Course Title: CYB 101 Introduction to Cybersecurity

Course Team: Steve Shank

- Perform and share cooperatively in team projects competition
- Review and practice computer and network etiquette and ethics found in working environments
- Evaluate and implement new and future technologies into current system
- Install, configure, use and manage offensive/defensive security tools on a working network
- Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems

Course Instructor(s): Steve Shank

Programs: AAS Cyber Security, AS Cyber Security

Expected Learning Outcomes:

- Think critically
- Communicate effectively with both verbal and written forms
- Perform and share cooperatively in team projects
- Review and practice computer and network etiquette and ethics found in working environments
- Preform risk assessment
- Install, configure, use and manage anti malware software on a working network
- Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems

Assessment: (How do students demonstrate achievement of these outcomes?)

Satisfactory scores on exams and quizzes.

Satisfactory scores on exams modeled after industry standard certification exams. Models are developed from the following certification exams: IC3, Security 5 (ECCouncil)

Completion of Individual Project.

1. Research 3 malware attacks that can be performed on a computer system and/or network systems using Internet and printed reference material
2. Create a written report in Microsoft Word comparing and contrasting the malware attacks.
3. Create a PowerPoint presentation highlighting best practices in defending against the malware attacks described.
4. Create an Excel spreadsheet comparing anti-malware software features, components and costs.
5. Develop rubric to evaluate.

Completion of Group Project.
Perform a risk assessment for a home network or a lab network or corporate network. Identify assets and list vulnerabilities. Discuss mitigation of the network risks. Outline a security policy and guidelines for the chosen network.

Participation in Discussion Boards

Submittal of security journals and periodicals.

Develop a 50-question multiple choice pretest/posttest to administer at beginning of semester and at end of semester.

Validation: (What methods are used to validate your assessment?)

1. Approval of Information Systems Technology Advisory Council

2. Tests comparable to Industry Standard Certification Exams.

3. Faculty Review

Results: (What do the data show?)
N/A (New course)

Follow-up: (How have you used the data to improve student learning?)
N/A (New course)

Budget Justification:
(What resources are necessary to improve student learning?)

PC lab hardware; switches, routers, projection unit, cabling, tools, printers, PCs, servers
Wireless hardware and software
Security hardware and software
Simulation software, Virtual PC licenses.
Testing Software.
Course Management software
Classroom Management system software