Meeting Date: 9/20/2017

Campuses Represented: Robin Schmidt (Kokomo), Skip Hahnert (Sellersburg), Danette Coughlan (Evansville), Justin Baitz (Lafayette), Melanie Hurst (Terre Haute), Anthony Ford (Indy), Mike Kingsley, Greg Hanson (Anderson), Rami Salahieh (Northwest), Daryl Togashi (Ft Wayne), Ben Marerro (Valpo), Chris Carroll (Bloomington), Bill Worden (Bloomington), Matt Gull (phone, Warsaw), Joe Kennedy (phone, Lawrenceburg), Matthew Cloud (phone), Matt Etchison, Roland Martin (phone, Richmond), Brandi Fabel (Sellersburg), Valerie Golay (phone, South Bend), Christine Bresnahan (Indy), Pam Schmelz (Columbus)

**Curriculum Changes** - *None*

**Course Changes**

*Include the COR as well as the COR Checklist for new and revised courses.*

New Courses - *For each course added, list new course id and list rationale for addition. Include effective date for change.*

* **CSIA216** – Workforce certification prep class for CCNA Security. This will extend the existing Cisco curriculum that exists in the program. Course first available Fall 2018.

Revised Courses - *(List only substantive course changes) For each revised course, list course id, briefly describe change, and rationale for change. Include effective date for change.*

* **CSIA 105** – Remove Cert/Licensure Disclaimer from COR. Revised course available Fall, 2018.

**Action Items**

*Summarize action items requiring post-meeting follow-up, responsible party and date due. Add additional lines if needed.*

|  |  |  |
| --- | --- | --- |
| **Action Item** | **Responsible Party** | **Date Due** |
| **Create CSIA216 COR** | **Pam Schmelz** | **10/10/17** |
| **Add CSIA216 to the summer 2018 development cycle with CSIA215** | **Madison Lehr** | **11/30/17** |
| **Add CSIA106 to the spring 2018 development cycle because of new certification** | **Madison Lehr** | **11/30/17** |
| **Check to see if old Security+ certification can be extended through May, 2018** | **Matthew Etchison** | **11/30/17** |
| **Update instructions/instructor guides for additional MindTap integration for CSIA105** | **Pam Schmelz** | **11/3/17** |
| **Remove Cert/Licensure Disclaimer from COR for CSIA105** | **Pam Schmelz** | **10/10/17** |
| **Fix the ASOM 7.1 course standard for CSIA105 to read CSIA105/106** | **???** | **9/30/2017** |
| **Add the ASOM 7.1 course standard for CSIA215 to read CSIA215/216 and the text: A qualified faculty member teaching CSIA 215/216 meets the Cyber Security/Information Assurance (CSIA) program standard and holds a CCNA Security certified instructor or an up to date certified CCNA Security certification and is a current Cisco Academy Instructor.**  | **????** | **For Fall 2018**  |
| **Edit the certification crosswalk to add CCNA Security for CSIA 215/216****Edit the certification crosswalk to add EC Council C|HFI for CSIA 135/235.** | **????** |  |

Location: Lawrence Campus, room 177 and GoToMeeting Time: 9:30-2:00 EDT

Members Present in Person (include campus represented): See first page

Members Present via Distance (include campus represented): See first page

**Program Curriculum Development and Maintenance. Review of ASOM 6.8**

*1) Lead Chair and Committee Responsibilities*

*a. Note changes that votes can occur both summer and fall “Although curricula discussions are appropriate during the discussion meeting, votes related to curriculum changes shall be confined to the summer and fall curriculum maintenance meetings”*

*Participants should vote:*

*3) Statewide Lead Committee Chair Selection (only if lead chair is vacant)*

*a. Voted last year. New vote fall 2018*

**Incorporating Certifications Into Courses. Review of ASOM 4.13**

1. *Potential Certifications embedded into program*
2. *Discussion of adding a course for CEH WF Prep and CHFI WF Prep. Cost issues of course. No good idea where/if to put in curriculum. Issues with working with EC Council as well. No motion at this time.*
3. *Discussion of CCNA Security back into CSIA 215 now that we can (and have) credentialed Cisco Security faculty. Daryl motions to add CSIA 216 as WF prep for CCNA Security, Valerie 2nds, voted unanimously. Valerie will do the COR for CSIA 216 now.*

**Academic Degree Structure. Review of ASOM 6.3**

*Reviewed/no changes*

**Academic Degree Structure. Review of ASOM 7.1**

CSIA105 course standard should say CSIA105/106? – current version does not

Long discussion about whether cert should apply to the acad course, the 1CR course, or both – can hirers be trusted to accurately assess faculty candidates. This discussion also spilled to academic credentials as well (BS, etc.).

Do same for CSIA 215/216 for Fall 2018 (CCNA Security certified instructor or a up to date certified CCNA Security, once CCNA 215 changes are made). Moved Skip, 2nd Daryl, passed unanimously.

**STGEC Update**

*Need to stress the usage of the Degree Completion Tracker in order to pick the correct general education elective. There has been some confusion around this, but the bottom line is to use the tool to avoid issues.*

**Curriculum Maintenance**

*See other topics*

**Discuss Requests Related to Program Maintenance and Development**

*See other topics*

**Crosswalk Review**

1. *The training and certification crosswalks*
	1. *CLEP/Dantes – CSIA 105. Do people know about this? Make sure campuses do.*
	2. *AP/IB – None*
	3. *UExcel – None*
	4. *Certification – Review/add new ones -*

*add CCNA Security for CSIA 215/216. Move by Jason B, 2nd Mike K voted unanimously.*

*Add EC Council C|HFI for CSIA 135/235. Move by Skip H, 2nd Daryl T, voted unanimously.*

1. [*Dual credit crosswalk*](https://www.ivytech.edu/files/HS-Based-Dual-Credit-Crosswalk.pdf)*—John Newby document*

*There is a push for a cyber course like CSIA 105 at HS side. There is not one now. DOE would have to build a course based on ours . . . and why not just have the students take course here.*

1. *Military crosswalk*

*Will discuss with lead chairs*

**Strategies for Workforce Focus**

*Notes*

**Review and Discussion of Program Outcomes**

1. *Technical Outcomes*
	1. *Need to resolve what to do for capstone TOA.*
	2. *Valerie is interested in leading the portfolio charge. For cybersecurity, we need to make sure a portfolio addresses (do we need to change some of the outcomes? Compare with CAE2Y ones):*

*Groups should all review their Program Outcomes.*

*Skip suggested Lead Chairs try to come to CPIN wide agreement on whether to do portfolio or not, and set a deadline to shoot for --- Fall 18? Fall 19?*

##### *Cyber Security-Information Assurance Program Outcomes:*

* *Apply standard statistical inference procedures to draw conclusions from data.*
* *Demonstrate proficiency in the use of scripting languages to write simple scripts including simple linear and looping scripts.*
* *Write simple and compound conditions within a programming language or similar environment.*
* *Identify the bad actors/entities in cyberspace, compare and contrast their resources, capabilities/techniques, motivations, and aversion to risk.*
* *Simulate different types of attacks and their characteristics.*
* *List the first principles of security and describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies. Illustrate basic security design fundamentals that help create systems that are worthy of being trusted.*
* *Describe potential system attacks and the actors/entities that might perform them and choose the appropriate cyber defense tools, methods and components to demonstrate cyber defense methods to prepare a system to repel attacks and deploy appropriate measures in the event of a system breach.*
* *Demonstrate the fundamental concepts of information assurance/cyber defense that can be used to provide system security.*
* *Construct the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.*
* *Describe strengths and weaknesses, modes, and issues that have to be addressed in an implementation and describe how cryptography can be used.*
* *Use the hardware components of modern computing environments and their individual functions.*
* *Describe and apply the fundamental and higher concepts, technologies, components and issues related to communications and data networks.*
* *List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.*
* *Describe the responsibilities related to the handling of information about vulnerabilities and how the type of legal dispute including civil, criminal, and private affects the evidence used to resolve industry wide issues.*
* *Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity operating system.*

**Add each additional agenda item**

1. *Consumable fees (attached)*

*Only one we have is 106 w UCertify*

*Added materials for CCNA Security / CSIA 216 materials will be “free”? What will we need – what will costs be – and will they be a fee?*

1. *Regional Program Initiatives*
	1. *Purdue NW partnership. Scholarship opportunity for 2nd yr. at Ivy and 3/4 years at Purdue through CAE*
	2. *Middle Georgia state articulation. No update from Pam. They are also CAE4y. Matt E says we can do these things as we wish – but time consuming.*
	3. *Talked about the cybersecurity website and how we need to be able to edit the page to add/remove/edit activities, seminars, etc. Tracy Allen is the person (for all programs).*

*Perhaps we need a committee to make sure each program’s activities are listed in a central space (speaker at Sellersburg, event in Columbus, etc.) Discussion of our own URL that we can better control – organize – etc. Matt E says we cant control, but that the marketing people are very amenable. So a mock-up. Maybe input from VISC and/or SDEV …. perhaps need a group to just play with ideas . . . perhaps meet after the meetings on Fri 9/29? Will suggest lead chairs as available discuss after TechPoint on Friday 9/29*

*Topics Advisors Should Know Relevant to the Program*

*a) NETI105 and ITSP135 should be face to face, or synchronous online for best student outcomes*

*b) ITSP135 is a critical path*

*c) First semester (13 credit hour) sequence (INFM109, ITSP135, SDEV120, ENGL111, IVYT115)*

*Pam brought up the desire to reduce CSIA courses from CSIA courses from 4CO to 3CO. Discussion ensued. Many issues, some beyond CPIN. Will discuss with lead chairs.*

**COLLEGEWIDE COURSE OUTLINE OF RECORD**

**CSIA 105, INTRODUCTION TO CYBER SECURITY/INFORMATION ASSURANCE**

COURSE TITLE: Introduction to Cyber Security/Information Assurance

COURSE NUMBER: CSIA 105

PREREQUISITES: ITSP 135 Hardware/Software Support

SCHOOL: Computing and Informatics

PROGRAM: Cyber Security/Information Assurance

CREDIT HOURS: 3

CONTACT HOURS: Lecture: 3

DATE OF LAST REVISION: Fall, 2015

EFFECTIVE DATE OF THIS REVISION: Fall, 2018

CATALOG DESCRIPTION: The students will explore the field of Cyber Security/Information Assurance focusing on the technical and managerial aspects of the discipline. Students will be introduced to the basic terminology, concepts, and best practices of computer/network security and the roles and responsibilities of management/security personnel. The students will learn the technologies used and techniques involved in creating a secure computer networking environment including authentication and the types of attacks against an organization.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Use virtual machine technology to test security tools in a sandbox environment.
2. Identify security threats to network services, devices, traffic and data.
3. Use tools to secure network communications.
4. Monitor the security infrastructure with current industry standard utilities.
5. Discuss roles and responsibilities of information security personnel.
6. Use cryptography and public key infrastructures to secure remote access, wireless, and virtual private networks.
7. Implement “defense in depth” to shield against network attacks.
8. Discuss computer forensics and incident response.
9. Discuss basic characteristics of information.
10. Discuss information security as it applies to application guidance, and policies.
11. Describe the legal elements of investigative authorities in criminal prosecution, evidence collection, and evidence preservation.
12. Understand the concepts of trust through assurance, mechanism, and policy.
13. Understand the practical performance measures employed in designing security measures and programs.
14. Describe and discuss administrative security procedural controls.
15. Discuss the auditing and monitoring of security systems.

 COURSE CONTENT: Topical areas of study include –

|  |  |
| --- | --- |
|   |  |
| Security reviews Effectiveness of security programs Investigation of security breaches Monitoring systems for accuracy and abnormalities Privacy Accountability controls Audit trails and logs Software design standards  | Denial of service, spoofing, and hijacking Networking Defense in depth Cryptography Security Technologies Legal, ethical and professional issues in Information Security Attribution Destruction of media  |

HOW TO ACCESS THE IVY TECH COMMUNITY COLLEGE LIBRARY:

The Ivy Tech Library is available to students on- and off-campus, offering full text journals and books and other resources essential for course assignments. Go to <http://www.ivytech.edu/library/>and choose the link for your campus.

ACADEMIC HONESTY STATEMENT:

The College is committed to academic integrity in all its practices. The faculty value intellectual integrity and high standard of academic conduct. Activities that violate academic integrity undermine the quality and diminish the value of educational achievement.

Cheating on papers, tests or other academic works is a violation of College rules. No student shall engage in behavior that, in the judgment of the instructor of the class, may be construed as cheating. This may include, but is not limited to, plagiarism or other forms of academic dishonesty such as acquisition without permission of tests or other academic work. This includes students who aid and abet as well as those who attempt such behavior.

COPYRIGHT STATEMENT:

Students shall adhere to the laws governing the use of copyrighted materials. They must insure that their activities comply with fair use and in no way infringe on the copyright or other proprietary rights of others and that the materials used and developed at Ivy Tech Community College contain nothing unlawful, unethical, or libelous and do not constitute any violation of any right of privacy.

ADA STATEMENT:

Ivy Tech Community College seeks to provide reasonable accommodations for qualified individuals with documented disabilities. If you need an accommodation because of a documented disability, please contact the Office of Disability Support Services.

If you will require assistance during an emergency evacuation, notify your instructor immediately. Look for evacuation procedures posted in your classroom.

|  |  |  |
| --- | --- | --- |
|  **COR Review Checklist** – *Attach a COR Checklist for each new or revised course. Include the COR in packet. At a minimum, consideration of the questions below should be evident in meeting notes.***Standard Criteria** | **Statewide Lead Chair Confirmation** | **Curriculum Mentor Confirmation** |
|  |  |  |
| Title of the Course | pcs |  |
| Course Number* If new course, has the course number been approved by Registrar?
* If this course is replacing an existing course, what is the teach-out plan?
 | pcs |  |
| Pre-Requisites* Review for Currency
* If changed, do the new pre-requisites create any barriers in the curriculum sequence?
 | pcs |  |
| Contact Hours* Please refer to [ASOM 6.14](https://www.ivytech.edu/files/ratio-contact-to-credit-hours.pdf) to ensure correct calculation
 | pcs |  |
| Date of Revision and Effective Date* Updated?
* Appropriate for curriculum timelines?
 | pcs |  |
| Catalog Description* Ensure catalog description includes a broad scope of what will be explored in the course. The catalog description should include approximately 2-4 concise sentences.
 | pcs |  |
| Course Learning Objectives* Are all objectives measureable?
* Do all objectives utilize Bloom’s Taxonomy?
* Is there a balance in the difficulty of cognition levels?
* If this course is a part of a TSAP degree, are the objectives aligned to the degree competencies?
 | pcs |  |
| Course Content* Does the course content reflect the majority of content addressed in the course?
* Is Course Content arranged in alphabetical order?
 | pcs |  |
| Assessment* Does this course have an embedded certification? If so, have you included the standard certification exam statement?
* Are there standard forms of assessment for this course? If so, have you included a description of those assessments?
 | pcs |  |
| Standardized Information* Library
* Academic Honesty Statement
* Copyright and ADA
* Faculty Credentials
 | pcs |  |

**COLLEGEWIDE COURSE OUTLINE OF RECORD**

**CSIA 216, WORKFORCE PREPARATION: CCNA SECURITY CERTIFICATION**

COURSE TITLE: Workforce Preparation: CompTIA Security+ Certification

COURSE NUMBER: CSIA 216

PREREQUISITES: CSIA 215 Perimeter Defense

COREQUISITES: CSIA 215 Perimeter Defense

SCHOOL: Information Technology

PROGRAM: Security/Information Assurance

CREDIT HOURS: 1

CONTACT HOURS: Lecture: 1

DATE OF LAST REVISION: Fall, 2018

CATALOG DESCRIPTION: The workforce preparation course is focused on the CCNA Security certification. Students can use this course as preparation leading to the certification or keeping the certification up to date. The preparation is designed to be a continued validation of one’s expertise and a tool to expand one’s skillset. Preparation includes practice tests and assignments based on the certification exam. Students are required to demonstrate course objectives through the appropriate certification exam preparation materials and completion of the appropriate certification exam at the end of the course. The fee for the certification exam is assessed upon enrollment in the course.

MAJOR COURSE LEARNING OBJECTIVES:Upon successful completion of this course, the student will be expected to:

1. Apply skills necessary to prepare for workforce employment.
2. Examine the objectives of the certification objectives.
3. Plan the approach to certification exam taking skills.
4. Explore the skills required in preparation for the workforce and the certification exam.

COURSE CONTENT: Topical areas of study include –

Skills evaluation

Skills development

Workforce needs

Certification preparation

Certification objectives

*CERTIFICATION ASSOCIATED COURSE:*

*All students enrolled in this course are required to take the corresponding certification exam at some point on or before the last day of the course. The seat, allowing the student to take the certification exam, was paid for by the student as consumable fee at the beginning of the course, along with tuition. If the student does not take the exam, the student will earn an “F” for the class. If the student takes the exam and does not pass the exam, the highest grade possible in the course is a “B.” However, if the student passes the exam, it will account for 20% of the total course grade. Students will be assessed the current fee in order to take the examination. This consumable fee will be automatically encumbered upon enrollment in the course.*

*CERTIFICATION/LICENSURE DISCLAIMER:*

*Ivy Tech cannot guarantee that any student will pass a certification or licensing exam. Your success will be determined by several factors beyond the instruction you are given in the classroom including your test-taking skills, your willingness to study outside of class, and your satisfactory completion of appropriate practice exams. Certification exam questions are drawn from databases of tens of thousands of possible questions and no two people are asked exactly the same progression of questions. Therefore, a thorough understanding of the subject matter is required. The goal of Ivy Tech in providing a certification exam studies class is to assist you in understanding the material sufficiently to provide a firm foundation for your studies as you prepare for the exam.*

HOW TO ACCESS THE IVY TECH COMMUNITY COLLEGE LIBRARY:

The Ivy Tech Library is available to students’ on- and off-campus, offering full text journals and books and other resources essential for course assignments. Go to <http://www.ivytech.edu/library/>and choose the link for your campus.

ACADEMIC HONESTY STATEMENT:

The College is committed to academic integrity in all its practices. The faculty value intellectual integrity and a high standard of academic conduct. Activities that violate academic integrity undermine the quality and diminish the value of educational achievement.

Cheating on papers, tests or other academic works is a violation of College rules. No student shall engage in behavior that, in the judgment of the instructor of the class, may be construed as cheating. This may include, but is not limited to, plagiarism or other forms of academic dishonesty such as the acquisition without permission of tests or other academic materials and/or distribution of these materials and other academic work. This includes students who aid and abet as well as those who attempt such behavior.

COPYRIGHT STATEMENT:

Students shall adhere to the laws governing the use of copyrighted materials. They must insure that their activities comply with fair use and in no way infringe on the copyright or other proprietary rights of others and that the materials used and developed at Ivy Tech Community College contain nothing unlawful, unethical, or libelous and do not constitute any violation of any right of privacy.

ADA STATEMENT:

Ivy Tech Community College seeks to provide reasonable accommodations for qualified individuals with documented disabilities. If you need an accommodation because of a documented disability, please contact the Office of Disability Support Services.

If you will require assistance during an emergency evacuation, notify your instructor immediately. Look for evacuation procedures posted in your classroom.

**COR Review Checklist** – *Attach a COR Checklist for each new or revised course. Include the COR in packet. At a minimum, consideration of the questions below should be evident in meeting notes.*

|  |  |  |
| --- | --- | --- |
| **Standard Criteria** | **Statewide Lead Chair Confirmation** | **Curriculum Mentor Confirmation** |
|  |  |  |
| Title of the Course | Pcs |  |
| Course Number* If new course, has the course number been approved by Registrar?
* If this course is replacing an existing course, what is the teach-out plan?
 | The course number has not been approved by the registrar. I don’t know who to ask about that. |  |
| Pre-Requisites* Review for Currency
* If changed, do the new pre-requisites create any barriers in the curriculum sequence?
 | Pcs |  |
| Contact Hours* Please refer to [ASOM 6.14](https://www.ivytech.edu/files/ratio-contact-to-credit-hours.pdf) to ensure correct calculation
 | Pcs |  |
| Date of Revision and Effective Date* Updated?
* Appropriate for curriculum timelines?
 | Pcs |  |
| Catalog Description* Ensure catalog description includes a broad scope of what will be explored in the course. The catalog description should include approximately 2-4 concise sentences.
 | Pcs |  |
| Course Learning Objectives* Are all objectives measureable?
* Do all objectives utilize Bloom’s Taxonomy?
* Is there a balance in the difficulty of cognition levels?
* If this course is a part of a TSAP degree, are the objectives aligned to the degree competencies?
 | Pcs |  |
| Course Content* Does the course content reflect the majority of content addressed in the course?
* Is Course Content arranged in alphabetical order?
 | Pcs |  |
| Assessment* Does this course have an embedded certification? If so, have you included the standard certification exam statement?
* Are there standard forms of assessment for this course? If so, have you included a description of those assessments?
 | Pcs |  |
| Standardized Information* Library
* Academic Honesty Statement
* Copyright and ADA
* Faculty Credentials
 | Pcs |  |