Course Code	**:**	**MCS-215**
Course Title	**:**	**Security and Cyber Laws**
Assignment Number	**:**	**MCA_NEW(I)/215/Assign/2026**
Maximum Marks	**:**	**100**
Weightage	**:**	**30%**
Last date of Submission	**:**	**30th April 2026 (for January session)** **31st October 2026 (for July session)**

This assignment has six questions. Answer all questions. The remaining 20 marks are for viva voce. You may use illustrations and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of the presentation.

Q1: **(3*4= 12 Marks)**

(a) What are the three pillars of digital security? Explain any three benefits of digital security.
(b) Explain the following in the context of security threats and vulnerabilities**:**
(i) Phishing
(ii) Distributed Denial of Service Attack
(iii) Web Jacking
(c) Explain the technology safeguards that can help you counter the cybersecurity threats asked in part (b) of this question.
(d) What are the laws governing punishments against Social Engineering Attacks and Malware?

Q2: Explain the following terms with the help of an example of each, giving their advantages and disadvantages. **(3*6=18 Marks)**

(a) Substitution Ciphers
(b) Functions of Cryptography
(c) Steganography
(d) Symmetric Key Cryptography
(e) Electronic Signature
(f) Pseudo-Random Numbers and Sequences

Q3: **(3*4= 12 Marks)**

(a) Explain the key concerns that are to be addressed when you implement the CIA triad indata security.
(b) Explain the following security threats or attacks:
(i) State-sponsored attacks
(ii) Cyber-physical attacks
(c) Explain the following data security measures:
(i) Anti-Virus Protection
(ii) Access Security
(d) Explain the terms security policy and security management. How can you balance system security and user convenience**?** Explain.

Q4: **(3*4= 12 Marks)**

(a) What is the need for the regulation of Cyberspace? Explain.
(b) What are the uses of filtering devices and rating systems for Internet content? Explain with the help of an example of each.
(c) Explain the key principles and provisions of the UNCITRAL Model Law on Electronic Commerce.
(d) Explain the international initiatives for the regulation of cyberspace.

Q5: **(3*5= 15 Marks)**

(a) What is the classification of cybercrimes? Explain with the help of examples. Also, differentiate between cybercrime and traditional crime. Give one example of each.
(b) List the Penalties and compensation in Section 43 of the Information Technology Act 2000.
(c) List and explain any three sections from section 68 to section 72 as per the Information Technology Act, 2000.
(d) Explain the role of cyber forensics with the help of an example.
(e) List and explain any four cyber forensic techniques.

Q6: **(6+3+2= 11 Marks)**

(a) Explain the following forms of IPR with the help of an example of each:
(i) Patents.
(ii) Open license CC BY SA
(iii) Trademarks
(b) Explain domain name disputes and manipulation of search engine ranking with the help of an example of each.
(c) Briefly discuss the remedies that are available for the protection of Intellectual Property Rights.

Q1: (3*4= 12 Marks)

(a) What are the three pillars of digital security? Explain any three benefits of digital security.

Answer

The three pillars of digital security are Confidentiality, Integrity and Availability, commonly called the CIA triad. They give a simple way to decide what must be protected in a computer system and what can go wrong if security fails.

Three pillars of digital security

1. Confidentiality means that information is seen only by authorised persons. Passwords, access control, encryption and data classification are used to stop unauthorised disclosure. For example, only the account holder and authorised bank staff should be able to view confidential banking information.
2. Integrity means that data remains correct, complete and trustworthy. It should not be altered, deleted or replaced by an unauthorised person. Hash values, digital signatures, audit logs and controlled permissions help detect or prevent improper changes. A marks database, for instance, must not be changed without proper authority.
3. Availability means that authorised users can obtain information and services when they need them. Backups, redundant servers, power protection, network monitoring and disaster recovery plans support availability. A hospital information system that is secure but unavailable during an emergency is still failing an important security requirement.

Any three benefits of digital security

1. Protection of information and privacy. Security controls reduce the risk of personal, financial and organisational information being stolen, exposed or changed. This protects both the organisation and the people whose data it holds.
2. Continuity and reliability of services. Protection against malware, denial-of-service attacks, equipment failure and accidental loss helps systems remain usable. Regular backups and recovery arrangements also reduce the effect of an incident.
3. Trust and reduced financial loss. Customers and employees are more willing to use digital services when they believe their data and transactions are safe. Good security also reduces fraud, recovery cost, legal exposure and loss of reputation. Thus, the CIA triad is not only a technical idea; it supports dependable day-to-day digital operations.