# SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMAKURU

## COURSE PLAN FOR THE ODD SEMESTER OF THE ACADEMIC YEAR 2025 – 2026

| | | | |
|---|---|---|---|
| **Faculty In-charge** | **Ramu S** | **Dept.** | **Information Science and Engineering** |
| **Semester** | **7th** | **Course Name** | **Cyber Security and Digital Forensics** |
| **Section** | **E and F (Online)** | **Course Code** | **S7IS01** |

| **Course Learning Objectives (CLOs): This course will make student to:** | |
|---|---|
| 1 | Understand the fundamentals of information systems, the evolution of cybersecurity, and foundational security principles and models. |
| 2 | Explore various types of cybercrimes, their motivations, methods, and global countermeasures |
| 3 | Identify common vulnerabilities in IT systems and assess risk factors impacting data, networks, and third-party dependencies. |
| 4 | Understand the cybersecurity management practices, policies, standards, and business continuity strategies. |
| 5 | Evaluate the role of technologies, legal frameworks, human factors, and emerging trends in building a secure cyber ecosystem. |

| **Course Code** | **Course Title** | **Teaching & Learning Scheme** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Classroom Instruction (CI) (in hrs / sem )** | | **Lab Instruction (LI) (in hrs / sem)** | **Self-Learning (SL) (in hrs / sem)** | **Term Work (TW) (in hrs / sem)** | **Assessment (A) (hrs / sem)** | **Total no. of Hours per sem** | **Total Credits (C) = (Total Hours/30)** |
| | | **L** | **T** | **P** | **SL** | **TW** | **A** | | |
| **S7IS01** | **Cybersecurity and Digital Forensics** | **42** | **28** | **-** | **14** | **29** | **7** | **120** | **4** |

| Sl. No. | Date | Topic | Remarks |
|---|---|---|---|
| **UNIT 1** | | | |
| 1. | 02/09/2025 | **Security in an Interconnected World:** Cyberspace and Cybersecurity | |
| 2. | 03/09/2025 | Information Security, Organisation and Governance of the Internet and Cybersecurity, Information Security Models. | |
| 3. | 04/09/2025 | **Cybercrime, Cyberattack Tools and Methods, Threat Sources and Cyber Offenders:** What is a Cybercrime? Classification of Cybercrimes, Forms of Cybercrimes, Cyber Scams and Frauds | |
| 4. | 09/09/2025 | Sources of Threats: Threat Actors and their Motivations, Tools and Methods Used in Cyberattacks/Cybercrimes, what is a Cyberattack? | |
| 5. | 10/09/2025 | Responding to Cyberattacks and the Cyber Kill Chain | |
| 6. | 11/09/2025 | cyberattacks: Organizational Implications | |
| 7. | 16/09/2025 | Cyberattacks Impacting Citizens and Communities, Prevention of Cybercrime | |
| 8. | 17/09/2025 | International Efforts to Deal with Cybercrime, National Cyber security Policy, Online Code of Conduct and Computer Ethics. | 8Hrs |
| **UNIT II** | | | |
| 9. | 18/09/2025 | **Cybersecurity Vulnerabilities:** Security Considerations and Challenges | |
| 10. | 23/09/2025 | Types of Vulnerabilities, Project OWASP | |
| 11. | 24/09/2025 | Vulnerabilities Assessment, Common Vulnerabilities and Exposures (CVE): Institutional Mechanism | |
| 12. | 25/09/2025 | **Cybersecurity Management Practices**: Overview of Cybersecurity Management | |
| 13. | 30/09/2025 | Information Classification Process, Security Policies | |
| 14. | 08/10/2025 | Security Procedures and Guidelines, Security Controls | |
| 15. | 09/10/2025 | Security Organization, Incident Response | 8Hrs |
| 16. | 14/10/2025 | Business Continuity and Disaster Recovery. | Quiz-I |
| **UNIT III** | | | |
| 17. | 15/10/2025 | **Developing Secure Information Systems:** Securing Information Assets | |
| 18. | 16/10/2025 | Data Security and Protection, Application Security | |
| 19. | 21/10/2025 | Security Architecture and Design Security Issues in Hardware, Mobile Devices and Internet of Things | |
| 20. | 23/10/2025 | Network Security, Operating system security, Database security | |
| 21. | 28/10/2025 | User Management, Physical Security of IT Assets, Techniques/ Methods for Data Security and Protection, Issues Related to Digital File Sharing. | |
| 22. | 29/10/2025 | **Cybersecurity Strategies and Approaches:** Information Security governance and Risk Management, | |
| 23. | 30/10/2025 | Cyber Risk Management, Cybersecurity Frameworks, Cyber Resilience | |
| 24. | 04/11/2025 | Industry-specific Cybersecurity Frameworks, The Human Factor in Cybersecurity | |
| 25. | 05/11/2025 | Algorithms and Techniques for Cybersecurity | 9 Hrs |

| | | | |
|---|---|---|---|
| **UNIT IV** | | | |
| 26. | 06/11/2025 | **Cybersecurity Technologies:** Securing Networks, Web Applications | |
| 27. | 11/11/2025 | Services and Servers, Email Security, Antivirus Technologies and Solutions | |
| 28. | 12/11/2025 | Identity and Access Management, Authentication, Cryptography | |
| 29. | 13/11/2025 | How Do Digital Money, Cryptocurrency and NFTs Work?, Digital Signatures, | |
| 30. | 18/11/2025 | Advanced Technologies and Approaches in Cybersecurity, Internet Protocols and Ports. | |
| 31. | 19/11/2025 | **Cyber Laws and Forensics:** Need for Cyber Laws and Regulations, Role of International Law and Governments, | |
| 32. | 20/11/2025 | Challenges for Law-makers and Law Enforcement Agencies, Cybersecurity Regulations, | |
| 33. | 25/11/2025 | Cyber Forensics Cybercrime Techniques, Prevention of Cybercrime and Protection, Cybercrime Investigation, | 9 Hrs |
| 34. | 26/11/2025 | Evidence Collection and Analysis, Intellectual Property Issues in Cyberspace. | Quiz-2 |
| **UNIT V** | | | |
| 35. | 27/11/2025 | **Personal Cybersecurity, Privacy and Data Protection:** What is Personal Cybersecurity? | |
| 36. | 28/12/2025 | Common Causes of Personal Security Breaches, Personal Cybersecurity Best Practices, Privacy | |
| 37. | 02/12/2025 | Regulations and Cybersecurity, The Role of Ethics in Cybersecurity. | |
| 38. | 03/12/2025 | **Cybersecurity in Evolving Technology and Practice:** Future Challenges in Cybersecurity, Web 3.0 | |
| 39. | 04/12/2025 | Harnessing Artificial Intelligence for Cybersecurity, Blockchain for Cybersecurity | |
| 40. | 09/12/2025 | Quantum Computing and Cybersecurity, Combating Advanced Persistent Threats, Digital Trust and Identity Management | |
| 41. | 10/12/2025 | 5G Networks and Cybersecurity, Adopting a 'Secure-by-Design' Approach, | |
| 42. | 11/12/2025 | Supply Chain Cybersecurity, Other Evolving Aspects of Cybersecurity. | 8 Hrs |

**Text Books:**


| | |
|---|---|
| 1. | Ajay Singh, “Introduction to Cybersecurity: Concepts, Principles, Technologies and Practices”, University Press, First Edition, 2023. |


**Reference Books:**


| | |
|---|---|
| 1. | Henrique M. D. Santos, Cybersecurity - A Practical Engineering Approach, CRC Press, First edition, 2022. |
| 2. | William Stallings, Lawrie Brown, Computer Security Principles and Practice, Pearson ed., 5th edition, 2023. |
| 3. | Anas Zakir, Cyber security and Digital Forensics, Clever Fox Publishing, 2022 |

**Tutorials:**

| Date | Topic |
|---|---|
| 05/09/2025 | Use Wireshark to analyze network traffic, look for signs of malicious utilization. |
| 13/09/2025 | Explore Nmap Tool to discover and characterize (scanning) machines in a network. |
| 20/09/2025 | Explore Nessus/ OpenVAS to discover system vulnerabilities. |
| 27/09/2025 | Use of the Metasploit tool, to exploit the identified vulnerabilities. |
| 04/10/2025 | Employ cryptography techniques and tools to protect the information when it is in transit.<br>Explore artifacts that are useful while conducting a forensics investigation. Find where the artifacts are placed and extract valuable information out of them. |
| 08/11/2025 | Investigate techniques for detecting common web application attacks by analyzing logs from web applications and firewalls, identify the attack point, and trace the root cause by pinpointing the exploited vulnerability |
| 22/11/2025 | Experiment on Cracking Passwords<br>Performing SQL Injection on a Test Web Application |
| 13/12/2025 | To simulate a simple DoS attack and observe its impact on a target system or service |

## Important Dates to be remembered:

| Sl No | Important Events | Date |
|---|---|---|
| 1. | I – Test | 11-10-2025 , 18-10-2025, 25-10-2025 |
| 2. | Last date for dropping of course | 21-10-2025 |
| 3. | II – Test | 15-11-2025, 29-11-2025,06-12-2025 |
| 4. | Last date for withdrawal of course | 01-12-2025 |
| 5. | Last working day | 13-12-2025 |
| 6. | Preparation Holidays | 14-12-2025 to 19-12-2025 |
| 7. | Semester end examination | 20-12-2025 to 05-01-2026 |
| 8. | Announcement of results | 17-01-2026 |

## Activities to meet Teaching Learning Scheme:

| Sl. No. | Activity Planned | Number of Hours |
|---|---|---|
| 1. | Classroom Teaching | 42 |
| 2. | Formative Assessment [Test (2 No.) +Quiz (2 No.) + Semester End Exam] | 07 |
| 3. | Tutorials | 28 |
| 4. | Student Study Hours – Self Learning | 14 |
| 5. | **Activity Based Learning:**<br>**I. Demonstration of Cybersecurity Toolsv (09 Hours)**<br>1. Identification of Cybersecurity Tools- 2 Hours<br>2. Learning and Exploration of Cybersecurity Tool - 5 Hours<br>3. Demonstration of Cybersecurity Tool - 1 Hour<br>4. Report Preparation - 1 Hours<br>**II. Projects on Cybersecurity (20 Hours)**<br>1. Identifying areas in which students want to carry out the project by literature survey - 5 Hours.<br>2. Meeting and discussing (online or offline) with the faculty and fixing the problem statement- 2 Hours.<br>3. Designing and implementing the project - 12 Hours<br>4. Presentation and submitting the final report - 1 Hour.<br>**Total** | 29<br><br>120 |

**Course Outcomes: Upon completion of this course, the student will be able to:**

| | |
|---|---|
| **CO1** | **Describe** the need for information security and the evolution of models and principles governing information systems. |
| **CO2** | **Analyze** different forms of cybercrimes, ethical considerations, and apply strategies for cybercrime prevention and digital evidence handling. |
| **CO3** | **Identify** and **analyze** vulnerabilities in information systems such as applications, networks, cloud, and third-party ecosystems. |
| **CO4** | **Apply** cybersecurity strategies using best practices in risk management, policymaking, and incident response aligned with industry frameworks |
| **CO5** | **Apply** legal and ethical principles to real-world cybersecurity issues and assess emerging technologies and trends to strengthen cyber resilience. |

**Mapping of Course Outcomes (COs) to Program Outcomes (POs) & Program Specific Outcomes (PSOs)**

| Course outcomes | Pos | | | | | | | | | | | | PSOs | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 |
| CO1 | 3 | | | | | | | | | | | | | 2 | |
| CO2 | 3 | 3 | | | | | | | | | | | | 3 | |
| CO3 | 3 | 3 | | | | | | | | | | | | 2 | |
| CO4 | | | 2 | | | | | | | | | | | 3 | |
| CO5 | 3 | | | | | | | | | | | | | 2 | |
| CO (Average) | 3 | 3 | 2 | | | | | | | | | | | 3 | |

Degree of compliance **1**: Low **2**: Medium **3**: High

**Course delivery methods, assessment tools and sample questions:**

| | |
|---|---|
| **CO1** | **Describe** the need for information security and the evolution of models and principles governing information systems. |
| **Delivery Methods** | Blackboard Teaching, Power point Presentation |
| **Assessment Tools** | Tests, Quiz and SEE |
| **Sample Questions** | 1. Cyberspace is a safe heaven for cybercriminals. Discuss.<br>2. Explain the distinction between vulnerabilities and threats.<br>3. What is the CIA model? Does it need to be expanded further? If so why?<br>4. The nature of cyber risks is such that cybersecurity can never ensure total or perpetual immunity from them. If so, what is the purpose of cyber risk management?<br>5. Why is a risk-based approach regarded as the best way to address cybersecurity?<br>6. What are the advantages of implementing cybersecurity frameworks?<br>7. What considerations should an organization keep in mind while choosing a framework? |

| | |
|---|---|
| **CO2** | **Analyze** different forms of cybercrimes, ethical considerations, and apply strategies for cybercrime prevention and digital evidence handling. |
| **Delivery Methods** | Blackboard Teaching, Power point Presentation |
| **Assessment Tools** | Tests, Quiz, SEE and Assignments |
| **Sample Questions** | 1. Describe the types of common cyberattacks and the implications of such attacks.<br>2. Explain the three strategies to reduce risks from cyberattacks.<br>3. Explain the reasons for the growth of cybercrime and the efforts required for its containment.<br>4. Explain the working of any three types of malware.<br>5. Why is there a need for specific cybersecurity legislations? |

| | |
|---|---|
| **CO3** | **Identify** and **analyze** vulnerabilities in information systems such as applications, networks, cloud, and third-party ecosystems. |
| **Delivery Methods** | Blackboard Teaching, Power Point Presentation |
| **Assessment Tools** | Tests, Quiz, SEE and Assignments |
| **Sample Questions** | 1. Comment on the statement "software applications are the major sources of vulnerabilities"<br>2. Explain the importance and steps in the vulnerability assessment process.<br>3. How can poor password management and system administration practices be a source of vulnerabilities and what can be done to fix them?<br>4. The human element is widely regarded as the weakest link in cybersecurity. Explain with examples<br>5. Discuss the role of OWASP in identifying software vulnerabilities. |

| | |
|---|---|
| **CO4** | **Apply** cybersecurity strategies using best practices in risk management, policymaking, and incident response aligned with industry frameworks |
| **Delivery Methods** | Blackboard Teaching, Power Point Presentation |
| **Assessment Tools** | Tests, Quiz, SEE and Assignment |
| **Sample Questions** | 1. What is the purpose behind adopting industry-specific cybersecurity frameworks?<br>2. Discuss the principles of incident response.<br>3. What are the steps in a vulnerability assessment process?<br>4. Explain the Zero Trust model and its key principles.<br>5. Explain how policies and standards can guide cybersecurity implementation. |

| | |
|---|---|
| **CO5** | **Apply** legal and ethical principles to real-world cybersecurity issues and assess emerging technologies and trends to strengthen cyber resilience. |
| **Delivery Methods** | Blackboard Teaching, Power-point presentation |
| **Assessment Tools** | Tests and SEE |
| **Sample Questions** | 1. Explain the need and role of cyber laws in combating cybercrimes.<br>2. What is the role of governments in formulating cybersecurity regulations?<br>3. Explain the difference between a digital signature and a digital certificate.<br>4. Discuss how blockchain technology can be applied in cybersecurity.<br>5. What challenges exist in enforcing cyber laws across different countries?<br>6. Explain the importance of protecting intellectual property in cyberspace. |

S. Ramu
**Faculty**

03/9/25
**HOD**

8/9/25
**Principal**