# National Forensics Sciences University, Goa Campus
## TA-1 Examination

**Program Name – M.Sc. DFIS** **Sem – I** **Date- 10.09.24**
**Subject Name- Incident Management Response** **Subject Code- CTMSDFIS SI P3**
**Time- 45 minutes** **Max. Marks- 25**
**Instructions - 1) Answer all questions. 2) Assume suitable data.**

| | | |
|---|---|---|
| Q.1 | Multiple Choice Questions (1 mark each) | 10 marks |
| | 1a. A threat action in which sensitive data are directly released to an unauthorized entity is:<br>a. Corruption<br>b. Intrusion<br>c. Disruption<br>d. Exposure | 1 mark |
| | **1b.** A(n) ______is an attempt to learn or make use of information from the system that does not affect system resources.<br>a. Passive attack<br>b. Outside attack<br>c. Inside attack<br>d. Active attack | 1 mark |
| | **1c.** An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n)<br>a. Risk<br>b. Attack<br>c. Asset<br>d. Vulnerability | 1 mark |
| | **1d.** A loss of ____is the unauthorized disclosure of information.<br>a. Confidentiality<br>b. Authenticity<br>c. Integrity<br>d. Availability | 1 mark |
| | **1e.** Which of the following usually observes each activity on the internet of the victim, gathers all information in the background, and sends it to someone else?<br>a. Malware<br>b. Spyware<br>c. Adware<br>d. None of the above | 1 mark |
| | **1f.** Which of the following refers to violating the principle if a computer is no longer accessible?<br>a. Access control<br>b. Confidentiality<br>c. Availability | 1 mark |

| | | |
|---|---|---|
| | d. All of the above | |
| | **1g.** What describes the immediate action taken to isolate a system in the event of a breach?<br>a. Containment<br>b. Eradication<br>c. Recovery<br>d. None | 1 mark |
| | **1h.** Is the following statement true or false? 'Incident response is a structured methodology for handling security incidents, breaches, and cyber threats.'<br>a. True<br>b. False | 1 mark |
| | **1i.** Under which plan does personnel perform business processes in an alternate manner until normal operations resume?<br>a. Disaster recovery plan (DRP)<br>b. Business continuity plan (BCP)<br>c. Business impact analysis (BIA)<br>d. None | 1 mark |
| | **1j.** In the CIA Triad, which one of the following is not involved?<br>a. Availability<br>b. Confidentiality<br>c. Authenticity<br>d. Integrity | 1 mark |
| Q.2 | Answer any 3 questions (3x5 marks each) | 15 Marks |
| | i. Explain different Signs of the incidents. | 5 marks |
| | ii. How do you categorize different types of incidents? | 5 marks |
| | iii. List out the possible different incidents types an organization may face. | 5 marks |
| | iv. Explain the procedure to handle an incident faced by a Fintech company. | 5 marks |

Seat No.: ________ Enrolment No.____________

# NATIONAL FORENSIC SCIENCES UNIVERSITY

**M.Sc. DFIS**

**Semester – I – December - 2024**

**Subject Code: CTMSDFIS SI P3** **Date: 06.12.24**
**Subject Name: INCIDENT RESPONSE MANAGEMENT**
**Time: 02:30 PM to 05:30 PM** **Total Marks: 100**

**Instructions:**

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

| | | | **Marks** |
|---|---|---|---|
| **Q.1** | | **Attempt any three.** | |
| | **(a)** | Discuss the different functions/activities of the incident reporting organization such as CERT-IN | **08** |
| | **(b)** | List out the different categories of the incident, and explain with an example. | **08** |
| | **(c)** | Discuss the different types of botnets used to launch the attack. How would you control it? | **08** |
| | **(d)** | How do you analyze the data of a network and discuss its challenges & mitigations? | **08** |
| | | | |
| **Q.2** | | **Attempt any three.** | |
| | **(a)** | Discuss the different Signs of the incidents faced by a retail company such as Amazon/Flipkart. | **08** |
| | **(b)** | How do you prioritize the incidents, explain by considering a security breach at a critical infrastructure. | **08** |
| | **(c)** | Discuss the methodology and tools used for live data collection on Unix machine | **08** |
| | **(d)** | Discuss the different types of logs used and their role in IRM. | **08** |
| | | | |
| **Q.3** | | **Attempt any three.** | |
| | **(a)** | Discuss the role of virtualization in incident handling. | **08** |
| | **(b)** | Explain and discuss static, dynamic, and hybrid approaches for malware analysis. | **08** |
| | **(c)** | How do you handle and write a report of an incident where CIA is compromised? | **08** |
| | **(d)** | What are the two key forensic artifacts in Windows, explain. | **08** |
| | | | |
| **Q.4** | | **Attempt any two.** | |
| | **(a)** | What is an application data and where it stored, explain | **07** |

|  |  |  |  |
|---|---|---|---|
|  | **(b)** | How do you estimate the cost of an incident occurred at Fintech company? | **07** |
|  | **(c)** | How do you investigate email client when you suspect someone, explain the procedure? | **07** |
|  |  |  |  |
| **Q.5** |  | **Attempt any two.** |  |
|  | **(a)** | How does the IRM team handle phishing attacks and employee password compromise? Explain the procedure in detail. | **07** |
|  | **(b)** | How does the IRM team handle infrastructure monitoring and weak passwords? Explain the procedure in detail | **07** |
|  | **(c)** | How do you identify the occurrence of an incident in your organization? | **07** |
|  |  |  |  |

**--- End of Paper---**