



## **Agreement between Hagerstown Community College and Capitol College for the Articulation of the A. A. S. Cybersecurity to the B.S. in Information Assurance**

### **PURPOSE**

This agreement facilitates the transfer of **Hagerstown Community College** (HCC) students who graduate with an A.S. in Cybersecurity to the B.S. in Information Assurance (BSIA) at **Capitol College** (CC). This agreement defines the terms of the transfer.

The three goals inherent in the agreement are to:

1. Facilitate students' transfer from the A.S. in Cybersecurity at HCC to the BSIA program at CC as efficiently as possible.
2. Establish a clear set of understandings and expectations for institutions, students, and their respective degrees.
3. Establish a pathway for HCC's A.S. in Cybersecurity graduates to earn a Bachelor's degree in information Assurance as a means to advance their careers in information assurance.

### **Articulation Agreement**

Hagerstown Community College (HCC) and Capitol College (CC) agree to offer articulated programs leading to the award of an A.S. in Cybersecurity and a B.S. in Information Assurance. The two institutions further agree that students from HCC, under the articulation agreement, may transfer credits earned for the A.S. in Cybersecurity toward the B.S. in Information Assurance at CC. The following general principles guide the implementation of this agreement:

1. The program is designed for graduates of the A.S. degree in Cybersecurity at HCC to transfer specific courses in which they have earned the grade of C or higher. The number of courses transferred may not exceed 60 credit hours. The credit hours transferred from HCC contribute to the fulfillment of the 127 credit hours required for baccalaureate completion (BSIA) at Capitol College.
2. The course transfer table included with this document specifies courses that will transfer from HCC to Capitol College.

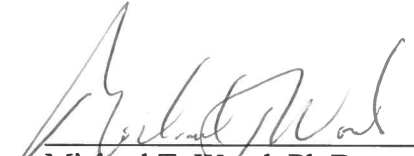
3. Capitol College will consider, on a case-by-case basis, accepting credit from non-direct classroom instruction (including CLEP, AP, and other nationally recognized standardized examination scores).
4. For a smooth transition, students at HCC may start taking courses in the Information Assurance program at CC while they are completing the A.S. degree at HCC. However, students are advised to complete the A.S. degree prior to officially transferring to CC.
5. If HCC and CC develop a dual enrollment program, this articulation agreement will not prevent students from applying for, participating in, or receiving the benefits of dual enrollment. Those students would then be subject to the dual enrollment program criteria.
6. HCC students who complete the A.S. in Cybersecurity will be given consideration for financial assistance and will be eligible to compete for academic scholarships at CC. Students who finish the A. S. degree with a GPA of 3.0 or higher and subsequently attend CC full-time will be considered for larger scholarship under a special program.
7. At the request of the HCC Academic Dean, the CC Academic Dean will provide general information as the academic progress of HCC students enrolled in the CC BSIA program. Any feedback must adhere to FERPA.
8. HCC and CC agree to monitor the performance of this agreement and to revise as necessary.
9. HCC and CC agree to publicize this agreement.
10. The course transfer table is subject to annual review for updating and revising as necessary by the appropriate HCC and CC officials without affecting the signed agreement.
11. Either party may terminate the agreement with 60 days advance written notice to the other. Termination of the agreement will not affect any students currently enrolled in the A.S. in Cybersecurity program who are taking courses at CC or who have been accepted into the BSIA at CC.
12. This agreement becomes effective on the date that the last authorizing party has signed the agreement. The last signer will write the date on the signature page.


**Agreement between Hagerstown Community College and Capitol College  
for the Articulation of the A. A. S. Cybersecurity to the  
B. S. in Information Assurance**


**Authorizing Signatures**


This agreement is authorized for implementation on the


14 day of September, 2014  
date month

  
Michael T. Wood, Ph.D.  
President, Capitol College

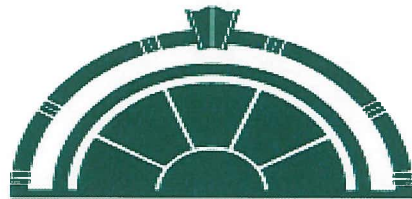
  
Guy Altieri, Ed.D.  
President, Hagerstown Community College

  
W. V. Maconachy, Ph. D.  
VP for Academic Affairs, CAO

  
C. David Warner, Ed.D.  
VP for Academic Affairs

  
Helen G. Barker, D.M.  
Dean Business/Information Sciences

  
Margaret C. Spivey  
Director Technology/Computer Studies



**HAGERSTOWN  
COMMUNITY  
COLLEGE**

**Cybersecurity, A.S.**

Student ID: \_\_\_\_\_  
 Student Name: \_\_\_\_\_  
 Adviser Name: \_\_\_\_\_

Catalog: 2014-2015 Catalog  
 Program: Cybersecurity, A.S.  
 Minimum Credits Required: \_\_\_\_\_

**Cybersecurity, A.S.**

The transfer program in Cybersecurity is designed for students who plan to transfer to a four-year institution and major in Cybersecurity, Information Assurance, or a related field. Students should identify an intended transfer institution as early as possible and complete appropriate courses. Students should always confer with advisors and transferring institutions for specific requirements as these are subject to change.

- View the Cybersecurity Fact Sheet.

**Program Pathway**

First Year Fall			First Year Spring		
Course Number	Course Name	Credits	Course Number	Course Name	Credits
Gen Ed	ENG 101 - English Composition	3	Gen Ed	Arts & Humanities Gen Ed	3
Gen Ed	Math Gen Ed	3	Gen Ed	Biological/Physical Science Gen Ed (of your two Science requirements, one must have a lab)	3
CYB 101	Introduction to Cybersecurity	3	IST 154	Networking Basics	3
CSC 132	Introduction to C and C++ Programming	3	IST 160	Introduction to Security Fundamentals	3
Restricted Elective	Choose in consultation with an advisor	3	Restricted Elective	Choose in consultation with an advisor	3
<b>TOTAL</b>		<b>15</b>	<b>TOTAL</b>		<b>15</b>
Second Year Fall			Second Year Spring		
Course Number	Course Name	Credits	Course Number	Course Name	Credits
Gen Ed	English Gen Ed	3	Gen Ed	Diversity Gen Ed	3
Gen Ed	Biological/Physical Science Gen Ed (of your two Science requirements, one must have a lab)	4	Gen Ed	Behavioral/Social Sciences Gen Ed in a different discipline from the first	3
Gen Ed	Behavioral/Social Sciences Gen Ed	3	Gen Ed	Arts & Humanities Gen Ed in a different discipline from the first	3
CYB 210	Ethics in the Information Age	3	CYB 225	Tactical Perimeter Defense	3
IST 166	Computer Forensics I - Principles and Practices	3	Free Elective	Choose in consultation with an advisor	2
<b>TOTAL</b>		<b>16</b>	<b>TOTAL</b>		<b>14</b>

**General Education Requirements (31-32 Credits)**

**Arts/Humanities**

- Select two courses in different disciplines from approved General Education course list (6 Credits)

**Behavioral/Social Sciences**

- Select two courses in different disciplines from approved General Education course list (6 Credits)

**Biological/Physical Science**

- Select two courses from approved General Education course list - one must be a laboratory course (7-8 Credits)

**Diversity**

- Select a course from the approved General Education course list in the Diversity category (3 Credits)

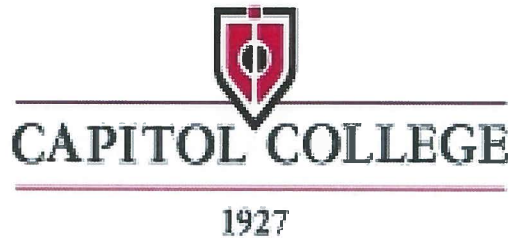
**English**

Course Name	Credits	Term Taken	Grade	Gen Ed
ENG 101 - English Composition	(3 Credits)			
Select an other ENG course from approved General Education course list (3 Credits)				



## Cybersecurity, A.S.

<b>Mathematics</b>				
Course Name	Credits	Term Taken	Grade	Gen Ed
MAT 101 - College Algebra	(3 Credits)			
Or any higher level Mathematics course (3 Credits)				
<b>Program Requirements (21 Credits)</b>				
Course Name	Credits	Term Taken	Grade	Gen Ed
CSC 132 - Introduction to C and C++ Programming	(3 Credits)			
CYB 101 - Introduction to Cybersecurity	(3 Credits)			
CYB 210 - Ethics in the Information Age	(3 Credits)			
CYB 225 - Tactical Perimeter Defense	(3 Credits)			
IST 154 - Networking Basics	(3 Credits)			
IST 160 - Introduction to Security Fundamentals	(3 Credits)			
IST 166 - Computer Forensics I - Principles And Practices	(3 Credits)			
<b>Restricted Electives (6 Credits)</b>				
Electives should be selected in consultation with an advisor to satisfy career goals or a transfer college curriculum. Select 6 credits from the following list:				
Course Name	Credits	Term Taken	Grade	Gen Ed
ADJ 101 - Introduction to Criminal Justice	(3 Credits)			
CSC 232 - Advanced C++ Programming	(3 Credits)			
CYB 240 - Ethical Hacking Fundamentals	(3 Credits)			
IST 266 - Computer Forensics II - Investigations Practices	(3 Credits)			
<b>Free Electives (2 Credits)</b>				
Electives should be selected in consultation with an advisor to satisfy career goals or a transfer college curriculum.				
<b>Degree Requirement (60 Credits)</b>				
<b>Notes:</b>				



## Degree Requirements (BSIA)

### Bachelor of Science - 127-130 credits

**Programming and Computers - 31 Credits**

<u>CS-130 Computer Science Fundamentals I</u>	4
<u>CS-150 Introduction to Programming Using C</u>	3
<u>CS-220 Database Management</u>	3
<u>CS-230 Computer Science Fundamentals II</u>	3
<u>CS-320 Database Administration</u>	3
<u>CS-418 Operating Systems</u>	3
<u>CT-152 Introduction to Unix</u>	3
<u>CT-206 Scripting Languages</u>	3
<u>CT-240 Internetworking with Routers and Switches</u>	3
<u>SE-458 Senior Project</u>	3

**Information Assurance - 27 Credits**

<u>IAE-201 Introduction to Information Assurance Concepts</u>	3
<u>IAE-301 Comprehensive Computer and Network Security I*</u>	3
<u>IAE-315 Secure System Administration and Operation*</u>	3
<u>IAE-321 Applied Wireless Network Security*</u>	3
<u>IAE-325 Secure Data Communications and Cryptography*</u>	3
<u>IAE-402 Introduction to Incident Handling and Malicious Code*3</u>	3
<u>IAE-405 Malware Analysis/Reverse Engineering*</u>	3
<u>IAE-406 Digital Forensics and the Investigative Process*</u>	3
<u>IAE-410 Penetration Testing*</u>	3

**Management - 6 Credits**

<u>BUS-174 Introduction to Business and Management</u>	3
<u>BUS-301 Project Management</u>	3

**Mathematics and Sciences - 17 Credits**

<u>MA-114 Algebra and Trigonometry</u>	4
<u>MA-124 Discrete Mathematics</u>	3
<u>MA-128 Introduction to Statistics</u>	3
<u>MA-261 Calculus I</u>	4
Science elective (1)**	3

**English Communications - 9 Credits**

<u>EN-101 English Communications I</u>	3
<u>EN-102 English Communications II</u>	3

<u>EN-408 Writing Seminar in Technical Research</u>	3
<b>Humanities/ Social Sciences - 18-19 Credits</b>	
<u>FS-100 Freshman Seminar</u>	1
<u>HU-331or HU-332 Arts and Ideas</u>	3
<u>SS-351 Ethics</u>	3
Humanities/History/Philosophy electives (2)**	6
Social Sciences electives (2)**	6
<b>General Electives 19-21 Credits</b>	

\* Offered online only.

\*\* See appropriate department for approved list.

All bachelor of science degrees require a minimum of 27 credits at the 300-level or above.

**Course Transfer Table**  
**A. S. Cybersecurity at Hagerstown Community College**  
**B. S. in Information Assurance at Capitol College**  
*Effective Fall 2014*

Students graduating from the Hagerstown Community College (HCC) with an A. S. degree in Cybersecurity may transfer up to 60 credit hours, with a minimum grade of “C” required in each course transferred, towards the Bachelor of Science in Information Assurance (BSIA) degree at Capitol College (CC). This table specifies course equivalents up to 60 credits. Additional courses completed at HCC will be considered and accepted on a case by case basis, with the total transfer not to exceed 60 credits. This table may be revised as necessary with the mutual consent of both institutions without affecting the basic articulation agreement.

<b>Capitol College</b>	<b>Hagerstown Community College</b>
<b>Program Requirements (21 Credits)</b>	
<p><b>CS-150 Intro to Programming using C (3)</b></p> <p>This introductory course in programming will enable students to understand how computers translate basic human instructions into machine executable applications. The language of choice for this course is C. The C syntax that will be covered includes functions; variables and memory allocations including pointer notation; conditional statements and looping. Students will also learn binary to hexadecimal and decimal conversions along with basic computer architecture. Memory management, data input output and file manipulations will be among some other topics discussed and applied during this course. (3-1-4)</p>	<p><b>CSC 132 Intro to C and C ++ Programming</b></p> <p>This course provides students with a thorough understanding of the basic principles of C and C++. It covers the basic syntax and structure of the language with an emphasis on problem solving techniques. Students create programs using input/output statements; if, while, do while, and for-loop logic structures; arrays, functions, pointers and reference variables, record structures, header files, file I/O, and basic object-oriented programming techniques. Students will be able to recognize and correct common programming errors. Course fee required. Total of 45 hours of lecture.</p>
<p><b>IAE 201 Introduction to IA Concepts (3)</b></p> <p>This course covers topics related to administration of network security. Topics include a survey of encryption and authentication algorithms; threats to security; operating system security; IP security; user authentication schemes; web security; email security protocols; intrusion detections; viruses; firewalls; Virtual Private Networks; network management and security policies and procedures. Laboratory projects are assigned as part of the homework requirements. Corequisites: MA-110 or MA-114 or MA-261 and EN-101. (3-0-3)</p>	<p><b>CYB 101 Intro to Cybersecurity</b></p> <p>Introduction to Cybersecurity is a beginning guide for anyone interested in computer security. Core security topics such as vulnerability assessment, virus attacks, hacking, spyware, network defense, passwords, firewalls, VPNs and intrusion detection are covered. Crucial issues from industrial espionage to cyberbullying are discussed. Additionally, students are expected to learn the latest computer attacks and counter measures. Course fee required. 45 contact hours.</p>



<p><b>SS 351 Ethics (3)</b></p> <p>This course is designed to help students improve their ability to make ethical decisions in business. This is done by providing a framework that enables the student to identify, analyze, and resolve ethical issues that arise when making decisions in business. Case analysis is a primary tool of this course. Prerequisite: EN-102. (3-0-3)</p>	<p><b>CYB 210 Ethics in the Information Age</b></p> <p>In this course, students become familiar with the large impact ethical issues have on the use of information technology in the modern business world. Course includes coverage of cloud computing, cyber terrorism, social networking Web sites, and infringement of intellectual property, security risks, identity theft, employee surveillance, privacy, compliance, and ethics of IT corporations, including the use of foreign workers, outsourcing, and green computing. Ethics and the Information Age is a study of ethics and moral philosophy as a means for providing a framework for ethically grounded decision making in the information age. Course fee required. 45 contact hours</p>
<p><b>Elective (3)</b></p>	<p><b>CYB 225 Tactical Perimeter Defense</b></p> <p>This course examines the critical defensive technologies needed to secure network perimeters. Coverage includes network security threats and goals, advanced TCP/IP concepts, router security, intrusion detection, firewall design and configuration, IPSec and virtual private network (VPN) design, and wireless design and security. 45 contact hours.</p>

<p><b>Elective (3)</b></p>	<p><b>IST 154 Networking Basics</b></p> <p>Students become familiar with networking terminology and concepts. This course introduces the fundamental building blocks that form a modern network, such as protocols, topologies, hardware, and network operating systems. It then provides coverage of the most important concepts in contemporary networking, such as client/server architecture, TCP/IP, Ethernet, wireless transmission, and security. A current network operating system is used to examine managing users, groups and devices. Additional networking operating systems are surveyed. Also included are discussions of the OSI model, subnets, troubleshooting, and networking integrity. Course objectives map to the CompTIA Net+ Exam. Successful completion of a DOS or Windows course is strongly recommended. May be offered in lecture, hybrid, or online format. Course fee required. Total of 45 hours of lecture.</p>
<p><b>IAE 301 Comprehensive Security (3)</b></p> <p>Building on IAE-201, this course provides learners with detailed and hands-on knowledge of computer and network security. The course emphasizes current topics such as network security, compliance and operational security, threats and vulnerabilities, application security, access control, as well as cryptography. Additionally, underlying theory and concepts are presented in order to extend learners' understanding of computer and network security. Weekly laboratory exercises are utilized to reinforce practical, real-world security techniques. Classes are a mixture of lecture, current event discussions, and laboratory exercise review and will prepare learners for the CompTIA Security+ certification. Pre-requisite: IAE-201 (3-0-3)</p>	<p><b>IST 160 Introduction to Security Fundamentals</b></p> <p>This is a first course in the fundamentals of information, computer and network security. The course discusses common security issues, identifies methods of assessing systems to identify critical data and presents tools and techniques for securing computers and networks. Course objectives map to the CompTIA Security+ Exam and include general security concepts, communication security, infrastructure security, basics of cryptography and operational/organizational security. May be offered in lecture, hybrid, or online format. Total of 45 hours of lecture</p>

<p><b>Elective (3)</b></p>	<p><b>IST 166 Computer Forensics I</b></p> <p>Computer Forensics I is an introductory course in electronic evidence; what types exist, where it may be found and the methods to investigate it. Discussions include legal, technical, investigative, intrusive attacks and ethical issues. First course in the fundamentals of information, computer and network security. The course is presented in lecture, lab and discussion format. Case studies are included. May be offered in lecture, hybrid, or online format. Total of 45 hours of lecture</p>
<p><b><i>Restricted Electives (6 Credits)</i></b></p>	
<p><b>Elective (3)</b></p>	<p><b>ADJ 101 Introduction to Criminal Justice</b></p> <p>This course provides an overview of the history, philosophy, and development of police, courts, and corrections in a democratic society. Identification and operations of local, state, and federal agencies are covered within a criminal justice career orientation. Total of 45 hours of lecture.</p>
<p><b>CS 230 Computer Science Fundamentals II (3)</b></p> <p>Advance pointers and dynamic memory usage. Concepts of object-oriented design and programming. Includes classes, friend functions, templates, operator overloading, polymorphism, inheritance, exception handling, containers, iterators and the standard template library. Applications involve the use of simple data structures such as stacks, queues, linked lists and binary trees. Recursion, searching and sorting algorithms. The above concepts are implemented through a series of hands-on programming projects, all of which are completed as part of the homework requirements. Prerequisite: CS-130. (3-0-3)</p>	<p><b>CSC 232 Advanced C ++ Programming</b></p> <p>This course continues to introduce students to object-oriented programming (OOP) using C++ and Visual C++. It builds on the foundation of <u>IST 132/CSC 132</u>. Students learn OOP concepts such as classes, friends, and templates and use these to build a program designed to run under a Microsoft Windows environment. Using a hands-on approach, students have the opportunity to design, code, and test object-oriented applications. Additional time outside of class will be necessary to write programs. Course fee required. Total of 45 hours of lecture.</p>

<p><b>IAE 410 Penetration Testing (3)</b></p> <p>This course explores the foundational concepts, methods and techniques in preparing and conducting penetration tests. Throughout the course students are introduced to various tools as well as unravel complex methods for exploiting client-side, service side and privilege escalation attacks. Most importantly students learn how to construct a final report outlining discovered vulnerabilities, make suggested recommendations to remediate and/or mitigate those vulnerabilities. Students also learn how to describe the findings wherein non-technical personnel understand the ramifications of these vulnerabilities in a business sense. Prerequisites: CT-240 and IAE-315. Recommended Co-requisite: IAE-402. (3-0-3)</p>	<p><b>CYB 240 Ethical Hacking II</b></p> <p>In this course students will become familiar with offensive network security, ethical hacking and responsibility and network defense and counter measures. Students will study testing, scanning and securing information systems. Topics include hacker methodology and tools, how they operate and how to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Course fee required. Total 45 contact hours.</p>
<p><b>IAE 406 Forensic Investigative Processes (3)</b></p> <p>Students explore forensics and the investigation processes. Students explore current computer forensics tools, conduct live computer forensic analysis, conduct e-mail investigations, recovery of graphics files and data carving, and engage in report writing for high-tech investigations. Prerequisites: IAE-315 and CT-152. (3-0-3)</p>	<p><b>IST 266 Computer Forensics II</b></p> <p>Computer Forensics II provides a foundation for those seeking skills to investigate criminal and civil cases. Hands-on experience is provided with operating systems, computer hardware and forensic software. The course is presented in lecture, lab and discussion format. Case studies are examined. Course content includes data acquisition, processing crime scenes, computer forensics tools, and recovering graphics files. Total of 45 hours of lecture.</p>
<p><b><i>Mathematics (3 Credits)</i></b></p>	

<p><b>Elective</b></p>	<p><b>MAT 101 College Algebra</b>  This course is a problem solving approach to the nature of mathematics as a logical system. The structure of the number system is developed axiomatically and extended by logical reasoning to cover essential algebraic topics: algebraic expression, functions, and theory of equations. Approximately two additional hours per week should be expected using MyMathLab to complete online homework and tutorial programs. In addition to class time, students are required to do an additional 1 hour of math study in the Learning Support Center. Total of 60 contact hours.</p>
------------------------	--

***General Education (31-32 Credits)***

<p><b>EN 101 English Communications I (3)</b></p> <p>This introductory college-level course focuses on effective oral and written communication skills and the development of analytical abilities through various reading and writing assignments. Students must be able to demonstrate competence in writing mechanics, including grammar, structure and logical content development when writing essays, summaries, and short reports. Rhetorical modes may include description, compare/contrast, personal experience, definition, illustration and process demonstration. Oral presentation skills are developed through the delivery of two speeches on related topics. (3-0-3)</p>	<p><b>ENG 101 English Composition</b></p> <p>This course examines paragraph and theme development with emphasis on syntax, organization, logical thinking, and diction as a basis for writing. Students are given extensive practice in creating and revising their own compositions. Documentation and plagiarism are discussed. Selected readings may be used.</p> <p>Prerequisite: ENG 100 or appropriate score on placement test. Semesters offered: Fall, Spring, and Summer. 3 Credits</p>
---	--

**EN 102 English Communications II (3)**

This sequel to EN-101 involves more sophisticated reading, writing, speaking, and research assignments. Students must demonstrate competence in writing mechanics, as well as advanced research skills, the ability to handle complex information, and effective team skills. Students write research papers: an information paper, a cause-and-effect paper, an argument paper, and a final research paper. Course includes group work. Presentations are required. Prerequisite: EN-101 (3-0-3)

**ENG Composition and Literature**

This course refines the writing process through the reading and interpretation of literature. Students learn manuscript presentation, inquiry, and research skills by writing a clearly documented research paper. Prerequisite: ENG 101. Semesters offered: Fall, Spring, Summer. 3 Credits