Cybersecurity

Program Learning Outcomes

Learning outcomes represent culminating demonstrations of learning and achievement. In addition, learning outcomes are interrelated and cannot be viewed in isolation of one another. As such, they should be viewed as a comprehensive whole. They describe performances that demonstrate that significant integrated learning by graduates of the program has been achieved.

The graduate has reliably demonstrated the ability to

1. Develop and implement cyber security solutions to protect network systems and data.
2. Plan and implement security assessment methodologies, vulnerablility management strategies and incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization.
3. Recommend processes and procedures for maintenance and deployment of cyber security solutions.
4. Select and deploy optimal security appliances and technologies to safeguard an organization's network.
5. Comply with existing industry policies, regulations and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded.
6. Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards.
7. Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization.
8. Implement and conduct penetration testing to identify and exploit an organization's network system vulnerablility.
9. Perform various types of cyber analysis to detect actual security incidents and suggest solutions.
10. Maintain ongoing personal and professional development to improve work performance in the field of information technology.
11. Present and summarize cybersecurity solutions to business stakeholders in a professional manner to inform decision making.