A. Knowledge and Understanding:

Upon successful completion of the Program, graduates should be able to:

A1. Demonstrate an in-depth knowledge of terminology, concepts, methods, principles and theories relaed to the field of cyber security.

A2. Demonstrate a profound knowledge of computing tools, techniques, and methods for solving the real world computing problems.

A3. Identify the user and organizational needs and issues involved in the management and security of digital information and computer technology, and the development and maintenance of secure information systems.

A4. Describe the concepts and techniques to achieve authentication, authorization, access control, and data integrity.

B. Cognitive/ Intellectual Skills:

Upon successful completion of the program, graduates should be able to:

B1. Analyze the basic concepts, principles, analytical and mathematical models, algorithms and software tools in the context of cybersecurity.

B2. Select an appropriate range of security protocols, tools, and techniques for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation.

B3. Select an appropriate range of tools and technologies to plan, organize, and implement a cyber security project considering human factors, user and organisational requirements.

B4. Evaluate a computing-based solution to meet a given set of computing requirements in the context of cybersecurity discipline.

B5. C. Practical and Professional Skills:

B6. Upon successful completion of the program, graduates should be able to:

B1. Apply mathematical foundations, algorithmic principles, cryptography, design and development principles, and computing theory in the modeling and design of security solutions for software, network, or system architecture.

B2. Design, implement, and test a computing-based solution to meet a given set of computing requirements in the context of cyber security.

B3. Deploy effectively computing tools and techniques used for the construction and documentation of secure computer applications of varying complexity.

B4. Apply principles, processes, tools and techniques used in mitigating security threats and responding to security incidents.

B5. D. General and Transferable Skills:

B6. Upon successful completion of the program, graduates should be able to:

B1. Function effectively individually, as a member, or leader of a team engaged in activities appropriate to the cybersecurity program's discipline to accomplish a common goal.

B2. Commit to professional ethics, responsibilities, and norms of professional computing practices.

B3. Communicate effectively in writing and verbally computing and cybersecurity concepts and implicationsto wide range of audiences.

B4. Engage in continuing professional development and lifelong learning as a computing professional.