# CYBER LAW AND SECURITY POLICY
# (INFO 4142)

**Time Allotted : 3 hrs** **Full Marks : 70**

***Figures out of the right margin indicate full marks.***

***Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.***

***Candidates are required to give answer in their own words as far as practicable.***

## Group – A
## (Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) Act of breaking into phone or other communication systems is known as
(a) War dialer (b) Cracking
(c) Phreaking (d) Hacking.

(ii) Ping flood is associated with
(a) Ping of death attack (b) Nuke
(c) Teardrop attack (d) Flood attack.

(iii) Tools used to launch DDoS attack is
(a) Trinoo (b) Targa
(c) Crazy Pinger (d) none of these.

(iv) What is the name of the virus that fool a user into downloading and/or executing them by pretending to be useful applications?
(a) Cracker (b) Worm
(c) Trojan horses (d) Keylogger.

(v) What kind of attempts is made by individuals to obtain confidential information from a person by falsifying their identity?
(a) Computer viruses (b) Spyware scams
(c) Phishing scams (d) None of the above.

(vi) Sniffing is a technique used for
(a) attack on computer hardware
(b) attack on computer software
(c) attack on operating system
(d) attack on wireless network.

(vii) _____ is a example of Cybercrime against society.
(a) Logic bomb (b) Cyberterrorism
(c) Password sniffing (d) Internet time theft.





(viii) Method in which Phisher identify prospective victims in advance and convey false information to entice them for disclosing personal and financial data is
(a) Rod and Reel (b) Lobsterpot
(c) Gillnet (d) Dragnet.

(ix) What is the self replicating program called?
(a) Keylogger (b) Cracker
(c) Worm (d) All of the above.

(x) Which one of the following is not a malware?
(a) Worm (b) Application Software
(c) Trojan (d) None of the above.

## Group – B

2. (a) Differentiate between Cyberspace, Cybersquatting and Cyberterrorism.

(b) Explain any four Active attack tools used in Cybercrime.

(c) What is Cyberstalking?

**6 + 4 + 2 = 12**

3. (a) State the phases involved in planning Cybercrime.

(b) State different types of Cybercriminals with examples.

(c) Explain any four Passive attack tools used in Cybercrime.

**3 + 5 + 4 = 12**

## Group – C

4. (a) Discuss about different types of attacks on mobile network.

(b) Explain the countermeasures to be practiced to prevent attacks on mobile/cell phones.

(c) Differentiate between virus and worms.

**6 + 4 + 2 =12**

5. (a) What kind of cyber security measures an organization should take in case of portable storage device?

(b) Differentiate between Software and hardware Keylogger.

(c) Suggest some techniques to prevent Vishing attack?

**6 + 4 + 2 = 12**

## Group – D

6. (a) State any five guidelines applicable to password policies to be implemented in organization.

   (b) What are the steps to prevent DoS/DDoS attack?

   (c) State the preventive measures from Trojan horse and Backdoor.

**5 + 4 + 3 = 12**

7. (a) Explain different types of DoS (Denial of Service) attacks in detail.

   (b) Explain the steps in SQL Injection attack.

   (c) Discuss the functions of Backdoor.

**6 + 4 + 2 = 12**

## Group – E

8. (a) Explain different types of Computer based Techniques of Identity Theft.

   (b) State and discuss the steps of Forensic investigation.

   (c) Discuss any four tools to protect online identity.

**3 + 5 + 4 = 12**

9. (a) Explain different types of Human based Techniques of Identity Theft.

   (b) State the preventive measures from being a victim of Identity Theft.

   (c) Explain any four tools for Digital Forensic Analysis.

**5 + 3 + 4 = 12**