Proposed Certificate of Proficiency in Cybersecurity and Data Management (15 hours)

a. Curriculum Outline

Required Core Courses (9 hours)
ISYS 4013, Principles of Data and Cybersecurity
ISYS 4023, Network and Data Security in a Changing World
ISYS 4043, Cybersecurity, Crime, and Data Privacy Law Fundamentals

Elective Courses (6 hours)
ISYS 4033, Advanced Information Security Management
ISYS 4053, Advanced Cybersecurity, Crime, and Privacy Law
ISYS 4173, Blockchain Fundamentals
ISYS 3273, Cryptocurrency
MGMT 4243, Ethics and Corporate Responsibility

b. Total semester credit hours required for proposed program:

15 hours

c. New courses and new course descriptions

ISYS 4013, Principles of Data and Cybersecurity
This course provides students with insight into the cybersecurity and data issues surrounding businesses and will familiarize students with fundamental concepts of the study of law - enabling students to understand the basics of reading and briefing a case as well as the process of legal analysis and case procedure and discovery. Cybersecurity and data issues which include securing organizational data, detecting and responding to cyber-based security breaches, emerging technologies, and ensuring a secured computing environment for safeguarding company information will be explored. The course reviews the security and cryptographic techniques that are currently being used. The nuances involved in defining cybersecurity strategies and complying with security standards to ensure governance are discussed as well as confidentiality, integrity, ethical use, and availability of data.
Prerequisite: Junior Standing

ISYS 4023, Network and Data Security in a Changing World
This course explores network and data security in the context of today's digital enterprise. In addition to traditional network protocol and security issues, this course will explore security issues unique to cloud environments, data protection, IoT ecosystems, ERP systems, and Blockchain deployments.
Prerequisite: ISYS 4013 with a grade of C or better.

ISYS 4033, Advanced Information Security Management
This course provides students with an in-depth, advanced understanding of cybersecurity and data management. Topics include risk assessment, continuity planning, data protection, threat

detection, threat/risk mitigation, and recovery issues and techniques. Current topics in data and cybersecurity will also be included.
Prerequisite: ISYS 4023 with a grade of C or better.

ISYS 4043, Cybersecurity, Crime and Data Privacy Law Fundamentals
this course examines the law governing computer crime, data privacy, and cybersecurity. Substantive crimes such as hacking, identity theft, economic espionage, and online threats are discussed. The Fourth Amendment, Privacy, the Wiretap Act, and other limits on law enforcement that might affect private industry developing surveillance tools used by governments are examined.
Prerequisite: ISYS 4013

ISYS 4053, Advanced Cybersecurity, Crime and Privacy Law
Advanced study of information privacy and security. The course will explore best practices for data privacy and security protection measures, mitigation techniques for privacy and security threats, and privacy and security law. The importance of informational privacy will be highlight and a high-level overview of U.S. laws and regulations including FTC roles, and government surveillance will be provided.
Prerequisite: ISYS 4023 and ISYS 4043

ISYS 3273, Cryptocurrency
This course is an introduction to cryptocurrency as a blockchain-based application. The course will focus on topics such as a brief history of money, Bitcoin and the origin of cryptocurrency, blockchain system fundamentals (cryptography and consensus algorithms), real-world application with software clients and wallets, as well as assessing the current regulatory environment, financial applications and exchanges. Upon completion, students will understand what constitutes as digital money and how this phenomenon is currently transpiring within an economic, legal, and financial context. In addition, students will be prepared to learn more about specific financial industry applications, make judgements on viability of certain crypto projects and speak to challenges facing the future of cryptocurrency.
Prerequisites: WCOB 2023 or ISYS 2103 and ACCT 2013 each with a grade of C or better

d. Program goals and objectives

The certificate is designed to develop graduates able to help organizations assess and detect threats while securing and protecting data and data-driven systems against a myriad of threats such as malicious software, hacking, insider threats, and other cybercrimes; to learn and apply best industry practices to minimize data collection, protect client and individual privacy, and otherwise further ethical data management. Students will not only learn about cybersecurity, crime, and privacy law; and learn about techniques of risk assessment, continuity planning, and threat detection.

e. Expected student learning outcomes

Upon completion of the certificate, students will:

- Have mastered the technical strategies, tools and techniques commonly used to secure data and information in the enterprise.
- Understand and be able to apply cybersecurity, crime, tort, and privacy law to the management of data and systems.
- Understand disclosure, notification, breach, and other privacy and transparency obligations under state, federal, and international law.
- Be able to detect and identify common malicious software and attack protocols.
- Be able to apply critical thinking to creatively and systematically solve problems and meet challenges of the ever-evolving environments of cyber security.
- Understand the state of cybersecurity nationally and globally.
- Be able to apply data and cybersecurity management techniques to their fields of study.

f. Documentation that the program meets employer needs

The demand for skilled professionals in cybersecurity and data management continues to outpace the supply of qualified applicants. Educated professionals in non-information technology disciplines are increasingly seeking opportunities to develop the knowledge and skills needed to transition into a career in this exciting and rewarding field. Additionally, information technology professionals continue to seek opportunities to expand their cyber knowledge and skills to more effectively position themselves for career growth. The Data and Cybersecurity Management Certificate is both timely and necessary to help meet the needs of employers. The cybersecurity area continues to be an area in high demand. According to the U.S. Bureau of Labor Statistics, information security positions are projected to increase 31.2% from 2019 to 2029.

The 2019 (ICS)2 Cybersecurity Workforce Study conducted by the (ICS)2 and The Center for Cyber Safety and Education reveals that a shortage in global cybersecurity workforce continues to be a significant concern to employers in all facets of industry, non-profit, and municipalities and of all sizes. According to the report, the top concern among cybersecurity professionals is the deficit of skilled cybersecurity personnel, and 65% of the organizations represented in the study indicated a shortage of staff dedicated to cybersecurity.

Also, according to the report, over half of the current cybersecurity workforce didn't start in this area. Instead they have migrated to the information and cybersecurity area from other information technology positions as needs have emerged in their organizations making the Data and Cybersecurity Management Certificate even more relevant, timely, and necessary to meet employers' needs.

References

https://data.bls.gov/projections/nationalMatrix?queryParams=29-1122&ioType=o

https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study#

g. Student demand (projected enrollment) for proposed program

25 students

h. Program approval letter from licensure/certification entity, if required

N/A

i. Scheduled program review date (within 10 years of program)

2021/2022