MASTER OF SCIENCE IN CYBERSECURITY
36 credits, 60 Weeks or 4 Terms (15 weeks in length each).

Program Description

The master's program in Cybersecurity provides students with the skills and knowledge necessary to design, implement and manage security solutions to prevent and detect cyberattacks. The curriculum emphasizes providing students with relevant, practical skills that meets the cybersecurity workforce needs of business, industries, and the government to address state, national and international cybersecurity challenges. Students will learn critical-thinking strategies to make informed decisions in an attack on computer networks and infrastructures. This program also provides practical experience by employing secure application development methodologies, tools, and techniques, as well as identifying cybersecurity attacks and mitigation strategies.

Program Objective

The objective of the master's program in Cybersecurity is to equip students with the necessary knowledge and skills to effectively analyze, design and implement cybersecurity solutions in a rapidly evolving technological environment. The curriculum provides students with a comprehensive understanding of key cybersecurity principles, practices and techniques, as well as an understanding of its cultural, ethical and legal implications. Students will also develop the skills needed to identify and analyze cybersecurity threats and to assess, manage and mitigate risks associated with these threats. By imparting a deep understanding of fundamental cybersecurity concepts, building practical skills and emphasizing ethical considerations, the Cybersecurity program prepares graduates for rewarding careers protecting businesses and organizations of all sizes from a wide range of cybersecurity threats.

Program outcomes: Upon completion of the program, students will:

- Gain proficiency in various technical areas such as network security, cryptography, data security, and secure software development to address cybersecurity challenges and contribute effectively to the protection of information systems and data in a variety of organizational settings.
- Enhance their ability to research and analyze cybersecurity threats, vulnerabilities, and risks to develop effective mitigation strategies.
- Empower students to navigate the complexities of cybersecurity with a sharp analytical mindset, ensuring they are well-equipped to tackle the evolving landscape of digital threats and security vulnerabilities.
- Develop the capability to strongly understand ethical considerations and social responsibility to navigate ethical challenges in cybersecurity with integrity.
- Develop skills in planning, executing, and managing cybersecurity projects from initiation to completion.

Master of Science in Artificial Intelligence PROGRAM OUTLINE		
Course Number	**Course Title**	**Credit Hours**
Semester 1		
CTS5120	Fundamentals of Cybersecurity	3
CNT5402	Foundation of Information Security	3
CIS5371	Introduction to Cryptography	3
Semester 2		
CNT5410	Computer and Network Security	3
CAP6701	Data Security and Privacy	3
CIS5604	Security and Privacy in Cloud Computing	3
Semester 3		
CIS6079	Secure Software Development	3
CAP6710	Multimedia Security and Forensics	3
CIS6100	Information Security and Privacy	3
Semester 4		
CIS6174	Information Security Planning	3
CIS6209	Penetration Testing: Ethical Hacking	3
CIS6220	Cybersecurity Capstone Project	3
	TOTAL:	**36**