Cybersecurity B.S.

Program Description

The purpose of the Bachelor of Science with a major in Cybersecurity (BS-CYBR) program is to create technologically capable, business-aware cybersecurity professionals capable of applying technical skills and the knowledge of security management to protect computerized information systems from a wide variety of threats, and to manage the risks associated with modern information technology usage. Cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of information technology, law, policy, human factors, ethics, and risk management often in the context of adversaries.

The Department of Homeland Security and the National Security Agency have jointly designated Kennesaw State University as a National Center of Academic Excellence in Cyber Defense Education with specialized focus areas in Security Policy Development & Compliance and Systems Security Administration.

The Bachelor of Science with a major in Cybersecurity is a fully online degree that has the primary objective of meeting the high demand for professional degrees in the area of cybersecurity. The degree has core requirements, major requirements, major specializations, and required electives. The major contains those courses considered fundamental to the cybersecurity field and the electives give the student some flexibility in choice.

The Institute for Cybersecurity Workforce Development requires that BS-CYBR candidates must earn a grade of "C" or better in all upper-division courses in order to be counted toward their degree.

💼 This program is a part of the Michael J. Coles College of Business.

Admission, Enrollment and Graduation Policies

Admissions Requirements

This program does not have specific admission requirements and only admission to Kennesaw State University is required. For more information, please visit the Admissions section of the catalog.

Graduation Requirements

Each student is expected to meet the requirements outlined in Academic Policies 5.0 PROGRAM REQUIREMENTS & GRADUATION.

Program Course Requirements

Core IMPACTS Curriculum (42 Credit Hours)

General Education Core IMPACTS Curriculum

Core IMPACTS Curriculum Requirements Specific to This Major

Science Majors: Must take MATH 1113 or higher in Mathematics & Quantitative Skills and MATH 1179 or higher in Applied Math.

Science and Engineering Majors: Must take two four-hour laboratory sciences in Natural Sciences. Students must choose from CHEM 1211/1211L , CHEM 1212/1212 , PHYS 1111/1111L* , PHYS 1112/1112L , PHYS 2211/2211L *, PHYS 2212/2212L, BIOL 1107/1107L , or BIOL 1108/1108L.

*Students cannot take both PHYS 1111/L and PHYS 2211/L nor PHYS 1112/L and PHYS 2212/L.

Core Field of Study (18 Credit Hours)

Students must earn a "C" or better in these courses.

- ACCT 2101: Principles of Accounting I
- ECON 2300: Business Statistics
  or
- STAT 2332: Probability and Data Analysis
- IT 1114: Programming Principles
- IT 1114L: Programming Principles Lab
- CSE 1321: Programming and Problem Solving I
- CSE 1321L: Programming and Problem Solving I Laboratory
- CYBR 2310: Software Assurance
  One (1) credit hour carried from Technology, Mathematics, & Sciences.

Major Requirements (37 Credit Hours)

Students must earn a "C" or better in these courses.

Upper-Division Technical Core (13 Credit Hours)

- CYBR 3123: Hardware and Software Concepts

- CYBR 3423: Operating Systems Concepts & Administration
- CYBR 4323: Data Communications & Networking
- CYBR 4423: Linux/Unix Administration
  One (1) credit hour carried over from Technology, Mathematics, & Sciences.

Upper-Division Security Core (21 Credit Hours)

- CYBR 3100: Principles of Cybersecurity
- CYBR 3200: Network Security
- CYBR 3210: Client Systems Security
- CYBR 3300: Management of Cybersecurity in a Global Environment
- CYBR 4200: Perimeter Defense
- CYBR 4220: Server Systems Security
- CYBR 4330: Incident Response and Contingency Planning

Capstone (3 Credit Hours)

- CYBR 4810: Cyber Defense

Upper Division Major Specializations (9 Credit Hours)

Students must earn a "C" or better in these courses. Students are required to take a minimum of 9 credit hours as an upper-level specialization. Choose one of the following:

Systems Security Track

Required Courses (9 Credit Hours)

- CYBR 3153: Database Systems
- CYBR 4843: Ethical Hacking for Effective Defense
  or
- CYBR 4883: Infrastructure Defense
- CYBR 4350: Management of Digital Forensics and eDiscovery
  or
- CYBR 4853: Computer Forensics

Network Security Track

Required Courses (9 Credit Hours)

- CYBR 4333: Network Configuration & Administration
- CYBR 4833: Wireless Security

- CYBR 4893: Internet of Things: Applications and Security

Cyber Crime Track

Required Courses (9 Credit Hours)

- CRJU 1101: Foundations of Criminal Justice
- CYBR 3305: Technology and Criminal Justice
- CYBR 4305: Technology and Cyber Crime

Major Electives (9 Credit Hours)

Students must earn a "C" or better in these courses. Select 9 credit hours from the following list of courses:

- CYBR 3220: Global IS Project Management
- CYBR 3223: Software Acquisition and Project Management
  Any CYBR prefix course not included in your chosen concentration.
- CYBR 3396: Cooperative Study
- CYBR 3398: Internship
- CYBR 4400: Directed Study
- CYBR 4490: Special Topics in Cybersecurity
  Any 3000 or 4000 level IS/ISA/IT/CS/CSE/CRJU course for which the student can meet the prerequisites except certain specific restricted ISA or IT Security course (see an advisor for complete listing).

University Electives (5 Credit Hours)

In accordance with KSU Graduation Policy, students must earn a grade of "D" or better in these courses while maintaining at minimum 2.00 cumulative GPA.

Free Electives (5 Credit Hours)

Select 5 credit hours of 1000-4000 level coursework from the University Catalog.

Program Total (120 Credit Hours)