MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WEST BENGAL
(Formerly West Bengal University of Technology)
Syllabus of B.Sc. in Cyber Security
(Effective from 2023-24 Academic Sessions)

Learning Outcome :

LO No.	Learning Outcome
LO1	**Cyber Security Knowledge:** Apply foundational and advanced knowledge of cyber security, networking, cryptography, operating systems, and computing principles to identify and solve security-related problems.
LO2	**Design/Development of Solutions:** Design, develop, and implement secure cybersecurity solutions, tools, and applications to address real-world security challenges using appropriate technologies and methodologies.
LO3	**Cyber Security Professional and Society:** Analyze the impact of cyber security solutions on society, ethics, law, privacy, and professional responsibilities while ensuring secure and responsible computing practices.
LO4	**Individual and Team Work:** Function effectively as an individual, team member, or team leader in multidisciplinary and collaborative cyber security environments.
LO5	**Communication:** Communicate effectively through technical reports, presentations, documentation, and professional discussions with technical and non-technical stakeholders.
LO6	**Life-Long Learning:** Recognize the need for continuous professional development and engage in lifelong learning to adapt to emerging cyber security technologies, threats, and industry practices.

Semester VII

Minor Project

Credit-5 credits
Course Code: FYCYS 781

CO No.	Course Outcome	BL	LO
CO1	Analyze real-world cyber security problems and identify appropriate methodologies and technologies for project implementation.	L4	LO1, LO3
CO2	Evaluate system requirements, security risks, and feasibility aspects for designing secure and efficient project solutions.	L5	LO1, LO2
CO3	Design and develop cyber security applications or systems integrating appropriate tools, technologies, and security mechanisms.	L6	LO2, LO4
CO4	Assess project performance, testing methodologies, security compliance, and implementation effectiveness through evaluation and validation techniques.	L5	LO3, LO6
CO5	Develop technical reports, project documentation, presentations, and demonstrations following professional and ethical standards.	L6	LO4, LO5, LO6

Project Module Structure

Module No.	Module Title & Activities	CO Mapping	BL
Module 1	Problem Identification and Literature Survey: Selection of project domain, identification of problem statement, literature review, requirement analysis, objective formulation and project planning.	CO1	L4
Module 2	System Design and Feasibility Analysis: Design of architecture, workflow diagrams, database design,	CO2	L5

	security analysis, feasibility study and technology selection.		
Module 3	Project Development and Implementation: Coding, module integration, configuration, implementation of security mechanisms and development of project components.	CO3	L6
Module 4	Testing, Validation and Performance Evaluation: Functional testing, vulnerability assessment, debugging, performance analysis, security evaluation and optimization.	CO4	L5
Module 5	Documentation, Presentation and Demonstration: Preparation of technical report, project documentation, presentation, viva-voce and final project demonstration.	CO5	L6
Total			

Network Security with AI

Credit- 4+1 credits

Course Code- FYCYS 701

CO No.	**Course Outcome**	**BL**	**LO**
CO1	Analyze network security principles, Linux operating system architecture, and common cyber threats affecting network infrastructures.	L4	LO1, LO3
CO2	Evaluate Linux-based networking services, access control mechanisms, and firewall configurations for secure system administration.	L5	LO1, LO2
CO3	Design and implement secure network configurations, intrusion detection mechanisms, and encrypted communication systems using Linux tools.	L6	LO2, LO4
CO4	Assess network vulnerabilities, attack vectors, and security monitoring techniques for incident detection and mitigation.	L5	LO3, LO6
CO5	Develop practical Linux-based network security solutions using scripting, monitoring, and penetration testing utilities for real-world applications.	L6	LO2, LO4, LO5

Theory Module Structure

Module No.	**Module Title & Topics**	**CO Mapping**	**BL**
Module 1	**Security in Computing Environment** Need for Security, Security Attack, Security Services, Information Security, Methods of Protection. Terminologies used in Cryptography, Substitution Techniques, Transposition Techniques.	CO1	L4
Module 2	**Encryption and Decryption** Characteristics of Good Encryption Technique, Properties of Trustworthy Encryption Systems, Types of Encryption Systems, Confusion and Diffusion, Cryptanalysis. Data Encryption Standard (DES) Algorithm, Double and Triple DES, Security of the DES, Advanced Encryption Standard (AES) Algorithm, DES and AES Comparison. Characteristics of Public Key System, RSA Technique, Key Exchange, Diffie-Hellman Scheme, Cryptographic Hash Functions, Digital Signature, Certificates, Certificate Authorities.	CO2	L5

Module 3	**Network Security** Network Concepts, Threats in Networks, Network Security Controls. Overview of IP Security (IPSec), IP Security Architecture, Modes of Operation, Security Associations (SA), Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange.	CO3, CO4	L5
Module 4	**Web Security** Web Security Requirements, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Electronic Transaction (SET). Threats to E-Mail, Requirements and Solutions, Encryption for Secure E-Mail, Secure E-Mail System. Firewalls – Types, Comparison of Firewall Types, Firewall Configurations	CO4	L5
Total			

Tutorial Module Structure

Module No.	Practical Module	CO Mapping	BL
Module 1	**Linux Fundamentals and System Administration:** Linux installation, shell commands, user/group management, file permissions, process management, and scripting basics.	CO1	L4
Module 2	**Linux Network Configuration and Services:** IP configuration, routing, DNS, DHCP, SSH, FTP, web server configuration and service management.	CO2	L5
Module 3	**Firewall and Intrusion Detection Mechanisms:** Firewall configuration using IPtables, packet filtering, VPN setup.	CO3	L6
Module 4	**Network Monitoring and Vulnerability Assessment:** Packet analysis using Wireshark, vulnerability scanning using Nmap, log analysis, and security auditing.	CO4	L5
Module 5	**Security Automation and Mini Project:** Shell scripting for automation, penetration testing basics, Linux-based security mini project, and documentation.	CO5	L6
Total			

Secure Software Design and Development

Credit- 3+1 credits

Course Code- FYCYS 702

CO No.	Course Outcome	BL	LO
CO1	Analyze secure software development lifecycle models, web application architectures, and common security vulnerabilities in software systems.	L4	LO1, LO3
CO2	Evaluate authentication, authorization, secure coding practices, and web security mechanisms for secure application development.	L5	LO1, LO2
CO3	Design and implement secure web applications incorporating encryption, session management, and API protection strategies.	L5	LO2, LO4

CO4	Assess software vulnerabilities, web attacks, and security testing methodologies for secure deployment and maintenance.	L5	LO3, LO6
CO5	Develop secure software solutions using modern security tools, testing frameworks, and collaborative development practices.	L6	LO2, LO4, LO5

Theory Module Structure

Module No.	Module Title & Topics	CO Mapping	BL
Module 1	**Introduction:** Defining computer security, the principles of secure software, trusted computing base, etc, threat modelling, advanced techniques for mapping security requirements into design specifications. Secure software implementation, deployment and ongoing management.Software design and an introduction to hierarchical design representations. Difference between high-level and detailed design. Handling security with high-level design. General Design Notions. Security concerns designs at multiple levels of abstraction, Design patterns, quality assurance activities and strategies that support early vulnerability detection, Trust models, security Architecture & design reviews	CO1	L4
Module 2	**Software Assurance Model:** Identify project security risks & selecting risk management strategies, Risk Management Framework, Security Best practices/ Known Security Flaws, Architectural risk analysis, Security Testing & Reliability (Penn testing, Risk-Based Security Testing, Abuse Cases, Operational testing , Introduction to reliability engineering, software reliability, Software Reliability approaches, Software reliability modelling.	CO2	L5
Module 3	**Software Security in Enterprise Business:** Identification and authentication, Enterprise Information Security, Symmetric and asymmetric cryptography, including public key cryptography, data encryption standard (DES), advanced encryption standard (AES), algorithms for hashes and message digests. Authentication, authentication schemes, access control models, Kerberos protocol, public key infrastructure (PKI), protocols specially designed for ecommerce and web applications, firewalls and VPNs. Management issues, technologies, and systems related to information security management at enterprises.	CO3	L6
Module 4	**Security development frameworks:** Security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and e-service systems, as well as the technologies required to develop secure information systems for enterprises, policies and regulations essential to the security of enterprise information systems. Vulnerability assessment, penetration testing basics, static and dynamic code analysis, secure DevOps concepts, cloud application security, container security and emerging software security trends.	CO4, CO5	L6

Total			

Tutorial Module Structure

Module No.	Practical Module	CO Mapping	BL
Module 1	**Secure Development Environment Setup:** Installation and configuration of web servers, IDEs, secure coding environment, version control basics and secure project setup.	CO1	L4
Module 2	**Implementation of Secure Coding Practices:** Input validation, password hashing, session handling, authentication and authorization mechanisms.	CO2	L5
Module 3	**Secure Web Application Development:** HTTPS configuration, SSL/TLS implementation, secure APIs, token-based authentication and secure database integration.	CO3	L6
Module 4	**Security Testing and Vulnerability Assessment:** Static and dynamic analysis tools, vulnerability scanning, penetration testing basics, web application testing.	CO4	L5
Module 5	**Secure Software Mini Project:** Development and documentation of a secure web application implementing secure coding standards and security testing methodologies.	CO5	L6
Total			

Semester VIII

Governance, Risk and Compliance

Credit- 4+1 credits

Course Code- FYCYS 801

CO No.	Course Outcome	BL	LO
CO1	Analyze governance frameworks, organizational policies, and risk management principles for secure and compliant information systems.	L4	LO1, LO3
CO2	Evaluate governance architectures, compliance requirements, business process frameworks, and organizational preparedness strategies.	L5	LO1, LO2
CO3	Design governance and compliance solutions integrating privacy, security, cloud technologies, and organizational controls.	L6	LO2, LO4
CO4	Assess international governance models, regulatory standards, ISO frameworks, and organizational compliance mechanisms.	L5	LO3, LO6
CO5	Develop governance, risk, and compliance strategies using auditing, monitoring, reporting, and modern enterprise technologies for organizational security management.	L6	LO2, LO4, LO5

Theory Module Structure

Module No.	Module Title & Topics	CO Mapping	BL

Module 1	**Fundamentals of Governance, Risk and Compliance:** Governance policies, strategies and frameworks, information society concepts, ICT in organizational governance, technology and society, governance models, globalization, business information systems and business process re-engineering.	CO1	L4
Module 2	**Governance Architecture and Organizational Frameworks:** Planning and implementation of governance frameworks, legal frameworks, enterprise architecture development, public administration models, change management, capacity building, infrastructure preparedness, leadership and strategic planning.	CO2	L5
Module 3	**Governance Technologies, Security and Compliance:** Virtual environments, information management, digital archiving, data exchange systems, ethics of technology, privacy and security in networked environments, IoT security, cloud technologies and software/database protection mechanisms.	CO3	L6
Module 4	**Global Governance Models and Compliance Standards:** Comparative study of governance models across countries, governance maturity models, compliance gaps, international governance case studies and organizational governance frameworks.	CO4	L5
Module 5	**Governance Services, Regulatory Standards and ISO Frameworks:** National digital governance initiatives, governance services and portals, auditing frameworks, compliance monitoring and ISO standards including ISO/IEC 27001, ISO/IEC 27005, ISO 31000 and ISO 22301.	CO4, CO5	L5, L6
Total			

Tutorial Module Structure

Module No.	**Practical Module**	**CO Mapping**	**BL**
Module 1	**Governance Framework Analysis:** Study and analysis of organizational governance structures, policy documentation, governance frameworks and business process models.	CO1	L4
Module 2	**Risk and Compliance Assessment:** Risk identification, compliance evaluation, audit preparation, governance reporting and regulatory assessment exercises.	CO2	L5
Module 3	**Security, Privacy and Cloud Governance:** Configuration and analysis of cloud governance mechanisms, privacy controls, access management and IoT security assessment.	CO3	L6
Module 4	**ISO Standards and Governance Auditing:** Practical implementation of ISO/IEC 27001 controls, ISO 31000 risk assessment techniques and compliance auditing exercises.	CO4	L5

Module 5	**GRC Mini Project and Case Study:** Development of governance and compliance framework for an organization including risk analysis, reporting dashboards and audit documentation.	CO5	L6
Total			

Cloud Security

Credit- 5 credits

Course Code- FYCYS 802

CO No.	Course Outcome	BL	LO
CO1	Analyze cloud computing architectures, deployment models, and cloud service frameworks for secure enterprise applications.	L4	LO1, LO3
CO2	Evaluate cloud security threats, vulnerabilities, privacy issues, and risk management approaches in cloud infrastructures.	L5	LO1, LO2
CO3	Design secure cloud-based systems implementing identity management, access control, encryption, and monitoring mechanisms.	L6	LO2, LO4
CO4	Assess cloud governance models, compliance standards, auditing mechanisms, and regulatory frameworks for secure cloud operations.	L5	LO3, LO6
CO5	Develop secure cloud infrastructure solutions using virtualization, automation, and cloud security best practices for real-world applications.	L6	LO2, LO4, LO5

Theory Module Structure

Module No.	Module Title & Topics	CO Mapping	BL
Module 1	**Fundamentals of Cloud Computing and Architectures:** Cloud computing concepts, cloud service models (IaaS, PaaS, SaaS), deployment models, virtualization, cloud architectures, standards, protocols and best practices for cloud-based enterprise IT services.	CO1	L4
Module 2	**Cloud Security Threats and Risk Management:** Cloud threats, vulnerabilities, privacy issues, risk assessment, attack vectors, security challenges in public, private and hybrid cloud environments.	CO2	L5
Module 3	**Cloud Security Controls and Safeguards:** Security principles for cloud systems, encryption, identity and access management (IAM), authentication, authorization, monitoring, auditing and secure cloud communication mechanisms.	CO3	L6
Module 4	**Secure Cloud Infrastructure Design:** On-demand computing, elasticity, shared resources, resource allocation, network security, storage security, virtualization security and secure cloud architecture design principles.	CO3, CO4	L5
Module 5	**Cloud Governance, Compliance and Emerging Trends:** Industry security standards, audit policies,	CO4, CO5	L6

	regulatory mandates, compliance requirements, cloud governance frameworks, secure DevOps, container security and future trends in cloud security.		
Total			

Tutorial Module Structure

Module No.	Practical Module	CO Mapping	BL
Module 1	**Cloud Environment Setup and Virtualization:** Installation and configuration of virtualization tools, creation of virtual machines, cloud deployment models and cloud service setup.	CO1	L4
Module 2	**Cloud Security Threat Analysis and Risk Assessment:** Identification of cloud vulnerabilities, risk analysis, cloud attack simulations and security assessment techniques.	CO2	L5
Module 3	**Identity Management and Data Protection in Cloud:** Configuration of IAM policies, authentication mechanisms, access control, encryption techniques and secure cloud storage.	CO3	L6
Module 4	**Cloud Monitoring, Auditing and Compliance:** Cloud monitoring tools, log management, auditing mechanisms, security compliance verification and cloud governance implementation.	CO4	L5
Module 5	**Secure Cloud Deployment and Mini Project:** Secure cloud infrastructure deployment, container and virtualization security, cloud automation and mini project on secure cloud application development.	CO5	L6
Total			

Course Code: FYCYS 881

Course Name: Industry Capstone Project
Course Type: Sessional
Credits: 12

CO Code	Course Outcomes	Bloom's Taxonomy Level	LO Mapping
CO1	Identify and analyze real-world industry problems using data science, artificial intelligence, and analytical techniques to develop feasible solutions.	L4	LO1, LO2
CO2	Apply appropriate data collection, experimentation, statistical analysis, and AI/ML methodologies to execute industry-oriented projects effectively.	L3	LO1, LO2, LO3
CO3	Develop and implement data-driven models, prototypes, products, or intelligent systems using modern AI and data science tools and technologies.	L6	LO2, LO3
CO4	Evaluate project outcomes with respect to reliability, reproducibility, ethical considerations, sustainability, and professional standards in	L5	LO4, LO6

	industry practices.		
CO5	Prepare professional technical reports, scholarly outputs, and project documentation following academic integrity, ethical guidelines, and publication standards.	L6	LO4, LO5
CO6	Demonstrate effective communication, presentation, teamwork, and defense of project findings through technical presentations and viva voce examinations.	L3	LO5, LO6

Rubric for Academic Project

S. No.	Assessment Parameter	Marks	Sub-components
1.	Completion of Experimentation / Fieldwork/ Data collection and Analysis	40	Quality, reproducibility, adequacy, and reliability of data or field observations
2.	Final Report Submission: Aim, Review of Literature, Objectives, Methodology, Results, Conclusions, Discussion, Further Scope of Research	80	Proper referencing, similarity index upto 10%, AI-generated content upto 20%, academic integrity, and adherence to ethical standards
3.	Recommendations and submission of any one Scholarly Output as listed below:	40	** Marks to be followed based on the outcomes.
	**Research Publication	30-40	
	**Book / Book Chapter Publication	20-40	
	** Prototype / Product /Patent	20-40	
	** Other Scholarly Work	Upto 30#	# Students can secure at the maximum 30 marks out of 40 under 'other scholarly work'.
	** Draft Policy formulation$	20-40	
4.	End-Term Presentation and Viva Voce	80	Presentation skills (20) + Viva voce (60) demonstrating understanding, defense of findings, and readiness for scholarly discourse

$: to be considered under Academic Projects

For students pursuing the Academic Project Track

Students pursuing the Academic Projects track must fulfil the following requirements by the end of Semester VIII:

1. **Completion of Research Activities**: Successful completion of experimentation, fieldwork, data collection, data analysis, or any equivalent academic and research tasks initiated in Semester VII.
2. **Final Report Submission**: Submission of the final Dissertation or Academic Project Report in the prescribed format.
3. **Research Outcomes**: Each student must provide evidence of **at least one [3(a-d)]** of the following scholarly outcomes:
    a. **Research Publication**: Publication in Scopus / Web of Science indexed journals or in any other reputed journal approved by the University. In case the publication is in the process then a proof of communication from the Editor / Editor-in-Chief indicating that the manuscript has been considered for review or is under consideration, should be submitted by the student. / **OR**
    b. **Book / Book Chapter Publication**: A Book or Book Chapter bearing an ISBN number must be published by a reputed publisher. In case the publication is still in process, the student must submit an official acceptance letter from the Editor / Publisher clearly stating that the manuscript has been accepted and is under consideration for publication. / **OR**

c. **Prototype / Product / Patent**: Development of a prototype or product or filing of a patent based on the research work. / **OR**

d. Any other scholastic work (any one of the following two):

   i. Paper or poster presentation related to the research topic at a recognized National or International Conference / Seminar. **/OR**

   ii. Participation in International / National / State level Hackathons, Exhibitions, or Entrepreneurship platforms to showcase the work.