BCA Examination 2023-24

(Even Semester)

SECURITY DATA PRIVATE LAWS AND STANDARDS

Time : Three Hours] *[Maximum Marks : 60*

Note :– Attempt all questions.

SECTION – A

1. Attempt all parts of the following : $8 \times 1 = 8$

   (a) What is cyber crime?

   (b) What is confidentiality?

   (c) Define inference.

   (d) What is database?

[P. T. O.

(e) List out the international cyber crime laws.

(f) What is multi-factor authentication?

(g) What is risk assessment?

(h) Define access control.

SECTION – B

2. Attempt any two parts of the following: 2×6=12

(a) What are the primary strategies individuals can employ to prevent cybercrime in their daily online activities?

(b) Explain cyber law and different types of cyber-crimes.

(c) Why is it important to sue different passwords for different applications and what considerations should be taken into account when selecting these passwords?

(d) Discuss ISO 27001 standard.

SECTION – C

Note :– Attempt all questions. Attempt any two parts from each questions. 8×5=40

3. (a) Define trusted system and explain its key characteristics.

(b) Explain IP addresses and illustrate the difference between IPv4 and IPv6.

(c) What is security policies and explain its various methods and approaches to implementing security policies?

4. (a) Explain SQL injections vulnerability in detail.

(b) Discuss D-dos attack and what is the solution of the D-dos attack?

(c) Define the term reliability and integrity.

5. (a) Define risk analysis and explain its significance in cyber security.

(b) What is the importance of having a comprehensive security plan for an organization?

(c) Identify common challenges organizations face in managing passwords effectively.

6. (a) Explain rights of employer security.

(b) What role does digital analysis play in forensic investigations and how can digital evidence be collected and preserved?

(c) Discuss various methods to track down cyber-crimes.

⌘⌘⌘