ALL POSSIBLE UNI QUESTIONS OF ISS

Section A

Very Short Answer Questions (2 Marks Each)

1. Why is information system security required for an organization?
2. What is a threat in an information system?
3. Define Digital Signature and PKI with components.
4. Differentiate symmetric cryptography with asymmetric cryptography.
5. Define Honey pots, Port scanner, and Packet sniffers, VPN.
6. Define NIST security model.
7. What is the role of risk assessment?
8. In which situation is Disaster Recovery Planning useful?
9. What kinds of digital forensic facilities are available in Nepal?
10. Why are Ethical Concepts important for IT Professionals?
11. Define Information system and write its types.
12. Compare public key and private key.
13. What are the types of firewalls used in information security?
14. What do you mean by IoT? Write its uses.
15. What are the information security risks?
16. Why do forms need an information security plan?
17. What are the terms Affidavits and Warrants?
18. What is professional ethics?
19. What are the critical characteristics of Information?
20. What do you mean by Deviations in QoS in context of threats and attacks?
21. Briefly introduce about SET.
22. Define Information System Audit.
23. For what purposes is Digital Forensic done?
24. What are the three main characteristics of Hash function?
25. What are the ethical concepts in Information Security?

ALL POSSIBLE UNI QUESTIONS OF ISS

26. What is business resumption planning?

27. What is IPsec tunnel? Where is it used?

28. Why is it important to strike a balance between providing adequate security measures and allowing appropriate access to information systems?

29. Define malware with examples.

30. What are hash functions and when is it used?

31. What is Penetration Testing?

32. What do you mean by Packet Filtering?

33. What is IDPS?

34. What are two major objectives of Digital Forensic?

35. In risk management strategies, why must periodic review be a part of the process?

36. What is business resumption planning?

37. What is evidentiary material?

38. What is the difference between policy and law?

39. What is a digital certificate?

40. What are different tools and techniques of Digital Forensics?

41. Write a brief note on DES.

42. What are the different processing modes of Firewall?

43. Write a brief note on Vulnerability Scanning.

ALL POSSIBLE UNI QUESTIONS OF ISS

Section B

Descriptive Answer Questions (10 Marks Each)

1. What is the CIA framework? Which security model is suitable for Nepalese Information System Security?

2. Explain/Categorize different types of attacks and threats with their characteristics.

3. Which cryptographic technique is better for information security? Explain the use of Hash function and message encryption algorithm.

4. What is a Firewall? What are the functions of Intrusion Detection and Prevention Systems?

5. Explain enterprise information security policy and IETF security architecture.

6. How do you describe business continuity planning, especially in information systems? Explain digital forensic.

7. What is Cyber Law? Describe national and international legal provisions related to information security.

8. What are the components of Information Security? Explain CNSS Security model in detail.

9. Differentiate firewall with IDS (Intrusion Detection System). Explain the packet filtering firewall with example rules to protect your intranet web server from a public network.

10. Evaluate the role of auditing and digital forensic procedures in maintaining information security. Discuss the essential components of a digital forensic team and methodology.

11. What do you understand by information security policy? Define NIST Security Model.

12. What is cryptography? Explain cryptographic techniques/algorithms with characteristics in detail.

13. What is Continuity Planning? Detail BCP and DRP in the context of Nepal.

14. Explain briefly about Mail Bombing and Spams. Explain how DOS and DDOS attacks are done with diagrams.

15. Compare public key cryptography with private key cryptography. What is the importance of Digital Signature? Explain signing and verification process of digital signature.

16. What is an Intrusion? What are the various types of Intrusion Detection Systems? How can Intrusion be prevented?

17. Define information security risk? How is risk identification done? Explain different risk-handling strategies. What do you mean by residual Risk?

ALL POSSIBLE UNI QUESTIONS OF ISS

18. What are the basic components of contingency planning? Draw the diagram which shows the steps for contingency planning. Explain Incident Response planning.

19. Differentiate between Traditional Forensics and Digital Forensics. Explain about data acquisition types and methods.

20. Draw the architecture of PKI. Explain in detail about the AES algorithm.

21. Define authentication and authorization. Discuss various identification and authentication techniques, such as passwords, biometrics, and multi-factor authentication.

22. What are the professional standards and certifications available in the field of information security? How do these certifications promote ethical behavior and professionalism among practitioners?

23. How has computer security evolved into modern information security?

24. What is a circuit gateway, and how does it differ from the other forms of firewalls?

25. Who is responsible for risk management in an organization and why?

26. Define Firewall. Explain Screen Host Firewall and Dual-Homed Host Firewall.

27. What are Information Security Policy, Procedures, and Standards? What different generally accepted principles and practices of Information Security?

28. Define IDS and IPS. Compare host-based and network-based IDS/IPS with their implementation approach, advantages, and disadvantages.

29. Explain the PDCA cycle of ISMS based on ISO 27000.

ALL POSSIBLE UNI QUESTIONS OF ISS

Section C

Case Analysis (20 Marks)

Case Situation:

Africa is facing several Internet-related challenges concerning security risk, intellectual property infringement, and protection of personal data. This has cost the South African economy $573 million, the Nigerian economy $200 million, and the Kenyan economy $36 million. Small and Medium-sized Enterprises (SMEs) account for over 95% of firms, 60%-70% of employment, and generate a large share of new jobs in Organization for Economic Co-operation and Development (OECD) economies. Similar trends are being observed globally, with risks brought about by disruptive internet technologies such as information security breaches.

Questions:

a. Elaborate on the business risks due to information system security risks, especially in small and medium-sized businesses.

b. What sort of risk control strategies do you recommend to fix the above situation? Justify your answer.

Case Situation:

Science and Technology has played an ever-increasing role in our society. In fact, forensic science must be seen to act as a "Watch Dog" on behalf of the community against all hazards and abuse that may threaten it. The Judicial Reform Commission (1983) recommended the establishment of a well-equipped modern forensic science laboratory in Nepal. In the wake of this recommendation, the National Forensic Science Laboratory was set up and ran under the aegis of Nepal Academy of Science and Technology (NAST) from 1986 to 1995. From 1995 to 2000, the laboratory was under the Ministry of Law, Justice & Parliamentary Affairs as an autonomous organization. As per the decision of the Government of Nepal, this laboratory is now running as an autonomous organization under the Ministry of Education, Science & Technology. The Nepal Police has established a Digital Forensics Technology on 10th December 2015. The laboratory is equipped with basic facilities and some modern equipment such as DNA Analyzer, GC, GCMS, Raman Spectrometer, VSC 6000, and RT PCR. Technical units are headed by qualified and experienced forensic scientists and are supported by trained staff.

ALL POSSIBLE UNI QUESTIONS OF ISS

Questions:

a. What do you understand by Auditing and Digital Forensic? (5 Marks)

b. What is the context of Digital Forensic service and process in Nepal? (7 Marks)

c. Analyze the situation of policies and laws of Nepal for information security? Enlist loopholes and suggest solutions. (8 Marks)

Case Situation:

1. Suppose you are appointed as an Information Security officer in a Multi-National Company, what would be your Information Security plan? (10 Marks)

2. Analyze different legal provisions in Nepal for Information Security. (10 Marks)

Case Situation:

1. Explain major provisions of the Electronic Transaction Act, 2063 of Nepal.

2. "There is always a tradeoff between security and access" — Explain this statement with at least three different example cases.