Master of Science in Cybersecurity

- Print
- Download PDF

A multidisciplinary graduate program addressing issues that ensure secure and reliable operations at all levels of interconnected computing and networking systems.

Cybersecurity is a multidisciplinary field addressing issues that ensure secure and reliable operations at all levels of interconnected computing and networking systems. The Master of Science in Cybersecurity is designed to train graduate scholars, professionals, entrepreneurs, leaders, and researchers in the advanced knowledge and skills required to fully understand and implement the technologies, tools, management methods, and policy issues related to cybersecurity.

This Master of Science program not only covers multidisciplinary fields related to cybersecurity technology but also examines policy, ethics, and management related to IT security and cyber threats. The program leverages strong partnerships and collaborations both within HBKU and beyond the university. Delivery of the program involves collaborations with HBKU's research institutes, most notably with QBRI.

This program also builds on work with industrial and governmental partners, both local and international, who are currently working on critical projects aimed at providing solutions to address global challenges and lead to a safer cyber world, in support of Qatar's aspirations in this area.

The program offers its students the option of either completing a research thesis or working on an industrial project. The thesis requires in-depth theoretical and research components, while the industrial project offers a route for students to further develop real-world problem-solving experience.

The program includes a core course in leadership and innovation, ensuring that all graduates are equipped with the skills and knowledge to assume leading roles within academic, governmental, and non-governmental organizations.

Program Focus

- The development of extensive and advanced knowledge in the field of cybersecurity, covering major areas such as applied cryptography, computer and network security, secure software/hardware systems, and cybersecurity policy, management, and ethics.
- A multi-faceted curriculum covering multidisciplinary aspects that are not only related to cybersecurity technology but also cover policy, management, ethics, and IT security.
- Hands-on experience with real-world projects related to secure software and hardware design and implementation, secure mobile systems, information security, risk analysis, computer and network forensics, among others.
- A research thesis or industrial project involving original work related to cybersecurity, guided by world-class faculty members from HBKU, its research institutes, and other stakeholders.

Curriculum

A 33-credit program taught in English, typically over two years, that includes:

- **Four core courses**

  Four core courses that provide students coming from diverse backgrounds with a coherent learning environment to tackle issues in cybersecurity.

  The core courses are:

  - Research Methods and Ethics in ICT
  - Applied Cryptography
  - Computer and Network Security
  - Security Risk Analysis

- **Four elective courses**

  - Four elective courses covering engineering and computer science topics, in addition to a variety of cybersecurity electives that provide students with a solid base and a depth of knowledge, which fully enables them to understand different aspects of cybersecurity. Additionally, there will be the opportunity to take an elective focusing on entrepreneurship.

- **Two semesters of graduate research seminars**

  - Two semesters of graduate research seminars aimed at expanding students' horizons by offering a broad range of topics, through talks by invited experts and presentations from those working in industry, research institutes, academia, and government institutions and organizations.

- **A nine-credit research thesis or a six-credit industrial project.**
