BACHELOR OF SCIENCE IN CYBERSECURITY AND INVESTIGATION

2022-2023 Degree Requirements

Name: _____ **ID Number:** _____

TOTAL CREDITS FOR DEGREE: 120

UNIVERSITY CORE CURRICULUM: 42 credits

Required Fundamental Courses:

COMM 101	Oral Comm. & Pres.		3 credits
ENGL 101	College Composition		3 credits
UNIV 101	City-University Life		3 credits
Senior Capstone		**CRMJ 400**	3 credits

Choose Thematic Core courses in the following:

Explore the World - Choice 1	3 credits
Explore the World - Choice 2	3 credits
Investigate Science	3 credits
Investigate Mathematics	3 credits
Interpret Creative Works	3 credits
Understand People - Choice 1	3 credits
Understand People - Choice 2	3 credits
Succeed in Business	3 credits
Appreciate & Apply the Arts	3 credits
Discover Technology	3 credits

MAJOR REQUIREMENTS: 69 cr.

CMPS 161 Networking and Security	3_____
CMPS 263 Cybercrime	3_____
CMPS 362 Networking	3_____
CMPS 363 Digital Security	3_____
CMPS 365 Cyber Analysis	3_____
CMPS 465 Cybersecurity Policy	3_____

Electives Select 3 in CMPS- 9 credits

_____

_____

_____

General Electives- 9 credits

_____

_____

_____

CYBR 101 Introduction to Cybercrime	
CYBR 102 Trends in IT Security	3_____
CYBR 103 Legal and Ethical Issues	3_____
CYBR 104 Countering Cybercrime	3_____
CYBR 200 Cybersecurity Risk Mgmt	3_____
CYBR 201 Cyber Crime Mindset	3_____
CYBR 202 Cybercrime Forensics	3_____
CYBR 300 Cybercrime Case Studies	3_____
CYBR 301 Cybercrime Social Media	3_____
CYBER 302 Cybercrime Internet	3_____
CYBR 400 The Costs of Cybercrime	3_____

Electives: Pick 3 of the following:

INTL 300 Critical Thinking Analysts	3_____
INTL 301 Integ. Intelligence Analysis	3_____
INTL 302 National Intelligence Auth	3_____
INTL 402 Current Issues in US Policy	3_____
INTL 406 Methods of Propaganda	3_____
INTL 407 Work Conflicts	3_____
INTL 411 Threat Analysis	3_____

BACHELOR OF SCIENCE IN CYBERSECURITY AND INVESTIGATION

2022-2023 Degree Requirements

PROGRAM OBJECTIVES

Upon successful completion of this program, a student will be able to:

1. Describe, Classify, and analyze the global threats and consequences of cyber crime and attacks on world governments, businesses, and populations.
2. Describe and explain the history and uses of TOR, the deep and dark webs, ways in which illegal trade and processes are undertaken, and the ways and which these activities are investigated and prevented.
3. Describe, explain, and evaluate the technologies and technical skills involved in cyber security and investigation measures.
4. Evaluate and analyze the most effective techinques for cyber security and investigations, based on patterns revealed through the thorough examination of real world case studies
5. Describe, explain, and assess the roles of various agencies and organizations in preventing, investigating, conducting, and prosecuting cyber attacks and cybercrimes.
6. Formulate, implement, and update plans to mitigate, prevent, deter, and investigate cybercrime and attacks.