance, risk limitation, risk planning, and risk transference.

8. Are federal agencies allowed to accept residual risk? What are the criteria for accepting residual risks?

9. What is “stateful protocol analysis” in the context of a network intrusion detection and protection system? Give two or three examples.

10. In a single paragraph, describe the procedure for risk assessment.