Management of Cybersecurity Operations BS Student Learning Outcomes

Objective 1: Demonstrate knowledge of the fundamental principles, concepts, people, and events in core areas of Management of Cybersecurity Operations.

Outcome 1.1: Students will demonstrate a comprehensive understanding of cyber security governance, including defining policies, strategies, and risk management plans tailored to business environments, and apply them to both private and government sectors.

Outcome 1.2: Students will demonstrate informed knowledge on evolving cybersecurity laws, regulations (e.g., GDPR, HIPAA), and industry standards, ensuring that business security strategies comply with current frameworks and best practices to support a secure operational environment.

Objective 2: Demonstrate ability to think critically and conduct research in Management of Cybersecurity Operations.

Outcome 2.1: Students will demonstrate the ability to analyze key information assurance frameworks (e.g., ISO 27000, NIST) and apply them to design, implement, and assess security controls, risk management strategies, and operational processes within a business context.

Outcome 2.2: Students will demonstrate the ability to assess and evaluate the effectiveness of cyber security programs within a business organization using key performance indicators (KPIs), metrics, and regular assessments to ensure continuous improvement and effective risk mitigation in business operations.

Objective 3: Demonstrate ability to communicate effectively verbally and in writing.

Outcome 3.1: Students will demonstrate the ability to effectively communicate technical concepts, analysis, and findings related to Cybersecurity Operations through clear, concise, and well-organized written documentation. This includes writing detailed reports, incident analysis, security assessments, and policy recommendations that demonstrate a deep understanding of cybersecurity principles while being accessible to both technical and non-technical audiences.

Outcome 3.2: Students will cultivate the ability to effectively communicate Cybersecurity Operations concepts, strategies, and findings through clear and persuasive oral presentations. This includes presenting complex technical information in a concise, organized manner, engaging both technical and non-technical audiences, and participating in discussions or briefings with confidence, professionalism, and clarity.

Objective 4: Demonstrate appreciation for ethical standards and understanding of societal, cultural, global differences, and human diversity issues as it relates to Management of Cybersecurity Operations.

Outcome 4.1: Students will develop a strong understanding and appreciation for ethical standards in Cybersecurity Operations, including the responsible use of technology, respect for privacy utilizing access control models (DAC, MAC, RBAC), and adherence to legal and regulatory frameworks. They will demonstrate the ability to identify and navigate ethical dilemmas in cybersecurity practices and foundational security concepts, ensuring that their decisions align

with organizational goals, business needs, and regulatory requirements, with professional integrity, societal responsibility, and the highest standards of conduct.

Outcome 4.2: Students graduating with a degree in Management of Cybersecurity Operations can apply disciplinary knowledge in gender/cultural neutral ways.

Outcome 4.3: Students graduating with a degree in Management of Cybersecurity Operations can complete coursework using the ethical and moral standards of the discipline.

Objective 5: Students will demonstrate proficiency in the use of technology as it related to Management of Cybersecurity Operations.

Outcome 5.1: Students will develop the ability to effectively utilize a variety of cybersecurity technologies and tools to identify, assess, and mitigate security threats. They will demonstrate proficiency in leveraging advanced technology through simulated lab solutions, such as intrusion detection systems, firewalls, encryption, and vulnerability management tools, to ensure the protection and resilience of digital assets in dynamic operational environments.

Objective 6: Demonstrated understanding and ability to use effective managerial, leadership and group interaction techniques.

Outcome 6.1: Students will demonstrate the ability to develop a comprehensive understanding of effective managerial, leadership, and group interaction techniques within the context of cybersecurity operations. They will develop the ability to lead and collaborate with diverse teams through group projects, make strategic decisions, and manage cybersecurity initiatives, ensuring the coordination of efforts to protect organizational assets and respond to evolving security threats