M.Sc. - Cyber Security

PROGRAM DETAILS

Faculty	Computing and IT (FCIT)
School	School of Computer Science (SCS)
Program	M.Sc - Cyber Security
Dean of Faculty	Dr. Shweta Marigoudar
Director of School	Ms. Shamina Attar

1	**Title of the Award**	M.Sc. - Cyber Security
2	**Modes of Study**	Full Time
3	**Awarding Institution /Body**	GM University
4	**Joint Award**	Not Applicable
5	**Teaching Institution**	GM University
6	**Date of Program Specifications**	November -2023
7	**Date of Course Approval by the Academic Council of GMU**	---
8	**Next Review Date:**	---
9	**Program Approving Regulating Body and Date of Approval**	---
10	**Program Accredited Body and Date of Accreditation**	---
11	**Grade Awarded by the Accreditation Body**	---
12	**Program Accreditation Validity**	---
13	**Program Benchmark**	N/A
14	**Program Overview- MSc-Cyber Security** The Master of Science program specializing in Cybersecurity is designed to equip students with advanced knowledge and skills to address the evolving challenges in the realm of digital security. This comprehensive program encompasses a multidisciplinary approach, integrating principles of computer science, cryptography, risk management, and ethical hacking. Students will engage in a rigorous curriculum covering topics such as network security, threat detection and response, and the legal and ethical aspects of cybersecurity. Emphasizing hands-on experience, the program enables students to develop practical skills in securing systems and networks through simulated exercises and real-world scenarios. The curriculum	

	is continually updated to reflect the latest threats and technologies in the rapidly evolving field of cyber security, ensuring graduates are well-prepared to tackle emerging challenges. Collaborative learning is fostered through group projects, encouraging students to work together to develop and implement effective cyber security strategies. Faculty members, often seasoned professionals in the field, guide students in applying theoretical knowledge to practical scenarios. The program also incorporates industry partnerships and internship opportunities, providing students with exposure to the latest tools and methodologies used in the cybersecurity landscape. Upon completion of the program, graduates emerge with a deep understanding of cybersecurity principles, ethical hacking techniques, and risk management strategies, positioning them as adept professionals ready to safeguard digital assets and contribute to the ongoing efforts in securing information systems.
15	**Program Educational Objectives (PEOs) for MSc- Cyber Security:** **1. Advanced Cybersecurity Expertise:** Graduates of the Master of Science program specializing in Cybersecurity will possess advanced expertise in the field, demonstrated through a deep understanding of cybersecurity principles, methodologies, and the ability to implement effective security measures to protect information systems. **2. Innovation and Adaptability:** The program aims to foster graduates' ability to innovate and adapt to evolving cybersecurity threats. Graduates will be equipped to stay abreast of emerging technologies, vulnerabilities, and attack vectors, enabling them to proactively address and mitigate cyber threats in diverse and dynamic environments. **3. Ethical and Responsible Cybersecurity Practices:** Graduates will exhibit a commitment to ethical and responsible cybersecurity practices. This involves understanding the legal and ethical considerations of cybersecurity, adhering to professional codes of conduct, and promoting cybersecurity measures that align with broader ethical standards and societal expectations.
16	**Program Outcomes for MSc-Cyber Security:** **1. Cybersecurity Fundamentals:** Graduates will demonstrate a comprehensive understanding of the fundamental principles of cybersecurity, including knowledge of encryption, access controls, and security protocols. **2. Threat Detection and Incident Response:** Graduates will be proficient in identifying and responding to cybersecurity threats, demonstrating the ability to detect and mitigate security incidents promptly and effectively.

	3. **Secure Network Design and Management:** Graduates will possess expertise in designing and managing secure network architectures, ensuring the confidentiality, integrity, and availability of digital assets within organizational networks. 4. **Ethical Hacking and Penetration Testing:** Graduates will be skilled in ethical hacking and penetration testing, conducting thorough assessments of system vulnerabilities to proactively identify and address potential security risks. 5. **Security Policy Development and Compliance:** Graduates will have the ability to develop and implement security policies and practices that comply with industry standards, legal regulations, and organizational requirements. 6. **Risk Management and Cybersecurity Governance:** Graduates will demonstrate proficiency in assessing and managing cybersecurity risks, understanding the governance structures that support effective cybersecurity practices within organizations. 7. **Cybersecurity Research and Innovation:** Graduates will engage in research activities, contributing to the advancement of cybersecurity knowledge and innovative solutions to emerging threats and challenges in the field. 8. **Effective Communication in Cybersecurity:** Graduates will be able to communicate complex cybersecurity concepts clearly and effectively to both technical and non-technical stakeholders, facilitating informed decision-making and collaboration within organizations.
17	**Program Specific Outcomes (PSOs) for MSc-Cyber Security:** 1. **Advanced Threat Hunting and Forensics:** Program-specific outcomes include the ability of graduates to conduct advanced threat hunting and forensic analysis, demonstrating expertise in identifying and investigating sophisticated cyber threats to support incident response and digital forensics. 2. **Security Architecture Design and Evaluation:** Graduates will showcase program-specific outcomes related to designing and evaluating security architectures, demonstrating the capacity to develop robust and scalable security frameworks tailored to organizational needs and evolving threat landscapes. 3. **Red Team Operations and Simulation:** Program-specific outcomes will encompass graduates' proficiency in executing red team operations and simulations. This involves the application of offensive security techniques to assess and enhance an organization's defensive capabilities, ensuring graduates are adept at simulating real-world cyber-attack scenarios.

18. Credit Requirements

- To complete a Postgraduate Program- M.Sc., a student is required to earn 80 credits
- Those students who successfully complete only course work (40 Credits) Postgraduate Diploma is awarded
- The credit distribution for M.Sc. Program:

Course Work – 16 X 3 Credits =	49 Credits
Course Work Lab – 5 X 2 Credits =	10 Credits
Research Work – 1 X 6 Credits =	06 Credits
Capstone Project =	08 Credits
Internship =	07 Credits
Total	**80 Credits**

19. Programme Structure

S. No.	Semester	Course Code	Course Title	Credits
1	1	PC25CY5101	Digital Forensic Fundamentals	3
2		PC25CY5102	Digital Forensic Lab	2
3		PC25CY5103	Ethical Hacking and Penetration Testing	3
4		PC25CY5104	Ethical Hacking Lab	2
5		PC25CY5105	Advanced Network Security with AI	3
6		PC25CY5106	Cryptography Foundation	3
7		PC25CY5107	Research Methodology & Ethics	3
Total				**19**
Break				
S. No.	**Semester**	**Course Code**	**Course Title**	**Credits**
1	2	PC25CY5201	Big Data Analytics for Security	3
2		PC25CY5202	Big Data Analytics for Security Lab	2
3		PC25CY5203/ PC25CY5204	**Elective – I**	3
4		PC25CY5205	Python Programming for Cyber Security	3
5		PC25CY5206	Python Programming for Cyber Security Lab	2
6		PC25CY5207	AI & Machine Learning for Cyber Security	3
7		PC25CY5208	Digital Evidence Analysis	3
8		PC25CY5209	Cloud Security and Virtualization	3
Total				**22**
Break				

S. No.	Semester	Course Code	Course Title	Credits
1	3	PC25CY6301	Malware Analysis and Reverse Engineering with Integrated Lab	4
2		PC25CY6302	Advanced Digital Forensics with AI	3
3		PC25CY6303	Advanced Digital Forensic Lab	2
4		PC25CY6304/ PC25CY6305	**Elective – II**	3
5		PC25CY6306	International Cyber Law and Regulation	3
7		PC25CY6307	Internship	7
Total				**22**

S. No.	Semester	Course Code	Course Title	Credits
1	4	PC24CY6401	IOT Security and Mobile Forensics	3
2		PC24CY6402	Capstone Project	8
3		PC24CY6403	Research Paper Publication	6
Total				**17**

List of **Elective – I** Offered:

1. Cyber Threat and Modelling
2. Security Policy and Audit

List of **Elective – II** Offered:

1. Artificial Intelligence for Cyber Security
2. Knowledge Engineering and Expert System

Suggested Courses

1. **Cybersecurity Fundamentals:**

   Covering foundational concepts, this course provides an overview of cybersecurity principles, terminology, and basic techniques, setting the groundwork for more advanced topics.

2. **Network Security:**

   Focused on securing network infrastructures, this course explores topics such as firewalls, intrusion detection systems, VPNs, and secure protocols to safeguard communication channels.

3. **Security Architecture and Design:**

   This course delves into designing secure systems and architectures, addressing principles of defense-in-depth, secure coding practices, and the integration of security controls.

4. **Ethical Hacking and Penetration Testing:**

   Providing hands-on experience, this course teaches ethical hacking techniques and penetration testing methodologies, enabling students to identify and remediate vulnerabilities in systems.

5. **Digital Forensics:**

   Covering investigative techniques for analyzing and recovering digital evidence, this course prepares students for roles in incident response and cybercrime investigation.

6. **Cloud Security:**

   With a focus on securing cloud environments, this course addresses the unique challenges and solutions associated with cloud computing security, including identity management and data protection.

7. **Cryptography and Cryptanalysis:**

   This course explores cryptographic algorithms, protocols, and their applications in securing data and communication, as well as the techniques for analyzing and breaking cryptographic systems.

8. **Security Policy and Compliance:**

   Covering the development and implementation of security policies, this course addresses compliance with regulatory frameworks, standards, and best practices in cybersecurity governance.

9. **Wireless and Mobile Security:**

   Examining security challenges in wireless and mobile environments, this course covers topics such as mobile device management, secure coding for mobile apps, and wireless network security.

10. **Risk Management in Cybersecurity:**

    Focused on assessing and mitigating cybersecurity risks, this course addresses risk analysis, risk management frameworks, and the development of effective risk management strategies within organizations.

	Teaching and Learning Methods 1. Face to Face Lectures using Audio-Visuals 2. Laboratory work/Fieldwork/Workshop 3. Project Based Learning 4. Problem Based Learning 5. Group Exercises/Assignments 6. Demonstrations 7. Guest Lectures 8. Industry Visit 9. Workshops, Group Discussions, Debates, Presentations 10. Project Work 11. Project Exhibitions 12. Technical Competitions
21	**Attendance** A minimum of 85% attendance is essential for each module.
22	**Assessment and Grading** 1. Every course will be assessed for a weight of 100 2. Assignments- 50% weight 3. End of Module Examination-50% weight 2. If marks scored is: • 91 and above O (outstanding); 81-90: A+ (Excellent); 71-80: A (Very Good); 61-70: B+ (Good); 51-60 : B (Above Average); 40 -50: C (Average); below 40: D (Not satisfactory) • If one scores D grade, the candidate is required to re-register for the module and earn the required credits • **A minimum of overall 40% is required for completion of a course by acquiring minimum grade (pass) with a minimum of 40% in each component.** **4.** End of each semester –grade card will be issued
23	**Award of Degree** Every student registering for the program need to complete a **minimum of 80 credits, for the award of M.Sc. Degree** **Award of Degree Certificate:** Students will be issued consolidated grade card with CGPA displayed and GM University Degree Certificate. **Award of Gold Medal:** A student with highest CGPA (Not less than 9.0 on a scale of 10) in the class without getting a D grade in any course over 8 semester and completing the program within the specified period of 2 years (4 semesters) will be awarded Gold Medal.

24	**Student Support for Learning** 1. Course Notes 2. Reference Books in the Library 3. Magazines and Journals 4. Internet Facility 5. Computing Facility 6. Laboratory Facility 7. Workshop Facility 8. Staff Support 9. Lounges for Discussions 10. Any other support that enhances their learning
25	**Quality Control Measures** 1. Review of Course Notes 2. Review of Question Papers and Assignment Questions 3. Student Feedback 4. Moderation of Assessed Work 5. Opportunities for students to see their assessed work 6. Review by external examiners and external examiners reports 7. Staff Student Consultative Committee meetings 8. Student exit feedback 9. Course Assessment Board (CAB) 10. Programme Assessment Board (PAB)