GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Integrated MSc, 8th Semester
Branch: Computer Science
Subject Name: Cyber Security Administration and Management
Subject Code: 1380306

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	**Introduction to Cybersecurity Management:** Cybersecurity fundamentals - Confidentiality, integrity, availability. The role of cybersecurity in the organization. Cyber threats, vulnerabilities, and attack vectors. The importance of governance in cybersecurity, developing a cybersecurity strategy, Aligning security strategies with business goals.	04	20
2	**Risk Management and Compliance:** Risk Management Frameworks - Identifying and assessing risks in IT environments. Implementing risk management frameworks (NIST, ISO 27005). Risk mitigation strategies. Compliance and Regulatory Standards - Overview of global regulatory standards (GDPR, HIPAA, PCI-DSS, ISO 27001). Legal and ethical aspects of cybersecurity. Implementing policies to ensure compliance.	07	20
3	**Security Administration:** Security Policies and Procedures - Developing security policies and standard operating procedures (SOPs). Creating an Incident Response Plan (IRP). Access control policies and identity management. • Security Infrastructure Management - Administering firewalls, intrusion detection/prevention systems (IDS/IPS), and network security tools. Secure configuration management. Managing encryption and VPN technologies	07	20
4	**Incident Management and Response:** • Cyber Incident Response - Incident detection, analysis, and prioritization. Creating and managing an incident response team. • Tools and techniques for effective incident handling.	07	20

	• Disaster Recovery and Business Continuity - Business Continuity Planning (BCP) fundamentals. Disaster recovery strategies. • Post-incident review and documentation.		
5	**Emerging Trends and Technologies in Cybersecurity** • Cloud Security Management - Securing cloud environments and SaaS platforms. Cloud security frameworks (CSA, NIST). Identity and Access Management (IAM) in the cloud. • Cybersecurity in Emerging Technologies - Securing IoT and mobile devices. Blockchain and cybersecurity applications. Artificial Intelligence and Machine Learning in cybersecurity.	07	20

Reference Books:

1. Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman
2. Managing Risk in Information Systems" by Darril Gibson
3. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up" by Evan Wheeler
4. The CISO Handbook: A Practical Guide to Securing Your Company" by Randal Nash
5. Information Security Management Principles" by David Alexander, Amanda Finch, David Sutton

Course Outcome:

By the end of the course, students will be able to:

1. Understand cyber security governance and risk management strategies that align with organizational goals and regulatory requirements.
2. Understand the security policies and incident response plans, managing security resources effectively.
3. Analyze and respond to cybersecurity incidents, implementing recovery and continuity strategies for minimizing business disruptions.
4. Understand the role of cybersecurity teams and handling organizational security audits.
5. Adapt to emerging cyber security technologies and trends, ensuring the secure deployment of cloud, IoT, and AI systems.

****