Program Outcomes Guide #3 (POG #3)

Program Title: AS Cyber Security
Program Team: Tatyana Zidarov/Steve Shank

Expected Learning Outcomes
- Think critically
- Communicate effectively with both verbal and written forms
- Perform and share cooperatively in teams or groups
- Review and practice computer and network etiquette and ethics found in working environments
- Administer and troubleshoot a network infrastructure
- Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems

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

Think Critically
Satisfactory scores on exams modeled after industry standard certification exams. Models are developed from the following certification exams: IC³, CompTia A+, CompTia Net+, CompTia, Security+, CEH
Successful completion of exams and lab assignments.
Analysis of packets captured in network traffic

Communicate effectively with both verbal and written forms
- Completion of an individual project
- Completion of a group project
- Journal submission of readings in the field
- Participation in discussion boards

Perform and share cooperatively in teams or groups
Completion of group project

Review and practice computer and network etiquette and ethics found in working environments
Completion of group project
Journal submission of readings in the field

Administer and troubleshoot a network infrastructure
Completion of vmware (virtual) project

Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems
- Journal submission of readings in the field
- Completion of individual project
- Completion of group project
- Successful completion of exams and lab projects

Validation (What methods are used to validate your assessment?)
1. Program maps to the National Security Telecommunication and Informatico Systems Security (NSTISSI) 4011 and 4013 Standards.
2. Program meets Center for Academic Excellence 2 year schools (CAE@Y) standards established by the National Security Agency (NSA) and the Department of Homeland Security (DHS)
3. Approval of Information Systems Technology Advisory Council

December 2015
4. Tests modeled after industry standard Certification Exams
5. Program curriculum mirrors CyberWATCH consortium curriculum
6. Faculty Review
7. Textbook Authors

**Results** (What do the data show?)
CyberWATCH suggests inclusion of case studies into curriculum

**Follow-up** (How have you used the data to improve student learning?)
Continue to use Netlabs product. This allows students to avail themselves of a virtual network environment on a 24/7 basis.

Improvements to programs also result from resources obtained from 2nd NSF Cybersecurity grant. The grant requires the creation of a new Cloud Computing Course (CYB 26) which will replace the CYB 245 course which will be incorporated into the CYB 240 Certified Ethical Hacking Course.

Continue to use online learning source – LabSim by Testout in IST 154 and IST 160. These allow students greater opportunity to work on course material including labs through the Internet

**Budget Justification**
(What resources are necessary to improve student learning?)
PC lab hardware; projection unit, cabling, tools, printers, PCs
Simulation software, Virtual PC licenses.
Internet based curriculum
Course Management software
Classroom Management system software