Pathway: Interdisciplinary Pathway in Cybersecurity

Purpose:

The Cybersecurity pathway is designed to provide students with comprehensive knowledge and skills necessary to protect information systems, analyze security threats, and respond to cyber incidents. This interdisciplinary program combines courses from business, communication, criminal justice, technology, entrepreneurship, and ethics to offer a well-rounded education in cybersecurity. Graduates will be prepared to navigate the complexities of cybersecurity in various organizational settings, ensuring the integrity, confidentiality, and availability of information.

Career Outcomes:

- Cybersecurity Analyst
- Information Security Manager
- Network Security Engineer
- Cybersecurity Consultant
- IT Auditor
- Incident Response Specialist
- Ethical Hacker
- Chief Information Security Officer (CISO)

10-Course Academic Pathway

1. **TECH 310 - Introduction to Cybersecurity**
    - **Description**: An overview of cybersecurity principles, including threat landscapes, security frameworks, and defensive measures.
    - **Level**: 300
2. **BUS 305 - Principles of Information Systems**
    - **Description**: Covers the fundamental concepts of information systems, focusing on the role of technology in supporting business operations and decision-making.
    - **Level**: 300
3. **CRJ 320 - Cybercrime and Digital Forensics**
    - **Description**: Examines cybercrimes, digital evidence collection, and forensic analysis techniques used in criminal investigations.
    - **Level**: 300
4. **COMM 301 - Communication in the Digital Age**
    - **Description**: Develops skills in digital communication, including online collaboration, information dissemination, and cyber communication strategies.
    - **Level**: 300
5. **ENTR 340 - Entrepreneurship in Technology**
    - **Description**: Focuses on entrepreneurial opportunities in the technology sector, including cybersecurity startups and innovation.
    - **Level**: 300
6. **TECH 410 - Network Security and Management**
    - **Description**: Covers the principles and practices of network security, including firewalls, intrusion detection systems, and secure network design.

   - **Level**: 400
7. **ETHC 450 - Cyber Ethics and Policy**
   - **Description**: Explores ethical issues and policies related to cybersecurity, including privacy, surveillance, and ethical hacking.
   - **Level**: 400
8. **BUS 450 - Risk Management and Compliance**
   - **Description**: Focuses on identifying, assessing, and managing risks in information systems. Includes compliance with legal and regulatory requirements.
   - **Level**: 400
9. **TECH 420 - Advanced Cybersecurity Practices**
   - **Description**: In-depth study of advanced cybersecurity techniques, including encryption, penetration testing, and incident response.
   - **Level**: 400
10. **CRJ 450 - Legal Issues in Cybersecurity**
   - **Description**: Examines the legal aspects of cybersecurity, including laws, regulations, and legal responses to cyber incidents.
   - **Level**: 400

These courses collectively build a strong foundation in cybersecurity, combining knowledge from multiple disciplines to prepare students for the challenges and opportunities in protecting information systems and responding to cyber threats.