General

Program Title
Cybersecurity

Program Code
-

Degree Designation(s)
Other

Program Level
Undergraduate

Status
Active

School
Theoretical & Applied Science

Convening Group
Cybersecurity (CYBR)

Program Description
The Cybersecurity minor provides students in any major with a foundation in protecting digital systems, networks, and data. Students develop skills in threat assessment, cyber defense, and information management while exploring the ethical and legal dimensions of cybersecurity. The interdisciplinary curriculum draws from Computer Science, Data Science, and Information Technology Management, with elective options in cryptography, digital forensics, network programming, and web application security. Tailored pathways allow students to select coursework aligned with their primary discipline and career goals. This minor complements degrees across all schools, preparing graduates to contribute to organizational cybersecurity in an era of growing digital threats.

Concentration(s)
-

CIP Code
-

Rationale
Cybersecurity is among the fastest-growing fields in the nation. Student interest is strong - the Cybersecurity major launched in Fall 2024 and has already exceeded enrollment of many majors, and current students in a variety of majors have directly requested a minor. The proposed minor requires no new courses, no additional faculty, and no new resources; it is composed entirely of existing coursework across Computer Science, Data Science, and Information Technology Management. Six regional institutions already offer comparable minors.

Effective Start Term
Fall 2026

Effective Start Date
Aug 26, 2026

Coursedog Only Catalog Fields

Catalog Display Name
Cybersecurity (Minor)

Catalog Short Description
Develops foundational skills in cyber defense, threat assessment, digital forensics, and the ethical and legal dimensions of information security.

Catalog Full Description
The Cybersecurity minor provides students in any major with a foundation in protecting digital systems, networks, and data. Students develop skills in threat assessment, cyber defense, and information management while exploring the ethical and legal dimensions of cybersecurity. The interdisciplinary curriculum draws from Computer Science, Data Science, and Information Technology Management, with elective options in cryptography, digital forensics, network programming, and web application security. Tailored pathways allow students to select coursework aligned with their primary discipline and career goals. This minor complements degrees across all schools, preparing graduates to contribute to organizational cybersecurity in an era of growing digital threats.

Ramapo Program Goals and Learning Outcomes

Learning Goals and Outcomes
Program Goals
- Produce graduates prepared to collaborate with organizations in implementing cybersecurity posture.
- Produce graduates who are able to contextualize cybersecurity challenges and solutions within ethical and legal parameters of the field.
- Produce graduates with experience assessing and implementing defenses to a broad set of cybersecurity threats.
- Produce graduates who have had exposure to cybersecurity across a broad range of systems and application concepts.

Student Learning Outcomes
- Information Management: Demonstrated knowledge of principles of information technology within an organization.
- Ethics and Law: Demonstrate a broad understanding of relevant literature on ethical and legal issues pertaining to computing technology and security.
- Cyber Defense: Demonstrated experience in identifying and assessing vulnerability, threat intelligence, penetration testing, and defending against common attack vectors in cyberinfrastructure.
- Application Breadth: Demonstrated ability to relate cybersecurity concepts to critical areas of software development, such as database systems, web applications, and operating systems.

Learning Outcomes (This card is NOT used and should remain hidden)

Requirements

Simple Requisites

(No Requirement Levels)

Cybersecurity Core
Type
Completion Requirement

Complete at least 1 of the following courses:

- CMPS305 - CYBER SECURITY
- CMPS370 - CYBER AND NETWORK DEFENSE
- INFO340 - CYBERSECURITY

Ethics / Policy / Law
Type
Completion Requirement

Complete at least 1 of the following courses:

- DATA225 - ETHICS OF TECHNOLOGY
- INFO315 - COMPUTER LAW AND ETHICS

Information Management
Type
Completion Requirement

Complete ALL of the following Courses:

- INFO224 - PRINCIPLES OF INFORMATION TECHNOLOGY

Cybersecurity Electives

Type

Completion Requirement

Complete at least 2 of the following courses:

- MATH240 - CRYPTOGRAPHY
- INFO316 - INTRO TO DIGITAL FORENSICS
- INFO320 - TOOLS FOR ANALYTICS AND AI
- INFO333 - DATA VISUALIZATION
- INFO335 - NETWORKS AND DISTRIBUTED PROCESSING
- INFO342 - SYSTEMS ANALYSIS AND DESIGN
- INFO441 - INFORMATION TECHNOLOGY MANAGEMENT
- DATA301 - DATA ANALYSIS & VISUALIZATION
- CMPS285 - MOBILE DEVELOPMENT
- CMPS315 - THE LINUX ENVIRONMENT
- CMPS327 - NETWORK PROGRAMMING
- CMPS364 - DATABASE DESIGN
- CMPS369 - WEB APPLICATION DEVELOPMENT

Degree Maps

Dependencies

Instructional Methods (This card is NOT used and should remain hidden)

Identifiers

SIS ID	id	programGroupId	programCode (code)
-	-	-	-