

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

(Common to All Branches)

QUESTION BANK



VII SEMESTER

Mandatory Courses-II

MCY201 – AWARENESS OF CYBER SECURITY AND CYBER LAW

Regulation – 2023

Academic Year 2026-2027 (ODD Semester)

Prepared by

Mr.E.Rajkumar – Assistant Professor / CYS

Ms. T.Sathya-Assistant Professor / CYS

Ms.M.Raghavi – Assistant Professor / CYS

Mr.G.Avinesh Kumar – Assistant Professor / CYS

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

**DEPARTMENT OF CYBER SECURITY
(Common to All Branches)**

QUESTION BANK

SUBJECT : MCY201 – AWARENESS OF CYBER SECURITY AND CYBER LAW

SEM / YEAR: VII / IV

UNIT I: INTRODUCTION TO CYBER SECURITY AND CYBER CRIME			
Introduction - Cyber Crime: Definition and origins - Cyber crime and information Security - Cyber criminals– Classification of Cyber crimes.			
PART A (2 MARKS)			
Q.No	Questions	BTL Level	Competence
1.	Define Cyber Security.	BTL-1	Remembering
2.	Define Cyber Crime.	BTL-1	Remembering
3.	What is Information Security?	BTL-1	Remembering
4.	List the objectives of Cyber Security.	BTL-1	Remembering
5.	State any four characteristics of Cyber Crime.	BTL-1	Remembering
6.	What are cyber threats?	BTL-1	Remembering
7.	Define cyber criminals.	BTL-1	Remembering
8.	List the major categories of cyber criminals.	BTL-1	Remembering
9.	What is hacking?	BTL-1	Remembering
10.	What is identity theft?	BTL-1	Remembering
11.	What is phishing?	BTL-1	Remembering
12.	Define malware.	BTL-1	Remembering
13.	Distinguish between Cyber Security and Information Security.	BTL-2	Understanding
14.	Explain the relationship between Cyber Crime and Information Security.	BTL-2	Understanding
15.	Differentiate cyber criminals from ethical hackers.	BTL-2	Understanding
16.	Explain the origin and evolution of Cyber Crime.	BTL-2	Understanding
17.	Classify Cyber Crimes based on their targets.	BTL-2	Understanding
18.	Explain the need for Cyber Security in the digital era.	BTL-2	Understanding
19.	Describe the impact of Cyber Crime on individuals and organizations.	BTL-2	Understanding
20.	Summarize the importance of awareness in preventing Cyber Crime.	BTL-2	Understanding

PART B (16 MARKS)

1.	Explain the concepts of Cyber Security and Information Security with suitable examples, and discuss their significance in protecting digital assets.	BTL-3	Applying
2.	Discuss the origin and evolution of Cyber Crime, highlighting the major factors responsible for its rapid growth.	BTL-3	Applying
3.	Classify Cyber Crimes based on their targets and nature, and explain each category with suitable examples.	BTL-3	Applying
4.	Analyze the relationship between Cyber Crime and Information Security, explaining how security principles help reduce cyber risks.	BTL-4	Analyzing
5.	Compare different categories of cyber criminals based on their objectives, skills, and methods of operation.	BTL-4	Analyzing
6.	Analyze the various threats posed by Cyber Crime to individuals, organizations, and governments.	BTL-4	Analyzing
7.	Explain the role of Cyber Security in protecting personal information, organizational resources, and national infrastructure.	BTL-3	Applying
8.	Evaluate the importance of Cyber Security awareness in minimizing cyber risks and preventing cyber attacks.	BTL-5	Evaluating
9.	Analyze how poor security practices contribute to the occurrence of Cyber Crimes.	BTL-4	Analyzing
10.	Examine the importance of adopting preventive security measures against common Cyber Crimes.	BTL-4	Analyzing
11.	Evaluate the impact of Cyber Crime on business operations, economic growth, and social well-being.	BTL-5	Evaluating
12.	Explain how the classification of Cyber Crimes assists investigators and security professionals in responding to incidents effectively.	BTL-3	Applying
13.	Analyze the responsibilities of individuals and organizations in maintaining Cyber Security and reducing cyber risks.	BTL-4	Analyzing
14.	Assess the challenges faced by society due to the increasing sophistication of Cyber Crimes.	BTL-5	Evaluating
15.	Explain how awareness, education, and responsible online behavior contribute to Cyber Security.	BTL-3	Applying
16.	Analyze the role of Cyber Security in ensuring confidentiality, integrity, and availability of information.	BTL-4	Analyzing
17.	Evaluate the effectiveness of different approaches for reducing Cyber Crime through awareness and security best practices.	BTL-5	Evaluating

**UNIT II:
LEGAL PERSPECTIVES**

Introduction to the Legal Perspectives of Cybercrimes and Cyber security, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India

PART A (2 MARKS)

Q.No	Questions	BTL Level	Competence
1	Define Cyber Law.	BTL-1	Remembering
2	What is meant by the legal perspective of Cyber Crime?	BTL-1	Remembering
3	Define Cyber Security from a legal perspective.	BTL-1	Remembering
4	State the need for Cyber Laws.	BTL-1	Remembering
5	What is the objective of the Indian Information Technology Act?	BTL-1	Remembering
6	Expand IT Act and mention the year in which it was enacted.	BTL-1	Remembering
7	List any four objectives of the Indian IT Act.	BTL-1	Remembering
8	What is electronic governance (e-Governance)?	BTL-1	Remembering
9	What is meant by electronic records?	BTL-1	Remembering
10	Define cyber offence.	BTL-1	Remembering
11	What is meant by legal jurisdiction in cyberspace?	BTL-1	Remembering
12	List any four challenges in enforcing Cyber Laws.	BTL-1	Remembering
13	Explain why Cyber Laws are essential in the digital environment.	BTL-2	Understanding
14	Differentiate traditional crimes from Cyber Crimes from a legal perspective.	BTL-2	Understanding
15	Explain the significance of the Indian IT Act in combating Cyber Crime.	BTL-2	Understanding
16	Summarize the Cyber Crime scenario in India.	BTL-2	Understanding
17	Explain the challenges faced by Indian laws in addressing Cyber Crime.	BTL-2	Understanding
18	Differentiate national and international legal perspectives on Cyber Crime.	BTL-2	Understanding
19	Explain the importance of legal awareness in Cyber Security.	BTL-2	Understanding
20	Describe the relationship between Cyber Law and Cyber Security.	BTL-2	Understanding

PART B (16 MARKS)

Q.No	Questions	BTL Level	Competence
1.	Explain the legal perspectives of Cyber Crime and discuss their importance in ensuring Cyber Security.	BTL-3	Applying
2.	Discuss the need for Cyber Laws in protecting individuals, organizations, and governments from Cyber Crimes.	BTL-3	Applying
3.	Explain the objectives, features, and significance of the Indian Information Technology Act in addressing Cyber Crime.	BTL-3	Applying

4.	Analyze the legal landscape of Cyber Crime across the world and discuss the challenges involved in enforcing Cyber Laws internationally.	BTL-4	Analyzing
5.	Examine the major provisions of the Indian IT Act that support secure electronic transactions and Cyber Security.	BTL-4	Analyzing
6.	Analyze the major challenges faced by the Indian legal system in investigating and prosecuting Cyber Crimes.	BTL-4	Analyzing
7.	Explain the Cyber Crime scenario in India and discuss the factors contributing to the increase in Cyber Crimes.	BTL-3	Applying
8.	Compare conventional legal systems with Cyber Laws in addressing digital offences.	BTL-4	Analyzing
9.	Analyze the importance of jurisdiction in handling Cyber Crime cases involving multiple countries.	BTL-4	Analyzing
10.	Evaluate the effectiveness of the Indian IT Act in preventing and controlling Cyber Crimes.	BTL-5	Evaluating
11.	Assess the role of Cyber Laws in promoting trust, privacy, and security in electronic communication and online transactions.	BTL-5	Evaluating
12.	Explain how legal awareness contributes to reducing Cyber Crimes among Internet users.	BTL-3	Applying
13.	Analyze the limitations of existing Cyber Laws in addressing emerging Cyber Security challenges.	BTL-4	Analyzing
14.	Evaluate the importance of international cooperation in combating Cyber Crimes and strengthening Cyber Security.	BTL-5	Evaluating
15.	Examine the relationship between Cyber Security policies and Cyber Laws in ensuring a secure digital environment.	BTL-4	Analyzing
16.	Analyze the impact of technological advancements on the development and enforcement of Cyber Laws.	BTL-4	Analyzing
17.	Evaluate the role of legal frameworks in creating a secure cyberspace for individuals, businesses, and governments.	BTL-5	Evaluating

UNIT III: CYBER ACT

Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

PART A (2 MARKS)

Q.No	Questions	BTL Level	Competence
1	Define the Information Technology (IT) Act.	BTL-1	Remembering
2	What is a Digital Signature?	BTL-1	Remembering
3	Define Cyber Law.	BTL-1	Remembering
4	What is meant by Cybercrime punishment?	BTL-1	Remembering
5	List any four objectives of the Information Technology Act.	BTL-1	Remembering

6	What are the consequences of weaknesses in the Information Technology Act?	BTL-1	Remembering
7	What is meant by electronic authentication?	BTL-1	Remembering
8	State the purpose of Digital Signatures in electronic transactions.	BTL-1	Remembering
9	List any four benefits of Digital Signatures.	BTL-1	Remembering
10	What is meant by legal recognition of electronic records?	BTL-1	Remembering
11	Define cyber offence under the IT Act.	BTL-1	Remembering
12	What is meant by cyber punishment?	BTL-1	Remembering
13	Explain the significance of Digital Signatures in ensuring secure electronic communication.	BTL-2	Understanding
14	Differentiate handwritten signatures and Digital Signatures.	BTL-2	Understanding
15	Explain the role of the IT Act in preventing Cyber Crimes.	BTL-2	Understanding
16	Summarize the consequences of not addressing weaknesses in the Information Technology Act.	BTL-2	Understanding
17	Explain the importance of Cyber Law for students in India.	BTL-2	Understanding
18	Differentiate Cyber Crime and Cyber Punishment.	BTL-2	Understanding
19	Describe the relationship between Digital Signatures and Cyber Law.	BTL-2	Understanding
20	Explain the role of Cyber Laws in promoting secure digital transactions.	BTL-2	Understanding

PART B (16 MARKS)

Q.No	Questions	BTL Level	Competence
1	Explain the objectives and significance of the Information Technology Act in promoting Cyber Security and secure electronic transactions.	BTL-3	Applying
2	Discuss the consequences of failing to address weaknesses in the Information Technology Act and their impact on Cyber Security.	BTL-3	Applying
3	Explain the concept of Digital Signatures and discuss their importance in ensuring authentication, integrity, and non-repudiation of electronic records.	BTL-3	Applying
4	Analyze the relationship between Digital Signatures and the Indian Information Technology Act in securing electronic transactions.	BTL-4	Analyzing
5	Examine the legal provisions relating to Cyber Crime and punishment under the Information Technology Act.	BTL-4	Analyzing
6	Analyze the importance of Cyber Laws in protecting individuals and organizations against Cyber Crimes.	BTL-4	Analyzing
7	Explain the role of Cyber Law in promoting responsible use of technology among students in the Indian context.	BTL-3	Applying
8	Analyze the challenges faced by students due to misuse of technology and explain how Cyber Laws help address these issues.	BTL-4	Analyzing
9	Compare conventional authentication methods with Digital Signatures in terms of security, reliability, and legal validity.	BTL-4	Analyzing
10	Evaluate the effectiveness of Digital Signatures in securing electronic communication and online transactions.	BTL-5	Evaluating

11	Assess the importance of strengthening the Information Technology Act to address emerging Cyber Security challenges.	BTL-5	Evaluating
12	Explain the legal implications of Cyber Crimes and discuss the importance of appropriate punishment in preventing digital offences.	BTL-3	Applying
13	Analyze the role of the Information Technology Act in supporting digital governance and electronic commerce.	BTL-4	Analyzing
14	Evaluate the impact of legal awareness among students in promoting ethical and secure use of information technology.	BTL-5	Evaluating
15	Examine how Digital Signatures enhance trust and confidence in electronic governance and digital services.	BTL-4	Analyzing
16	Analyze the effectiveness of the Indian Cyber Law framework in protecting users from Cyber Crimes in educational institutions.	BTL-4	Analyzing
17	Evaluate the need for continuous revision of Cyber Laws to address technological advancements and emerging Cyber Crime trends.	BTL-5	Evaluating

UNIT IV: CYBER LIABILITY			
Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right– source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing.			
PART A (2 MARKS)			
Q.No	Questions	BTL Level	Competence
1	Define Cyber Liability.	BTL-1	Remembering
2	What is meant by Private Ordering Solutions?	BTL-1	Remembering
3	Define Jurisdiction in Cyber Law.	BTL-1	Remembering
4	What is meant by Global Cyber Security?	BTL-1	Remembering
5	Define Copyright.	BTL-1	Remembering
6	What are the major sources of copyright risks?	BTL-1	Remembering
7	Who are software pirates?	BTL-1	Remembering
8	Define Internet Infringement.	BTL-1	Remembering
9	What is Fair Use?	BTL-1	Remembering
10	What is meant by online postings?	BTL-1	Remembering
11	Define Criminal Liability in cyberspace.	BTL-1	Remembering
12	What is Data Loss?	BTL-1	Remembering
13	Explain the importance of jurisdiction in Cyber Security.	BTL-2	Understanding
14	Differentiate Copyright infringement and Fair Use.	BTL-2	Understanding
15	Explain the significance of Private Ordering Solutions in cyberspace.	BTL-2	Understanding
16	Distinguish between Civil Liability and Criminal Liability in Cyber Law.	BTL-2	Understanding
17	Explain the role of Copyright in protecting digital content.	BTL-2	Understanding
18	Describe the impact of Internet Infringement on intellectual property rights.	BTL-2	Understanding

19	Explain the causes and consequences of Data Loss.	BTL-2	Understanding
20	Summarize the importance of legal compliance in online activities.	BTL-2	Understanding
PART B (16 MARKS)			
Q.No	Questions	BTL Level	Competence
1	Explain the concept of Cyber Liability and discuss its significance in protecting digital resources and online activities.	BTL-3	Applying
2	Discuss the role of Private Ordering Solutions in addressing Cyber Security issues and resolving online disputes.	BTL-3	Applying
3	Explain the importance of regulation and jurisdiction in ensuring Global Cyber Security.	BTL-3	Applying
4	Analyze the challenges involved in enforcing jurisdiction over Cyber Crimes that cross national boundaries.	BTL-4	Analyzing
5	Examine the importance of Copyright protection in the digital environment and explain the various sources of copyright risks.	BTL-4	Analyzing
6	Analyze the impact of software piracy and Internet infringement on individuals, organizations, and society.	BTL-4	Analyzing
7	Explain the concept of Fair Use and discuss its significance in the lawful use of copyrighted digital content.	BTL-3	Applying
8	Compare Copyright infringement and Fair Use with suitable examples from cyberspace.	BTL-4	Analyzing
9	Analyze the legal implications of unauthorized online postings and their effect on Cyber Liability.	BTL-4	Analyzing
10	Evaluate the role of Criminal Liability in preventing Cyber Crimes and ensuring accountability in cyberspace.	BTL-5	Evaluating
11	Assess the effectiveness of legal regulations in protecting intellectual property rights in the digital environment.	BTL-5	Evaluating
12	Explain the causes, consequences, and preventive measures for Data Loss in computer systems and networks.	BTL-3	Applying
13	Analyze the responsibilities of individuals and organizations in preventing copyright violations and ensuring legal compliance.	BTL-4	Analyzing
14	Evaluate the importance of international cooperation in addressing jurisdictional issues related to Cyber Liability.	BTL-5	Evaluating
15	Examine the relationship between Cyber Liability, Copyright protection, and Global Cyber Security.	BTL-4	Analyzing
16	Analyze the importance of adopting best practices to minimize legal risks associated with Internet usage and digital content.	BTL-4	Analyzing
17	Evaluate the effectiveness of Cyber Liability provisions in protecting intellectual property rights and reducing cyber-related legal disputes.	BTL-5	Evaluating

**UNIT V:
CYBER CHANGES**

Ethics, Legal Developments, Cyber security in Society, Security in cyber laws case studies, General law and Cyber Law—a Swift Analysis.

PART A (2 MARKS)

Q.No	Questions	BTL Level	Competence
1	Define Cyber Ethics.	BTL-1	Remembering
2	What is meant by Legal Developments in Cyber Law?	BTL-1	Remembering
3	Define Cyber Security in society.	BTL-1	Remembering
4	What is a Cyber Law case study?	BTL-1	Remembering
5	Define General Law.	BTL-1	Remembering
6	What is Cyber Law?	BTL-1	Remembering
7	List any four principles of Cyber Ethics.	BTL-1	Remembering
8	State the need for Cyber Ethics in the digital society.	BTL-1	Remembering
9	What is responsible online behaviour?	BTL-1	Remembering
10	What is digital citizenship?	BTL-1	Remembering
11	What is ethical use of information technology?	BTL-1	Remembering
12	Define cyber misconduct.	BTL-1	Remembering
13	Explain the importance of Cyber Ethics in ensuring a secure digital environment.	BTL-2	Understanding
14	Differentiate General Law and Cyber Law.	BTL-2	Understanding
15	Explain the significance of legal developments in Cyber Security.	BTL-2	Understanding
16	Summarize the role of Cyber Security in society.	BTL-2	Understanding
17	Explain the importance of Cyber Law case studies in understanding legal issues.	BTL-2	Understanding
18	Distinguish between ethical and unethical use of cyberspace.	BTL-2	Understanding
19	Explain the relationship between Cyber Ethics and Cyber Law.	BTL-2	Understanding
20	Describe the importance of legal awareness in promoting safe use of cyberspace.	BTL-2	Understanding

PART B (16 MARKS)

Q.No	Questions	BTL Level	Competence
1	Explain the concept of Cyber Ethics and discuss its importance in promoting responsible use of information technology.	BTL-3	Applying
2	Discuss the major legal developments in Cyber Law and explain their significance in addressing emerging Cyber Security challenges.	BTL-3	Applying
3	Explain the role of Cyber Security in society and discuss how it contributes to protecting individuals, organizations, and public services.	BTL-3	Applying
4	Analyze the relationship between Cyber Ethics and Cyber Law in ensuring a secure and responsible digital environment.	BTL-4	Analyzing

5	Examine the importance of Cyber Law case studies in understanding legal issues and improving Cyber Security practices.	BTL-4	Analyzing
6	Compare General Law and Cyber Law with respect to their objectives, scope, and applicability in cyberspace.	BTL-4	Analyzing
7	Analyze the ethical responsibilities of Internet users in preventing misuse of information technology.	BTL-4	Analyzing
8	Explain how legal developments have influenced the evolution of Cyber Security practices in modern society.	BTL-3	Applying
9	Analyze the role of ethical principles in promoting trust, privacy, and responsible behaviour in cyberspace.	BTL-4	Analyzing
10	Evaluate the effectiveness of Cyber Ethics in reducing cyber misconduct and promoting safe online practices.	BTL-5	Evaluating
11	Assess the importance of Cyber Law in addressing emerging technological challenges and protecting digital society.	BTL-5	Evaluating
12	Explain the significance of Cyber Law case studies in creating awareness about legal and ethical responsibilities.	BTL-3	Applying
13	Analyze the impact of legal awareness on ensuring compliance with Cyber Laws among Internet users.	BTL-4	Analyzing
14	Evaluate the role of Cyber Security in building a secure and trustworthy digital society.	BTL-5	Evaluating
15	Examine the importance of integrating ethical values with legal compliance for effective Cyber Security.	BTL-4	Analyzing
16	Analyze the need for continuous improvements in Cyber Laws to address evolving cyber threats and technological advancements.	BTL-4	Analyzing
17	Evaluate the role of Cyber Ethics, legal developments, and Cyber Law in creating a safe, secure, and legally compliant cyberspace.	BTL-5	Evaluating