DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

B.TECH (COMPUTER SCIENCE AND ENGINEERING-CYBER SECURITY)

(COLLABORATION WITH CYBER DOJO)

FOUR YEAR PROGRAM

CURRICULUM STRUCTURE & SYLLABI
(2025-2029 BATCH ONWARDS)

SCHOOL OF ENGINEERING AND TECHNOLOGY
MODY UNIVERSITY OF SCIENCE AND TECHNOLOGY
LAKSHMANGARH

B.Tech (CSE - Cyber Security)
(Collaboration with Cyber Dojo)
Four Year Program
Academic Curriculum (2025-2029 Batch Onwards)

Curriculum Components

Component	Credits
1. University Core (3 Courses)	6
2. University Elective (2 Courses)	6
3. Basic Science (9 Courses)	24
4. Engineering Science (9 Courses)	18
5. Program Core (36 Courses)	69
6. Program Elective / MOOCs (5 Courses)	21
7. Project / Summer Internship Project (7 Courses)	21
8. Proficiency (Non-Graded) (6 Courses)	6
Total	165

First Year - Autumn Semester

Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage			
		L	T	P			CW	MTE		ETE
UC 23.101	Human Values & Professional Ethics	2	0	0	2	3	10	40		50
MA 23.101	Mathematics I	3	1	0	4	3	10	40		50
ME 25.101	**Applied Mechanics**	**3**	**0**	**0**	**3**	**3**	10	40		50
EC 25.101	**Basics of Electronics Engineering**	**3**	**0**	**0**	**3**	**3**	10	40		50
CY 23.102	Environmental Sciences	2	0	0	2	3	10	40		50
CS 23.101	Programming for problem solving	3	0	0	3	3	10	40		50
CS 25.103	IT and Cyber Security Fundamentals	3	0	0	3	3	10	40		50
CS 23.111	Programming laboratory	0	0	4	2	2	50			50
ME 23.112	Mechanical Workshop	0	0	2	1	2	50			50
EC 23.111	Electronics Lab	0	0	2	1	2	**50**			**50**
PB 25.101	Project Based Learning	0	0	2	1		50			50
SF 101	Personal Grooming and Fine Dining(Non Grade)	0	0	2	1	2	50			50
	Total	19	1	12	**25**		100			

First Year -Spring Semester

Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration	Weightage			
		L	T	P			CW	MTE		ETE
UC 23.102	Pragmatic English Communication	2	0	0	2	3	10	40		50
MA 23.102	Mathematics-II	3	1	0	4	3	10	40		50
CY 23.101	Engineering Chemistry	3	0	0	3	3	10	40		50
PY 23.101	Engineering Physics	3	0	0	3	3	10	40		50
EE 25.101	**Basics of Electrical Engineering**	**3**	**0**	**0**	**3**	3	10	40		50
CS 25.113	Compliance & Data Protection	3	0	0	3	3	10	40		50
ME 23.111	Computer aided Engineering Drawing	0	0	4	2	2	**50**			**50**
CY 23.111	Chemistry Lab	0	0	2	1	2	**50**			**50**
EE 23.111	Electrical Laboratory	0	0	2	1	2	50			50
CS 25.114	Compliance & Data Protection Lab	0	0	2	1	2	**50**			**50**
PY 23.111	Physics laboratory	0	0	2	1	2	50			50
PB 25.102	**Project Based Learning**	**0**	**0**	**2**	**1**		**50**			**50**
SF 102	Social Grooming, Home & Decor and Business Communication (Non Grade)	0	0	2	1	2	50			50
	Total	17	1	16	**25**		100			

B.Tech (CSE - Cyber Security)
(Collaboration with Cyber Dojo)
Four Year Program
Academic Curriculum (2025-2029 Batch Onwards)

Second Year - Autumn Semester										
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage			
		L	T	P			CW	MTE	PBL	ETE
MA 23.201	Mathematics-III	3	1	0	4	3	10	40		50
CS 25.202	**Operating Systems Security**	3	0	0	3	3	10	40		50
CS 23.203	Data Structures	3	0	0	3	3	10	40		50
CS23.205	General Purpose Programming	3	0	0	3	3	10	40		50
CS25.207	**Networking from Security Perspective**	**3**	**0**	**0**	**3**	**3**	**10**	**40**		**50**
CS 23.253	Data Structures Lab	0	0	2	1	2	50			50
CS 23.255	General Purpose Programming laboratory	0	0	2	1	2	50			50
CS 25.257	**Operating Systems Security** Laboratory	0	0	2	1	2	50			50
CS 25.259	**Networking from Security Perspective Lab**	0	0	2	1	2	50			50
PB 25.201	**Project Based Learning**	**0**	**0**	**2**	**1**			**50**		**50**
SF 201	Personal Grooming Fine Dining and Home Safety (Non Grade)	0	0	2	1	2	50			50
	Total	15	1	12	**21**		100			

Second Year -Spring Semester										
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage			
		L	T	P			CW	MTE	PBL	ETE
UC 25.201	Management and Entrepreneurship	2	0	0	2	2	10	40		50
	University Elective-I	3	0	0	3	3	20			80
CS23.204	Database Management Systems	3	0	0	3	3	10	40		50
CS 23.202	Advanced Programming	3	0	0	3	3	10	40		50
CS 25.203	**Network Defence**	3	0	0	3	3	10	40		50
CS23.208	Computer Organization and Architecture	3	0	0	3	3	10	40		50
CS 25.204	**Network Analysis**	3	0	0	3	3	10	40		50
CS23.252	Advanced Programming Laboratory	0	0	2	1	2	20	50		50
CS23.254	Database Management Systems Laboratory	0	0	2	1	2	20	50		50
CS25.256	**Network Defense Lab**	0	0	2	1	2	20	50		50
CS25.258	**Network Analysis Lab**	0	0	2	1	2	20	50		50
PB 25.202	**Project Based Learning**	**0**	**0**	**2**	**1**			**50**		**50**
SF 202	Social Grooming and Professional Skills(Non Grade)	0	0	2	1	2	50			50
	Total	19	0	12	**25**		100			

Project Based Learning (PBL) in Group of 3-5 Students,

B.Tech (CSE - Cyber Security)
(Collaboration with Cyber Dojo)
Four Year Program
Academic Curriculum (2025-2029 Batch Onwards)

Third Year - Autumn Semester									
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage		
		L	T	P			CW	MTE	ETE
RM 23.101	Research Methodology	2	0	0	2	3	10	40	50
CS23.301	Design and Analysis of Algorithms	3	1	0	4	3	10	40	50
CS 25.303	**End Point Security**	3	0	0	3	3	10	40	50
CS 25.305	**Social Engineering & Network / Systems VA /PT**	3	0	0	3	3	10	40	50
CS 25.307	**Post Exploitation and Advanced Techniques**	3	0	0	3	3	10	40	50
CS23.351	Design and Analysis of Algorithms Laboratory	0	0	2	1	2	50		50
CS25.355	**End Point Security** Laboratory	0	0	2	1	2	50		50
CS25.353	**Social Engineering & Network / Systems VA /PT** Laboratory	0	0	2	1	2	50		50
	Post Exploitation and Advanced Techniques lab	0	0	2	1	2	50		50
CS 23.373	Summer Internship-I**	0	0	0	2		100		
CS 23.371	Project-1	0	0	4	2	2	-	50	50
GE 25.301	Proficiency (Non Credit, Non Grade)	-	-	-	1		100		
	Total	14	1	12	**23**		100		

Third Year -Spring Semester									
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage		
		L	T	P			CW	MTE	ETE
CS 23.302	Artificial Intelligence and Machine Learning	3	0	0	3	3	10	40	50
CS 25.304	**Web Application Security**	3	0	0	3	3	10	40	50
CS 25.306	**Incident Response & Redressal**	3	0	0	3	3	10	40	50
CS 25.309	**Threat Analysis and Security Operations Advanced**	3	0	0	3	3	10	40	50
CS 23.392	Colloquium	0	0	2	1	-	100		
CS 25.356	**Web Application Security Lab**	0	0	2	1	2	50		50
CS 25.357	**Incident Response & Redressal Lab**	0	0	2	1	2	50		50
CS 25.358	**Threat Analysis and Security Operations Advanced**	0	0	2	1	2	50		50
CS 25.359	Artificial Intelligence and Machine Learning lab	0	0	2	1	2	50		50
CS 23.372	Project-2	0	0	4	2	2	-	50	50
GE 25.302	Proficiency (Non Credit, Non Grade)	-	-	-	1		100		
	Total	12	0	14	**19**		100		

Proficiency (Non-Credit/Non Grade) shall be measured through level of participation in skill development programs i.e., sports, Yoga, Life skills, Music, Fine Arts,SEFS or or decided by Departmental academic Committee

B.Tech (CSE - Cyber Security)
(Collaboration with Cyber Dojo)
Four Year Program
Academic Curriculum (2025-2029 Batch Onwards)

Fourth Year - Autumn Semester									
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage		
		L	T	P			CW	MTE	ETE
UE	University Elective-II	3	0	0	3	3	20		80
CS 25.471	**Cloud Security**	3	0	0	3	3	10	40	50
CS 25.472	**IOT Security**	3	0	0	3	3	10	40	50
CS 25.473	**Cloud Security lab**	0	0	2	1	2	50		50
CS 25.474	**IOT Security Lab**	0	0	2	1	2	50		50
CS 23.473	Summer Internship-II**	0	0	0	2	-	100		
CS 23.471	Capstone Project-1	0	0	4	2	-	100		
	Total	9	0	8	**15**				

Fourth Year -Spring Semester									
Course Code	Course Title	Contact Hours Per Week			Credits	ETE Duration (Hours)	Weightage		
		L	T	P			CW	MTE	ETE
	Program Elective-1	3	0	0	3	3	10	40	50
	Program Elective-2	3	0	0	3	3	10	40	50
CS23.472	Capstone Project-2	0	0	12	6			50	50
	Total	6	0	12	**12**		100		

** Summer Internship-I & II must be performed in an Industry between summer vacation of end of Second Year and end of Third Year.

Credit Distribution across all Components								
Semester	**UC**	**UE**	**BS**	**ES**	**PC**	**PE**	**Proj/SIP**	**Total**
First	**2**	**0**	**10**	**5**	**8**	**0**	**1**	**26**
Second	**2**	**0**	**8**	**9**	**4**	**0**	**1**	**24**
Third	**0**	**0**	**4**	**4**	**15**	**0**	**1**	**24**
Fourth	**2**	**3**	**0**	**0**	**17**	**3**	**1**	**26**
Fifth	**0**	**0**	**2**	**0**	**13**	**3**	**4**	**22**
Sixth	**0**	**0**	**0**	**0**	**15**	**3**	**3**	**21**
Seventh	**0**	**3**	**0**	**0**	**0**	**6**	**4**	**13**
Eighth	**0**	**0**	**0**	**0**	**0**	**6**	**6**	**12**
Total	**6**	**6**	**24**	**18**	**72**	**21**	**21**	**165**

UC	**University Core**
UE	**University Elective**
BS	**Basic Science**
ES	**Engineering Science**
PC	**Program Core**
PE	**Program Elective / MOOC**
Proj/SIP	**Project/Summer Internship**

B.Tech (CSE - Cyber Security)
(Collaboration with Cyber Dojo)
Four Year Program
Academic Curriculum (2025-2029 Batch Onwards)

List of Program Elective Options

Program Elective 1	
CS 23.493	Foundations and Applications of IoT
CS 23.495	Principles and Practices of Secure Computing
CS 23.463	Agile Software Development (Infosys)**#**

Program Elective 2	
CS 23.494	Software Defined Networking
CS 23.464	Business Intelligence and its application (Infosys)
CS 23.465	Machine Learning using R (Infosys)**#**

Code	Industry Electives (Common to All Tracks)
CS 23.461	Cloud Computing (Infosys)
CS 23.462	Mobile App Development (Infosys)
	MOOC-1*
	MOOC-2*
	***Mooc-1 and Mooc-2 should be selected only in 7th and 8th Semester respectively from NPTEL with prior permission from Department** **#Courses included from 2021-22 session onwards**

B.Tech (CSE)-(2025-29) Batch Onwards

CS 25.113 **Compliance & Data Protection** **Total Lectures: 40**

Credit: 3-0-0-3

Prerequisite(s): Basic Knowledge of Cybersecurity, Familiarity with IT Governance and Regulatory Frameworks, Knowledge of Networking and Data Security, Basic Analytical Skills

Objective(s):

- Students will gain an understanding of compliance frameworks, industry standards, and regulatory requirements in cybersecurity.
- The course explores complex regulatory landscapes and cybersecurity challenges faced by organizations.
- Key standards covered include NIST, GDPR, ISO, SOC reports, HIPAA, PCI DSS, and CIS.
- Practical skills include risk assessment, program development, implementation of controls, policy creation, training, auditing, and vendor collaboration.
- Graduates will be prepared for roles such as Compliance Analyst, Security Consultant, and Risk Assurance Associate.

1	**Cybersecurity Compliance:** Importance of understanding compliance frameworks and industry standards, cybersecurity-related challenges commonly faced by the industry, compliance basics.	[10]
2	**Cybersecurity Frameworks & Standards:** Overview of the different cybersecurity standards commonly implemented in the industry: NIST, GDPR, ISO, SOC reports and auditor process overview, HIPAA, PCI DSS, CIS.	[10]
3	**Achieve & Maintain Cybersecurity Compliance:** Regulatory requirements, risk assessments, compliance program development, security controls, policy establishment, employee training, regular audits, vendor collaboration, monitoring and reporting.	[10]
4	**Organizational Implementation Strategies:** Internal policies and best practices for compliance, compliance team roles and responsibilities, compliance checklists and documentation, automation in compliance processes, training modules for organizational staff, periodic review processes.	[5]
5	**Career Roles and Evolving Trends in Compliance:** Real-world roles in cybersecurity compliance (e.g., Compliance Analyst, DPO, Regulatory Specialist), impact of global data protection laws, evolving regulatory trends, the role of AI and automation in compliance, certifications relevant to compliance careers (e.g., CISA, CISM, CIPM).	[5]

Outcome(s): On successful completion of this course, students will be able to

- Understand and apply compliance frameworks, industry standards, and regulatory requirements in cybersecurity.
- Address common organizational cybersecurity challenges and apply compliance-based solutions.
- Gain familiarity with cybersecurity standards like NIST, GDPR, ISO, HIPAA, PCI DSS, and CIS.
- Acquire practical skills in developing and maintaining cybersecurity compliance programs.
- Collaborate with stakeholders and apply continuous compliance improvement strategies. Identify, formulate, and solve data science related problems by applying principles of the course.

Text Books: CyberDojo Content through the LMS

Reference Books:

1. M. Whitman and H. Mattord, Principles of Information Security, Cengage Learning.
2. D. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards, Addison-Wesley.
3. J. Rittinghouse and J. Hancock, Cybersecurity Operations Handbook, Elsevier.
4. R. Kumar and A. Gupta, Compliance and IT Security for Beginners, BPB Publications.

B.Tech (CSE)-(2025-29) Batch Onwards

CS 25.103 **IT and Cyber Security Fundamentals** **Total Lectures: 40**

Credit: 3-0-0-3

Prerequisite(s): Basic Knowledge of IT and Computer Systems, , Awareness of Common Cyber Attacks

Objective(s):

- To understand the concept and importance of cyberspace and the foundational principles of cybersecurity.
- To understand the definitions of various types of cyber threats, vulnerabilities, and security challenges.
- Basic Understanding of common cybercrimes and have basic understanding of the tools and techniques used in such activities.
- To understand the basics of network, mobile, and wireless security, including associated risks and protective mechanisms.

1	**Understanding of IT Concepts:** Understand the basics of hardware and operating systems, Networking Fundamentals, types of software, basics of software installation & maintenance, Develop Basic problem solving skills,	[5]
2	**Introduction to Cyber Security:** What is Cyber Security & Its importance, definition and challenges in Cyber Security, Key terminologies in Cyber Security, Cyber threats, vulnerability and risk, types of attack: active attacks, passive attacks, motives of attackers, layers of security, CIA Triad, types of security attacks, security services and mechanisms.	[5]
3	**Cyber Crime & Basic understanding of Tools Used in Cyber Crime:** Cybercrime and its types, introduction to concepts of proxy servers and anonymizers, phishing, password cracking, keyloggers and spywares, virus and worms, Trojan horses and backdoors. Introduction and definition of steganography, DoS and DDoS attacks, SQL injection, buffer overflow, attacks on wireless networks, phishing and identity theft.	[10]
4	**Introduction to Network Security, Mobile and Wireless Devices: Introduction to** Network and computer security, Basic of threats to network security, Introduction to security tools, elements of network security, mobile/wireless device proliferation, ,Basics of laptop & Mobile security.	[10]
5	**Real-world Applications:** Overview of real-world cybersecurity scenarios, incident response strategies, importance of cybersecurity awareness and training, introduction to cybersecurity frameworks (e.g., NIST, ISO 27001), role of SOC (Security Operations Center), introduction to certifications (CEH, CISSP), and current trends.	[10]

Outcome(s): On successful completion of this course, students will be able to

- Understand IT Fundamentals, cyberspace, cybersecurity fundamentals, threats, and risks.
- Basic Understanding of cyber-attacks, motives, and layered security.
- Basic Understanding of cybercrime types and tools including malware, phishing, and keyloggers.
- Understanding of real world cyber threats and attacks
- Understanding on career opportunities and skill requirements in Cyber Security

Text Books:

1. CyberDojo Content Through LMS.

Reference Books:

1. Bhushan, Rathore et al. Fundamental of Cyber Security (Principles, Theory & Practices), BPB Publications, I Ed New Delhi. ISBN 978-9386551559

2. Anand Shinde , Introduction to Cyber Security : Guide to the World of Cyber Security Paperback. Notion Press, I Ed. ISBN 978-1637816424

CS 25.114 **Compliance & Data Protection Laboratory** **Total Hours: 26**
Credit: 0-0-2-1

Prerequisite: Basic Knowledge of Cybersecurity, Familiarity with IT Governance and Regulatory Frameworks, Knowledge of Networking and Data Security, Basic Analytical Skills

Objectives: The objective of this course is to:

- To understand and apply cybersecurity compliance frameworks (e.g., NIST, ISO 27001, GDPR) by performing hands-on activities such as risk assessments, control mapping, and compliance audits using sample organizational scenarios.
- To simulate real-world compliance tasks, including drafting security policies, creating audit checklists, and configuring security controls on systems, with an emphasis on aligning technical implementations to regulatory requirements.

Contents:

- Introduction to Compliance Frameworks (ISO 27001, GDPR, HIPAA, PCI-DSS)
- Data Classification and Handling: Confidential, Public, Restricted, etc.
- Setting File & Folder Permissions on Windows and Linux Systems
- Configuring and Auditing Access Control Lists (ACLs)
- Data Encryption at Rest using BitLocker (Windows) and LUKS (Linux)
- Data in Transit Protection using SSL/TLS – Wireshark vs HTTPS
- Data Loss Prevention (DLP) Concepts and Simulated Policy Enforcement
- Logging, Monitoring & Audit Trails – Enabling and Reviewing Security Logs
- Simulating a Compliance Audit: Evidence Gathering & Gap Identification
- Incident Response Lab – Reporting a Data Breach with Compliance Context (GDPR,
- HIPAA, etc.)

Outcomes: Upon completion of this course, students are able to:

- Demonstrate the ability to map organizational policies and technical controls to recognized cybersecurity compliance standards such as NIST, GDPR, and ISO 27001.
- Perform basic compliance assessments by identifying gaps, drafting mitigation strategies, and documenting findings in audit-ready formats.
- Develop and implement security policies and procedures that support regulatory compliance, including access control, data protection, and incident response.