Cyber Defense

- **Major: 57 credit hours**
- **Minor: 21 credit hours**
- **Major/Minor GPA required for graduation: 2.25**

PROGRAM REQUIREMENTS:

- **Capstone: Practicum in Cyber Defense**

Description of Major: Students in this major have the opportunity to gain knowledge and develop skills related to the protection of information and intellectual property in the public and private sectors. Courses align with the guidelines suggested by the National Initiative for Cybersecurity Education (NICE). The initiative focuses on securely provisioning, operating and maintaining, and overseeing and governing information technology systems and networks from a cyber-defense perspective to protect and defend information and intellectual property.

Student Learning Outcomes

Students will:

- Demonstrate understanding of the concepts and designs of secure information technology systems.
- Demonstrate understanding of the support, administration, and maintenance necessary to ensure effective and efficient defense of information and intellectual property.
- Demonstrate understanding of the leadership, management, direction, and development needed to advocate effectively for the cyber-defense needs of public and private organizations.
- Demonstrate the ability to analyze, identify, and mitigate threats to internal information technology systems and/or networks.
- Demonstrate an understanding of the process of evaluating and collecting data/information to develop useful cyber-defense intelligence.

Preparation: The major in cyber defense provides students the educational foundation to succeed in the ever-growing field of cyber defense. This major prepares students to work as analysts, investigators, consultants, and managers in public and private-sector organizations seeking to protect their sensitive information, intellectual property, and information technology systems and networks.

CYBER DEFENSE MAJOR		57 crs.
BUSINESS CORE REQUIREMENTS		**39 crs.**
ACC 205	PRINCIPLES OF FINANCIAL ACCOUNTING	3
ACC 230	PRINCIPLES OF MANAGERIAL ACCOUNTING	3
ECO 211	PRINCIPLES OF MICROECONOMICS	3
ECO 212	PRINCIPLES OF MACROECONOMICS	3
BUS 303	BUSINESS LAW I	3
or		
BUS 304	BUSINESS LAW II	3
BUS 324	BUSINESS ETHICS AND CORPORATE SOCIAL RESPONSIBILITY (W)	3
FIN 308	PRINCIPLES OF BUSINESS FINANCE	3
MTH 170	STATISTICS	3
BUS 310	QUANTITATIVE ANALYSIS FOR BUSINESS DECISIONS	3
MGT 204	PRINCIPLES OF MANAGEMENT	3
MKT 205	PRINCIPLES OF MARKETING	3
BUS 410	MANAGEMENT INFORMATION SYSTEMS	3
or		
ACC 220	ACCOUNTING INFORMATION SYSTEMS	3
BUS 450	BUSINESS STRATEGY AND POLICY	3

CYBER DEFENSE MAJOR REQUIREMENTS 18 crs.

BUS 350	BASIC PROGRAMMING FOR BUSINESS AND CYBER DEFENSE	3
CBD 330	INTRODUCTION TO CYBER DEFENSE	3
CBD 332	CYBER DEFENSE NETWORKING	3
CBD 334	LEGAL AND ETHICAL ENVIRONMENT OF CYBER DEFENSE (W)	3
CBD 336	CYBER RISK MANAGEMENT AND MITIGATION	3
CBD 451	PRACTICUM IN CYBER DEFENSE	3

CYBER DEFENSE MINOR 21 crs.

The minor in cyber defense is available to students in any major. To receive the minor, students must complete the required courses listed below.

BUS 350	BASIC PROGRAMMING FOR BUSINESS AND CYBER DEFENSE	3
BUS 410	MANAGEMENT INFORMATION SYSTEMS	3
CBD 330	INTRODUCTION TO CYBER DEFENSE	3
CBD 332	CYBER DEFENSE NETWORKING	3
CBD 334	LEGAL AND ETHICAL ENVIRONMENT OF CYBER DEFENSE (W)	3
CBD 336	CYBER RISK MANAGEMENT AND MITIGATION	3
MGT 204	PRINCIPLES OF MANAGEMENT	3

Cyber Defense (CBD)

CBD 330 **3**
INTRODUCTION TO CYBER DEFENSE
In this course, students learn the basic concepts, terminology, and technologies that comprise the field of cyber defense. Students in this course are introduced to topics such as risk/threats in the cyber environment, threat assessment, cyber-defense terminology, cyber-defense planning, and general cyber-defense management.

CBD 332 **3**
CYBER DEFENSE NETWORKING
Students in this course explore the fundamentals of network security and related topics. This course facilitates an understanding of the fundamentals of networking configurations and protocols, as well as threat and vulnerability recognition and mitigation from the perspective of the CIA triad: eavesdropping (confidentiality), man-in-the-middle (integrity), and denial-of-service (availability). Students will also engage in applied learning to reinforce lectures and provide practical implementation experience.

CBD 334 **3**
LEGAL AND ETHICAL ENVIRONMENT OF CYBER DEFENSE (W)
In this course, students are exposed to the legal and ethical issues that relate to the field of cyber defense. In addition to learning about the laws and policies that shape and govern this field, students will also study topics such as General Data Protection Regulation (GDPR), the protection of information/intellectual property, ethical hacking, and privacy concerns in public and private organization.

CBD 336 **3**
CYBER RISK MANAGEMENT AND MITIGATION
This course explores cyber defense from a risk-management perspective. Students focus on strategies for assessing risk, as well as for implementing effective and proactive risk-management practices and risk-mitigation measures. Topics in this risk assessment include risk analysis, risk mitigation, risk management, networking components and Virtual Private Networks (VPN). Students will also learn about the resources and methods used for information assurance. The student will apply this knowledge to develop an assessment methodology and strategies for managing and mitigating risks in the cyber environment.

CBD 451 **3**
PRACTICUM IN CYBER DEFENSE
This is the capstone course for the major in cyber defense. This is an applied, lab-based class that provides students an opportunity to apply the knowledge they have learned in a simulated environment. They will assess and identify vulnerabilities, threats, and suspicious activity in information technology systems and networks; assess the implication of threats; and implement management and mitigation responses to protect and defend sensitive information and intellectual property. Prerequisite: BUS 350, CBD 330, 332, 334, CBD 336.

CBD 470 **3-8**
INTERNSHIP IN CYBER DEFENSE