DeVry University

|  |  |
| --- | --- |
| SEC 360 FINAL EXAM

|  |
| --- |
| **1.** (TCO 1) Security policy contains three kinds of rules as policy clauses. What are they? (Points : 5)  |

       Preventive, detective, and responsive       Prohibitive, permissive, and mandatory       Administrative, technical, and physical       Management, technical, and operational       Roles, responsibilities, and exemptions  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 2. **2.** (TCO 2) The 10 IISSCC \_\_\_\_\_ cover 17 NIST control \_\_\_\_\_ which are arranged in three \_\_\_\_\_ called management, operational, and technical. (Points : 5)  |

       controls, domains, principles       domains, families, classes       principles, domains, families       domains, families, technologies       technologies, domains, families  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 3. **3.** (TCO 2) What are the effects of security controls? (Points : 5)  |

       Confidentiality, integrity, and availability       Administrative, physical, and operational       Detection, prevention, and response       Management, operational, and technical  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 4. **4.** (TCO 3) Three of the most important jobs of security management are to ensure \_\_\_\_\_ are organized according to sensitivity, ensure that roles maintain \_\_\_\_\_, and to manage \_\_\_\_\_ because that is the enemy of security. (Points : 5)  |

       assets, accountability, software       assets, separation of duties, complexity       software, separation of duties, complexity       software, accountability, people       people, separation of duties, technology  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 5. **5.** (TCO 4) Privacy legislation is written to protect \_\_\_\_\_. (Points : 5)  |

       companies       managers       citizens       employees       All of the above |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 6. **6.** (TCO 5) Ideas can be evaluated using \_\_\_\_\_, which are \_\_\_\_\_ that are not meant to be \_\_\_\_\_. (Points : 5)  |

       models, controls, solutions       controls, abstractions, solutions       models, abstractions, solutions       solutions, controls, abstractions       models, controls, abstractions  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 7. **7.** (TCO 6) Physical security controls traditionally include obstacles, alarms, lights, guards, cameras, and responders that produce a(n) \_\_\_\_\_. (Points : 5)  |

       sense of security       defense-in-depth       protective shield       entrance barrier       secure facility  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 8. **8.** (TCO 7) The controls that are used by a security operations center including vulnerability management, threat monitoring, and situation reporting from a variety of sensors are used to assess \_\_\_\_\_. (Points : 5)  |

       status       readiness       known good state       compliance monitoring       intrusion detection  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 9. **9.** (TCO 8) Security recovery strategies should always seek to restore \_\_\_\_\_. (Points : 5)  |

       system files       application data       user access       networks supporting the IT infrastructure       the known good state  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 10. **10.** (TCO 9) Mandatory access control uses labels and rules to mediate access to \_\_\_\_\_ by \_\_\_\_\_. (Points : 5)  |

       objects, subjects       files, people       computer cycles, applications       information assets, people       information assets, network devices  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 11. **11.** (TCO 10) Generally, \_\_\_\_\_ are encrypted using symmetric cryptography and \_\_\_\_\_ are encrypted using asymmetric cryptography. (Points : 5)  |

       data, messages       signatures, data       channels, data       messages, channels       messages, information  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 12. **12.** (TCO 10) A company wishes to ensure that e-mail recipients may be confident that the contents of official e-mail messages were not altered in transit. Given this scenario, what type of cryptographic solution would be the most appropriate? (Points : 5)  |

       Symmetric encryption       Asymmetric encryption       SSL       IPSec       L2TP |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 13. **13.** (TCO 11) A packet-filtering router operates at OSI Layer 3 so it can filter Internet protocol source and destination addresses, but it can also filter \_\_\_\_\_ port numbers. (Points : 5)  |

       Layer 1       Layer 2       Layer 3       Layer 4/7       applications  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 14. **14.** (TCO 12) A good intrusion detection system will have all of the characteristics of the \_\_\_\_\_ model and will be flexible enough to adapt to \_\_\_\_\_. (Points : 5)  |

       Bell LaPadula, mandatory access control       reference monitor, vulnerabilities       Biba, vulnerabilities       OSI, loss of availability       reference monitor, loss of availability  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 15. **15.** (TCO 13) The SDLC Task Force was composed of four subgroups. Which one of the following subgroups recommended that IT centers and software assurance groups that are outside mainstream academia also include security components in their SDLC? (Points : 5)  |

       Education subgroup       Incentives subgroup       Patching subgroup       Software process subgroup       IETF subgroup |

**1.** (TCO 1) Explain what is wrong with this policy clause, and show how you could fix it. *People shall obey corporate policies.* (Points : 15)

|  |
| --- |
|         |

|  |
| --- |
| Question 2. **2.** (TCO 2) Briefly explain how the three effects of security controls--prevention, detection, and recovery--can be used to maintain the known good state for a system. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 3. **3.** (TCO 3) Briefly explain how defense in depth is a management strategy for security. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 4. **4.** (TCO 4)  Briefly explain what needs to be accomplished before your company monitors the activities of authorized users of your company systems, and then explain what should be accomplished to legally monitor the activities of a hacker (unauthorized user) of your system. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 5. **5.** (TCO 5) Explain the effects of the three goals of information security. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 6. **6.** (TCO 6) Briefly explain why good physical security is critical to good information security. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 7. **7.** (TCO 7) Explain what media disposition means. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 8. **8.** (TCO 8) Explain the term cold site. (Points : 15)  |

**Page 3**

|  |  |
| --- | --- |
|

|  |
| --- |
| Question 1. **1.** (TCO 9) Describe the fundamental difference between Mandatory Access Control (MAC) and Discretionary Access Control (DAC). (Points : 15)        |

 |

|  |
| --- |
|         |

|  |
| --- |
| Question 2. **2.** (TCO 10) Briefly explain why key management is a critical requirement for a good symmetric cryptographic solution. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 3. **3.** (TCO 11) Explain how a demilitarized zone might be used to protect critical resources that are not to be shared outside of an organization. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 4. **4.** (TCO 11) With regard to application-level gateway firewalls, determine the added costs in terms of the activities and resources required to effectively use them. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 5. **5.** (TCO 12)  Explain what the symbol P(A|B) means. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 6. **6.** (TCO 12) Evaluate the characteristics of a WAN and justify why it is more complex than a LAN. (Points : 15)        |

|  |
| --- |
|         |

|  |
| --- |
| Question 7. **7.** (TCO 13) Explain how a worm propagates itself. (Points : 15)  |