Fundamental Concepts of Data Security
ISEC2001

Security Controls II

Question 1

- Give an example of administrative preventive controls that addresses Confidentiality and briefly explain how.
- Give an example of technical corrective controls that addresses Integrity and briefly explain how.

Question 2

Describe one (1) example of administrative preventive controls and one (1) example of physical recovery controls, both of which must address Availability. For each example, briefly explain how it helps address availability.

Question 3

A small health organization has asked for advice in regards to improving its security system. The organization is already implementing a defense-in-depth mechanism which combines a firewall with the encryption of traffic to prevent confidential information being accessed by unauthorised personnel. The company has very limited funding and you can only suggest two additional security mechanisms to be considered. Describe the mechanism you have selected and justify your selection.

Question 4

A retailer is selling goods via both physical and online stores. The online store allows customers to create their own accounts, update personal and financial information, order goods, and track order status. It also links to the inventory management back-end. It has been suggested that three universal security methods; Least privileges, Compartmentalisation, and Defense-in-depth need to be used to enhance the security of the system. Describe your interpretation of these three (3) security methods in this particular scenario.

Question 5

With the help of an example, explain the principle *Fail securely*.

Question 6

With the help of an example, explain why the principle of minimization is important from the point of view system security.

Question 7

You are asked to give an advice on the security set-up for a medical research laboratory which has computer terminals connected to a server that stores sensitive information. a) Suggest two physical preventive controls and two physical detective controls that can be used and explain your choice. b) The laboratory is going to provide an Internet presence to assist researchers in finding information online. However, this raises a serious concern that the sensitive information is accessed by intruders from the outside world. Under the defense-in-depth principle, suggest specific security solutions for at least two layers of defense that may be deployed to mitigate the risk.

Question 8

It is often suggested to suspend or delay access capability after a number of unsuccessful login attempts. Describe the reason behind this suggestion and clearly indicate what security threat that this recommended practice addresses.

Question 9

With the help of examples explain the differences between three universal security principles/methods: Least privilege, Minimization, and Keep things simple.

Question 10

The logon screen of workstations in an organisation reads *”Warning: All activity is constantly monitored and logged, including hostname and IP address.”* Explain the purpose of this notice and determine the type of security control and the universal security method of this practice.