

Bachelor of Technology (CSE-Cyber Security)

Programme Educational Objectives (PEOs)

PEO 1: Equip graduates with a solid foundation in computer science and specialized expertise in cybersecurity to identify, analyze, and mitigate security threats in modern computing systems and networks.

PEO 2: Foster continuous learning and innovation by empowering graduates to adapt to evolving cybersecurity challenges, leverage emerging technologies, and contribute to research and development in secure systems.

PEO 3: Prepare graduates to address global cybersecurity challenges with a strong sense of ethics, ensuring privacy, data protection, and sustainability while safeguarding critical information and infrastructure.

Program Outcomes (POs)

PO1: Engineering Knowledge: Ability to apply knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: Problem Analysis: Ability to identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: Design/Development of Solutions: Ability to design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and the cultural, societal, and environmental considerations.

PO4: Conduct Investigations of Complex Problems: Ability to conduct investigation into complex problems using research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: Modern Tool Usage: Ability to create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: Engineer and Society: Ability to apply reasoning informed by contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to professional engineering practice.

PO7: Environment and Sustainability: Ability to recognize and incorporate the diversity and commonalities of engineering solutions in societal and environmental contexts and demonstrate knowledge of and need for sustainable development.

PO8: Ethics: Ability to apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.

PO9: Individual and Team Work: Ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: Communication: Ability to communicate effectively on complex engineering activities with the engineering community and with society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: Project Management and Finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader to the teams to manage projects and interdisciplinary teams.

PO12: Life-long Learning: Ability to recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes (PSOs)

PSO1: Develop the ability to identify, analyze, and mitigate security threats using advanced cryptographic techniques, secure programming practices, and network defense mechanisms to protect digital systems and data.

PSO2: Leverage Artificial Intelligence and Machine Learning techniques to enhance cybersecurity measures, including anomaly detection, threat prediction, and automated incident response, ensuring robust and adaptive security solutions.