



January 16, 2020

James D. Fielder, Jr., Ph.D.
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Fielder,

I am forwarding the following substantial change to an academic program for Commission review:

Program	HEIGIS	CIP
Cybersecurity, AAS	5101.04	11.1003

This program modification will provide a new selection of electives in Information Assurance and Network Security with the inclusion of an existing introductory Cloud Computing course. Because each area of concentration has been reduced, the areas of concentration in Digital Forensics and Network Security will be removed from the program. Copies of the suspension letters are included with this proposal.

This submission has been thoroughly reviewed within the college and approved by the Board of Trustees. If further information is required, please feel free to contact by email at edabel@csm.md.edu or by phone at 301-934-7846.

Sincerely,

A handwritten signature in black ink, appearing to read "Eileen Abel".

Eileen Abel, Ph.D.
Vice-President of Academic Affairs

La Plata Campus
8730 Mitchell Road, PO Box 910
La Plata, MD 20646
301-934-2251 • 301-870-3008

Leonardtown Campus
22950 Hollywood Road
Leonardtown, MD 20650
240-725-5300

Prince Frederick Campus
115 J.W. Williams Road
Prince Frederick, MD 20678
443-550-6000

Regional Hughesville Campus
6170 Hughesville Station Place
Hughesville, MD 20637
301-539-4730



MHEC
Creating a state of achievement

Cover Sheet for In-State Institutions

New Program or Substantial Modification to Existing Program

Office Use Only: PP#

Institution Submitting Proposal

College of Southern Maryland

Each action below requires a separate proposal and cover sheet.

- | | |
|---|---|
| <input type="radio"/> New Academic Program | <input checked="" type="radio"/> Substantial Change to a Degree Program |
| <input type="radio"/> New Area of Concentration | <input type="radio"/> Substantial Change to an Area of Concentration |
| <input type="radio"/> New Degree Level Approval | <input type="radio"/> Substantial Change to a Certificate Program |
| <input type="radio"/> New Stand-Alone Certificate | <input type="radio"/> Cooperative Degree Program |
| <input type="radio"/> Off Campus Program | <input type="radio"/> Offer Program at Regional Higher Education Center |

Payment ☒ Yes
Submitted: ☐ No

Payment ☐ R*STARS
Type: ☒ Check

Payment Amount: \$250.00

Date Submitted: 1/22/2020

Department Proposing Program	Business, Technology, and Public Service		
Degree Level and Degree Type	Associate of Applied Science		
Title of Proposed Program	Cybersecurity		
Total Number of Credits	60		
Suggested Codes	HEGIS: 5101.04	CIP: 11.1003	
Program Modality	<input checked="" type="radio"/> On-campus <input type="radio"/> Distance Education (<i>fully online</i>)		
Program Resources	<input checked="" type="radio"/> Using Existing Resources <input type="radio"/> Requiring New Resources		
Projected Implementation Date	<input checked="" type="radio"/> Fall <input type="radio"/> Spring <input type="radio"/> Summer Year: 2020		
Provide Link to Most Recent Academic Catalog	URL: https://catalog.csmd.edu/		

Preferred Contact for this Proposal	Name: Bernice Brezina		
	Title: Prof. & Chair, Business, Technology, & Public Service Division		
	Phone: 301-934-7556		
	Email: bdbrezina@csmd.edu		

President/Chief Executive	Type Name: Maureen Murphy, Ph.D.		
	Signature:		Date: 1/21/2020
	Date of Approval/Endorsement by Governing Board: 1/16/2020		

A. Centrality to Institutional Mission and Planning Priorities:
--

This program modification will provide a new selection of electives in Information Assurance, update the Networking courses, and modify the Network Security elective offerings with the inclusion of an existing introductory Cloud Computing course, currently required by students in CSM's Information Services Technology, AAS program.

Because each area of concentration has been reduced to only two 3-credit courses over the past two years, the areas of concentration in Digital Forensics and Network Security will be removed from the program. The areas of concentration will be replaced by 6 credits of elective offerings according to areas of special interest. The elective offerings will include courses in Digital Forensics, Network Security, and Information Assurance.

The modified Cybersecurity AAS program is consistent with CSM's Strategic Priorities, which is to promote student success by providing outstanding education, relevant programming, regional focus, and related support services that help students achieve their goals. The new program will serve to increase graduate satisfaction with job preparation.

This Cybersecurity AAS program will effectively serve a changing student population and emerging workforce. The course selections reflect the changing local workforce needs. The recommendations enclosed are reflections of these elements and are consistent with the College's Vision, "Transforming lives through lifelong learning and service."

The mission statement of the College of Southern Maryland (CSM) inspires the development of close partnerships among the college and its tri-county (Calvert, Charles, and St. Mary's Counties) community stakeholders. The institutional commitment to "enhances lives and strengthens the economic vitality of a diverse and changing region by providing affordable postsecondary education, workforce development, and cultural and personal enrichment opportunities" aligns with the programmatic realities for the Cybersecurity AAS degree.

CSM was recently awarded an NSF Advanced Technological Education (ATE) grant to support the ongoing growth of our Cybersecurity program, specifically for introducing a multidisciplinary aspect to our Cybersecurity program as we continue to contribute to growing the Cybersecurity workforce talent pipeline in the Southern Maryland region.

This proposal presents an updated Cybersecurity AAS degree that aligns perfectly with our NSF grant project. This degree will provide a program that will prepare students for in-demand entry level careers in the broad field of Cybersecurity. The degree will provide students with marketable skills upon completion to enter the work force while also providing some flexibility for students who intend to transfer to a four-year institution.

These program changes do not require any new courses and are already included in the Cybersecurity program or in other related programs. Therefore, we do not anticipate any additional costs incurred by offering this program, other than the expected costs associated with our anticipated program growth shown in Section L. Additionally, our program will be enriched by support from our NSF grant funding, which will support curriculum development and provide benefits to students such as support for industry certification exam prep and testing.

CSM is committed to continuing the support this program administratively, financially, and in

providing the necessary technical support for this program. Our Cybersecurity AAS program has experienced continual growth since inception in 2016 with 16.7% growth between 2017-18. Our Cybersecurity program is supported by an active Program Advisory Council with industry partners who recruit heavily from our college. It is a priority program at CSM, and we continue to support the growth of this in-demand program by dedicating resources including recruiting faculty, supporting professional development, curriculum development, and dedicating resources to our lab facilities and student support services.

Because of our growing local Cybersecurity workforce needs and rapidly evolving threats at home and abroad, we anticipate healthy enrollment numbers for the foreseeable future.

B. Critical and Compelling Regional or Statewide Need as Identified in the State Plan:

The availability of an in-demand Cybersecurity career path in an ever-evolving high technology industry, attracts both traditional and returning adult students, those entering a new field of opportunity as well as workers changing or upgrading skills. These very changes are evident in CSM's own enrollment records. An examination of the demographics of our current student population reflects these realities and supports the needs identified in the current Maryland State Plan for Post Secondary Education.

The degree in Cybersecurity AAS at CSM is consistent with the elements of the 2017-2021 Maryland State Plan for Postsecondary Education. Much of our focus in curriculum development addressed the advisories cited in this document. All the goals were utilized as required criteria but considerable attention was given to the goal of Innovation. "Foster innovation in all aspects of Maryland higher education to improve access and student success." The modified Cybersecurity AAS program will strengthen economic development and help to support a skilled workforce for the Southern Maryland region.

Citations in the State Plan also address the need for post-secondary institutions to strive for academic excellence and effectiveness. Addressing the goal of Success, "Promote and implement practices and policies that will ensure student success.", the Cybersecurity program will provide the opportunity for students to complete this hands-on program in Southern Maryland close to their home and obtain the fundamental knowledge, skills, and practice to be prepared for entry-level employment. The very nature of this charge is to develop student-centered learning bolstered by the partnerships with the various employers in our region, including several major military installations. This format increases experiential learning through hands-on job-related activities assuring workplace readiness.

Formative and summative evaluations are an essential value of the educational process at CSM, and are a viable part of the new CSM program. Students are held to standards that are reflective of academic and professional systems, while the structure and operation of the program provides the environment to support the achievement of these standards.

Local employers have expressed interest in our Cybersecurity program and currently provide substantive experiential learning through their recruitment efforts, internship opportunities, and guest speaker events involving our students. These learning opportunities are extremely important as they provide students enrolled at CSM in the Cybersecurity program both vital experience and opportunities for networking, and will increase chances of getting a job significantly.

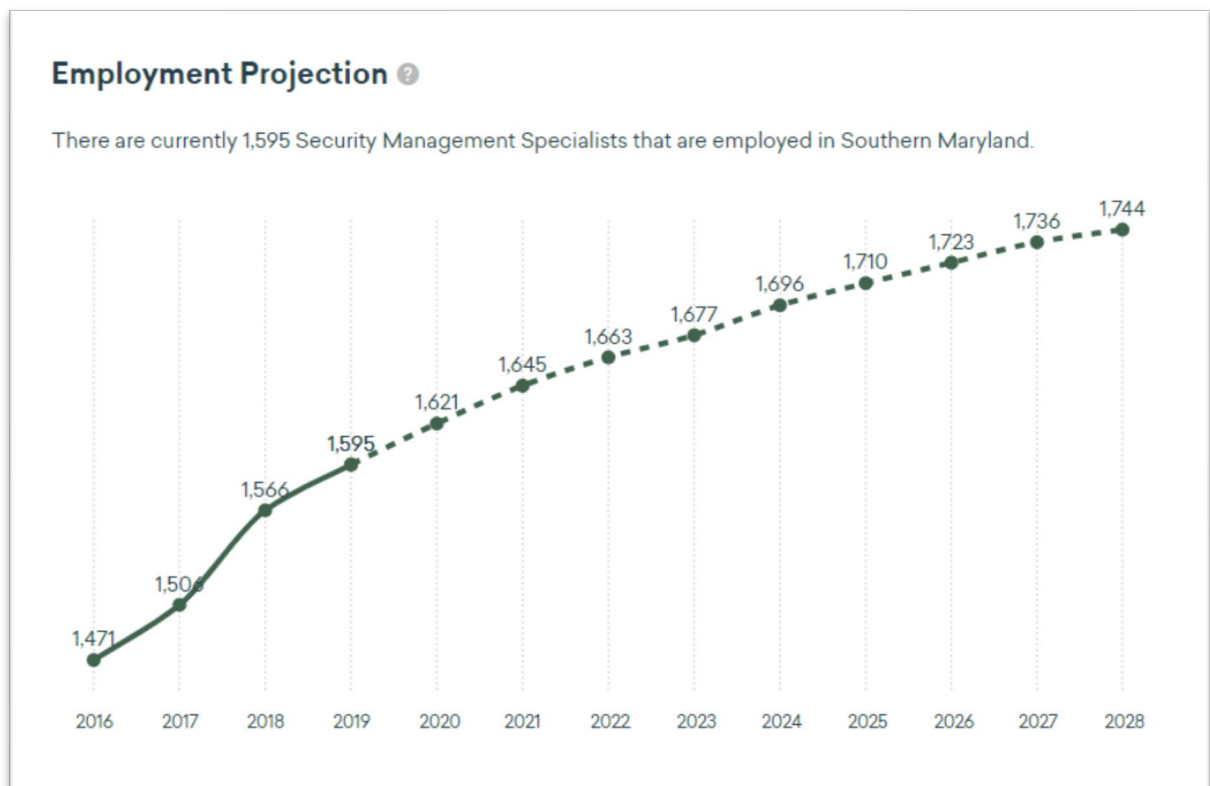
To expand our geographic reach, stimulate enrollment and provide increased access to this improved curricular option, the Cybersecurity program intends to incorporate alternative means

of course delivery. The program intends to provide traditional face-to-face courses complimented by offerings that are hybrid or fully online by form. The College of Southern Maryland has demonstrated success in delivering instruction by alternative methods, increasing flexibility and effective use of new technologies. The Division of Distance Learning and Faculty Development (DLF) supports the faculty in developing high quality, accessible and effective teaching and learning environments. To facilitate these goals, the DLF staff provides service to faculty including planning, consulting, training, and support. The DLF staff makes available the resources necessary to incorporate instructional technologies into their traditional or distance learning courses. As such, the DLF staff will contribute significantly to the delivery of all courses in the Cybersecurity program by providing the faculty with the necessary support structures to enhance student success in their delivery, particularly those identified for distance learning, be the methodology fully on line or hybrid.

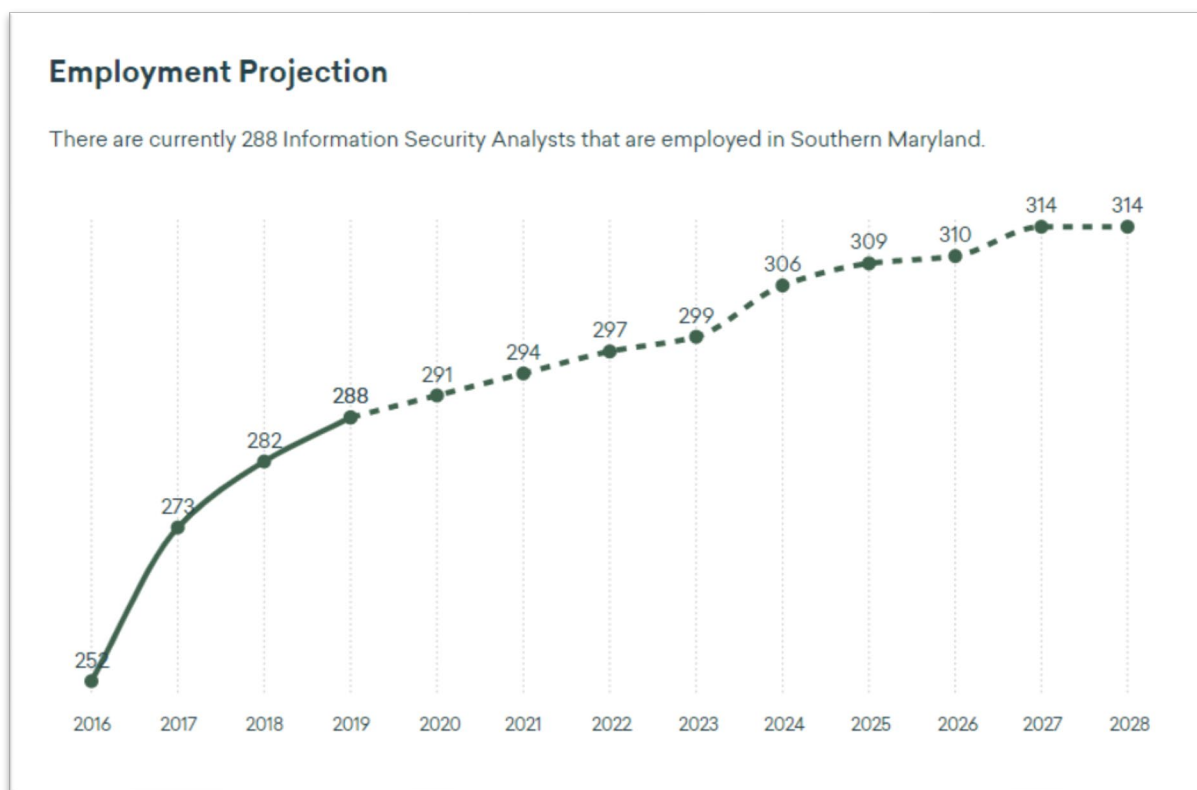
In summary, the Cybersecurity program at the College of Southern Maryland as proposed is consistent with and reflective of the current Maryland State Plan for Postsecondary Education.

C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State:

The Southern Maryland region is expecting a positive growth in Cybersecurity and related jobs. Much of this is driven by the college's close physical proximity to the Patuxent Navy Base in St. Mary's county which employs over 17,000 military, civilian, and contractors, with many of them in technical positions. Below is a representation of expected growth, according to employment project reports retrieved from EMSI in 2019. With the increased reliance of private industry and government reliance on computer systems, this growth is expected to continue to trend up in the foreseeable future. These new jobs provide opportunities for our students to obtain employment in in-demand fields with high starting salaries (approximately \$59K) and median salaries in the 100K range.



Retrieved from Economic Modeling Specialists (EMSI), 2019



Retrieved from Economic Modeling Specialists (EMSI), 2019

D. Reasonableness of Program Duplication:

The Cybersecurity AAS degree program prepares students who are interested in cybersecurity, information systems security, cybersecurity management, digital forensics, and network security to begin developing the skills and knowledge required for a variety of entry-level settings. The degree prepares students with a foundation and basis of knowledge and skills that students may develop further if they choose to continue their studies at a four-year institution. Others may choose to enter the workforce in entry-level, trainee, or internship positions after completing the two-year degree.

Students will be taking courses in this program through several course delivery formats. Students have the option of completing some of their courses in this degree online. Many courses are available in face-to-face, web-hybrid, or online course formats.

Below are the other similar programs in Maryland with Associate Degrees in Cybersecurity or related fields:

Institution	Program
Anne Arundel Community College	CYBERCRIME
Anne Arundel Community College	INFORMATION ASSURANCE & CYBERSECURITY

Baltimore City Community College	CYBER SECURITY AND ASSURANCE
Capitol Technology University	COMPUTER & CYBER OPERATIONS ENGINEERING
Carroll Community College	CYBERSECURITY
Cecil College	CYBERSECURITY
College of Southern Maryland	CYBERSECURITY
Community College of Balt County	CYBERSECURITY
Frederick Community College	CYBERSECURITY
Garrett College	CYBERSECURITY
Hagerstown Community College	CYBERSECURITY
Hagerstown Community College	CYBERSECURITY
Harford Community College	INFORMATION ASSURANCE AND CYBERSECURITY
Montgomery College-All Campuses	CYBERSECURITY
Prince George's Community College	CYBERSECURITY

Cybersecurity-Related Associate Degree Academic Program Offerings in Maryland
Retrieved from MHEC Academic Program Inventory, 2019

E. Relevance to High-demand Programs at Historically Black Institutions (HBIs)

There is no impact to the uniqueness, identities and missions of HBIs. The only other college in the tri-county area is St. Mary's College.

F. Relevance to the identity of Historically Black Institutions (HBIs)

There is no impact to the uniqueness, identities and missions of HBIs. The only other college in the tri-county area is St. Mary's College.

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes (as outlined in COMAR 13B.02.03.10):

CSM's Cybersecurity AAS program was first established in 2015. At the same time, our program was designated as a CAE-CDE 2Y - National Centers of Academic Excellence in Cyber Defense 2-Year Education by the National Security Agency (NSA) and Department of Homeland Security (DHS).

The program is led by Christopher Estes, who holds a current certification as a Certified Information Systems Security Professional (CISSP) as well as a BS degree from American University in Technology of Management in Computer Systems Applications and an MBA from University of Maryland, College Park. He also has many years of professional experience in the field of security and information systems.

Our program faculty is comprised of both full-time and part-time faculty. Our full-time faculty include both new instructors as well as long-time tenured faculty with both academic credentials and industry certifications in the field of cybersecurity, information science, computer science, and related fields. Some of our full-time faculty have current industry experience in the cybersecurity field as well. We have full-time faculty members who are Cisco Certified Academy Instructors and others with various cybersecurity certifications such as Security + and

Certified Ethical Hacking. Our adjunct faculty are current practitioners in cybersecurity, and they come with a great deal of relevant expertise to enrich their teaching and benefit our students.

Through the curriculum, professional organizations and engagement activities, graduates of the College of Southern Maryland's Cybersecurity AAS program will achieve the following educational objectives:

- a. Provide graduates with a common body of knowledge in cybersecurity.
- b. Provide graduates with the capability to develop the skills and knowledge required of cybersecurity practitioners in a variety of cybersecurity settings.
- c. Provide graduates the resources and skills allowing them to find employment or enter trainee programs in cybersecurity and related professions.

Through the curriculum, professional organizations and engagement activities, graduates of the College of Southern Maryland's Cybersecurity AAS program will achieve the following intended student learning outcomes:

Students will...

1. Analyze social, professional, security, and ethical issues related to computing.
2. Apply industry standard information security practices to solve a variety of business and technical problems.
3. Demonstrate understanding of key security domain concepts (policy development, physical security, computer application security, network defense, user support, and disaster and recovery planning).
4. Secure information as it exists in networks and computer systems by applying a layered security policy.
5. Explain as well as justify, in both oral and written form, security procedures and recommendations for a non-technical audience.

Our Academic Planning and Assessment's office's focus is the primary mission of the college: to provide quality opportunities for intellectual development that result in student learning. Our Student Learning Outcomes Assessment Plan (SLOAP) outlines the process of collecting information to determine whether CSM's academic offerings are having the appropriate educational impact on students. Student Learning Outcomes Assessment (SLOA) is defined as the systematic collection of information about academic offerings and analysis thereof, for the purpose of improving student learning.

Program Assessment at CSM is a cyclical process that includes:

1. Program Reviews conducted every five-six years, or more often as needed.
2. Academic certificate programs are included within the review of degree programs.
3. Program Monitoring conducted every other year (except in the year of a Program Review).
4. Program Assessments of Student Learning conducted on a cycle established by faculty.

In addition, CSM conducts course evaluations every semester or, more often when deemed necessary

Course list:

COM-1010 - Basic Principles of Speech Communication* (H) (3)

Prerequisite: ENG 0900 and RDG 0800

Students learn theories of listening, intrapersonal, interpersonal, intercultural, verbal, and nonverbal communication. Major units include informative and persuasive presentations and group discussion. College-level writing skills are recommended. This course satisfies the General Education Humanities requirement.

CSC-1110 - Program Design and Development* (3)

Prerequisite: MTH 0940 or MTH 0950 or higher

Students learn to solve business-oriented problems with emphasis on structured and object oriented programming techniques. Design tools are used to develop pseudo-code, flowcharting and 3D interactive environments. Students are introduced to several software packages that may be used to develop pseudo-code, flowcharts and interactive 3D environments. ITS-1110 is now CSC-1110.

ENG-1010 - Composition and Rhetoric* (3)

Prerequisite: ENG 0900; and RDG 0800; or placement

Students in this course complete their first semester college-level composition course. Students focus on planning, organizing, and developing a variety of argumentative compositions. Students practice the conventions of written Standard American English, gain information literacy skills, and learn research and documentation techniques including conducting online and print research and documenting sources. By the end of the semester, students demonstrate their ability to write a unified and coherent argument-based essay of about one thousand words that incorporates research and is nearly free of grammatical, mechanical, and structural errors. Students should refer to the schedule of classes for sections of this course taught in a computer lab. Students must pay an additional lab fee when taking this course in a computer-assisted classroom. Students may earn credit for this course through CLEP or Advanced Placement Examination. A minimum grade of "C" is required to pass the course. This course satisfies the General Education English Composition requirement.

ENG-2050 - Business and Technical Writing* (3)

Prerequisite: ENG 1010

Students develop writing skills through composing a variety of clear, effective memos, letters, and reports. Subject matter for the papers may come from the student's occupation or interests, whether scientific, technical, or non-technical. Students should refer to the schedule of classes for sections of this course which are taught in computer labs.

ITS-1050 - Computing Essentials* (3)

Students gain knowledge and practical experience with PC hardware and peripherals, mobile device hardware, networking and troubleshooting, hardware and network connectivity issues. Students also gain practical experience installing and configuring popular operating systems. Students will be introduced to topics in security, the fundamentals of cloud computing and operational procedures. Additionally, students will gain practice using Office productivity software tools such as Excel. This course helps students to prepare for the CompTIA A+ Certification.

ITS-1120 - Introduction to Database* (3)

Prerequisite: ITS 1050 or ITS 1020

Students learn how to use a relational Database Management Systems (DBMS). Topics include building, modifying, implementing, management and administration of a relational DBMS using Microsoft Access. Students will learn how to create tables, queries, forms, reports, and relationships according to project requirements. This course uses lecture and a hands-on format.

ITS-1960 - Introduction to Linux* (3)

Prerequisite: ITS 1020 or ITS 1050

Students learn the basic concepts of the Linux operating system as it relates to computer hardware, software, and operations, including command syntax, file management and maintenance, and troubleshooting of user problems. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business, Technology, and Public Service website.

ITS-2090 - Computer Security* (3)

Prerequisite: ITS 1050

ITS-2090 covers the fundamentals of operational security, network security, managing a public key infrastructure (PKI), authentication, access control, external attack, and cryptography. Students learn about the security procedures to protect data in computer environments, the different network attack scenarios, the many tools and procedures used by organizations to protect their resources, and the ethical issues raised by computer security in the business world. This course helps prepare students for the CompTIA Security+ exam. The vendor neutral CompTIA Security+ certification is the acceptable industry-level security certification. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business, Technology, and Public Service website.

ITS-2150 – Business Continuity & Disaster Recovery* (3)

Co-requisite: ITS 2545 and ENG 2050

Students will analyze and implement strategies to ensure business continuity in an information technology environment. This will involve the study of various risk management frameworks to support a robust and proactive approach to various types of threats. In addition, students will develop disaster recovery plans to support the entire business continuity and disaster recovery process. Specific technologies to support the process will also be examined.

ITS-2160 Cybersecurity Risk Management* (3) [NEW COURSE]

This course explores multidisciplinary and applied approaches to managing information security risk. Students examine technical, social, economic, legal, and political risks and implement strategies to remove not only these risks, but communication barriers between strategic, operational, and tactical level decision makers. This course also covers related government and industry regulations and standards, as well as effective practices frequently used to assess, analyze, and manage cybersecurity risks. Traditional cybersecurity risk management techniques are discussed alongside emerging strategies and topics such as the Internet of Things (IoT) and Cloud systems.

ITS-2190 - Microsoft Window Server Administration* (3)

Prerequisite: ITS 1050 or ITS 1020

This course teaches all skill sets related to the current Microsoft server including deployment, management, maintaining and monitoring of the server, and maintaining high availability of the servers in a network.

ITS-2400 – Introduction to Cloud Computing* (3)

Prerequisite: ITS 1050

This course is for students who seek a foundational understanding of cloud computing concepts, independent of specific technical roles. It provides an overview of cloud concepts, core services, security, architecture, pricing, and support. This course helps students to prepare for the AWS Certified Cloud Practitioner exam.

ITS-2500 - Ethical Hacking & Penetration Testing* (3)

Co-requisite: ITS 2190 and ITS 2536

Students learn how intruders, including hackers, attack systems and networks as well as best ethical practices for scanning, auditing, penetration testing, and securing assigned systems. In addition students will explore how intruders escalate privileges, strategies for preempting attacks as well as the legal and ethical nature of security countermeasures. For students who plan to use personal computers, this course may have specific computing requirements. Please refer to the Quick Link for Computing Requirements on the Business, Technology, and Public Service website.

ITS-2511 - Networking I* (3)

Prerequisite: ITS 1050

Students learn networking fundamentals and network terminology in this first of a three-course series. Topics covered include open system interconnection (OSI) models, Ethernet technologies, network media, basics of TCP/IP, and IP addressing. Training is provided in the use of networking software and tools that are required to troubleshoot networking problems.

ITS-2516 –Networking II* (3)

Prerequisite: ITS 2511

Students learn router and routing basics in this second of a three-course series. This course provides students with an understanding of wireless, security, TCP/IP, basic router configuration, installation of routing protocols, network troubleshooting skills, and configuration of networking software and tools that are required to troubleshoot networking problems.

ITS-2527 – Enterprise Networking* (3) [NEW COURSE]

Prerequisite: ITS 2516

Students learn advanced security concepts, virtualization, and network automation in this third of a three-course series. Topics covered commonly used networking automation tools. Training is provided in the use of networking software and tools that are required to troubleshoot network problems.

ITS-2536 - Network & Infrastructure Defense* (3)

Prerequisite: ITS 1960 , ITS 2090 and ITS 2511

In this course, student learn how to manage and apply technologies to protect networks. An understanding of security technologies including firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), virus protection, TCP packet sniffing and analysis, VPNs (virtual private networks), and disaster recovery will be addressed.

ITS-2545 - Information Systems Security* (3)

Prerequisite: ITS 2090, RDG 0800 and ENG 0900

Students learn the management principles of information security. The course will cover many aspects of security including hardware, software, communication, and physical security. Security policy, legal and ethical issues will also be covered. The relationship between course topics and CISSP domains are also highlighted.

ITS-2555 - Digital Forensics I* (3)

Prerequisite: ITS 2090 , RDG 0800 and ENG 0900

Co-requisite: ITS 1960

Students will navigate through each phase of the digital forensics analysis methodology using a practical and hands-on approach. Various open source and commercial digital forensic software packages will be used in conjunction with hardware based tools to support the process. Topics such as anti-forensics measures will be examined to demonstrate the impact they can have on an investigation. Students will also explore the various laws and regulations that guide the digital forensics process during both criminal and civil litigation. In addition, students will learn how to prepare policy documentation to build and maintain a successful digital forensics laboratory.

ITS-2560 - Digital Forensics II* (3)

Prerequisite: ITS 2555 or ITS 2550

Students will build upon digital forensics concepts and skills from ITS 2555 Digital Forensics I. Digital forensics specific hardware and software will be used to acquire and analyze images from common hardware and mobile based device types. Network forensics concepts will also be explored along with an introduction to malware analysis.

MTH-1010 - Quantitative Literacy and Reasoning* (3) or higher

Prerequisite: MTH 0940

This course develops student skills in interpreting, understanding and using quantitative information. It teaches algebraic reasoning and modeling skills through a quantitative literacy lens and emphasizes critical thinking and statistical reasoning. It also develops skills in reading and writing quantitative information. This course is not designed for students who need College Algebra or higher or are pursuing a degree that requires higher level mathematics. This course satisfies the General Education Mathematics requirement.

PHL-1150 - Cyber Ethics* (3)

Prerequisite: RDG 0800

Students consider the safe and ethical use of computer technology including the Internet. They study the role of technology in today's society, cyber protection issues and the moral challenges we face in using technology including cyber space. Topics to be included are privacy, intellectual property, cyber abuse/crime, codes of conduct, policy development as well as the digital divide. In addition, students consider how the global and anonymous nature of the Internet makes it difficult to transfer standard rules of conduct to this virtual environment. This course satisfies the General Education Humanities requirement.

Recommended Course Sequence:

First Semester

ENG-1010 - Composition and Rhetoric* (3)

PHL-1150 - Cyber Ethics* (3)

ITS-1050 - Computing Essentials* (3)

MTH-1010 - Quantitative Literacy and Reasoning* (3) or higher

Biological/physical sciences (3) See Gen Ed Listing

Second Semester

COM-1010 - Basic Principles of Speech Communication* (H) (3)

ITS-1960 - Introduction to Linux* (3)

ITS-2090 - Computer Security* (3)

ITS-2190 - Microsoft Window Server Administration* (3)
ITS-2511 - Networking I* (3)

Third Semester

CSC-1110 - Program Design and Development* (3)
ITS-2536 - Network & Infrastructure Defense* (3)
ITS-2516 – Networking II* (3)
ITS-2555 - Digital Forensics I* (3)
ITS-2545 - Information Systems Security* (3)

Fourth Semester

ITS-2500 - Ethical Hacking & Penetration Testing* (3)
ENG-2050 - Business and Technical Writing* (3)

Social/behavioral sciences (3 credits)

- Select from Gen Ed Listing and select any Social Behavioral Science course from within the Cultural and Global Awareness course list.

Cybersecurity Electives (6 credits)

Digital Forensics

ITS-1120 - Introduction to Database* (3)

ITS-2560 - Digital Forensics II* (3)

Network Security

ITS-2527 – Enterprise Networking* (3) [NEW COURSE]

ITS-2400 – Introduction to Cloud Computing* (3)

Information Assurance

ITS-2150 – Business Continuity & Disaster Recovery* (3)

ITS 2160 – Cybersecurity Risk Management* (3) [NEW COURSE]

Program Description for the Catalog:

The field of cybersecurity focuses on the protection of computers, networks, software, and data from unauthorized access, modification, and destruction. Continued adoption of new technologies, Software as a Service (SaaS), and migration to cloud environments in the face of evolving threats are accelerating demand for practitioners in this already growing field.

This degree program prepares students who are currently employed in the cybersecurity field as well as those without prior work experience to develop the skills and knowledge required of practitioners within a variety of cybersecurity related settings.

The first semester is the same for all students in this program; it is designed to provide all students with a foundation in information technology hardware and software fundamentals. During the second semester, students begin to explore cybersecurity concepts. At the conclusion of the second semester, the student will select elective offerings in areas of special interest in Digital Forensics, Network Security, or Information Assurance.

Cybersecurity students will take classes that will help to prepare for the following in-demand entry level cybersecurity industry certifications: CompTIA A+, CompTIA Security+, CompTIA Linux+, and EC Council Certified Ethical Hacker (CEH). Depending on elective selections, students may take courses to prepare for these additional certifications: EC Council CHFI, AWS Certified Cloud Practitioner, and CISCO CCNA.

Students opting to take more Digital Forensics electives will take classes that will help to prepare them for the Computer Hacking Forensic Investigator (CHFI) industry certification. These elective courses will place special emphasis on the knowledge and skills to conduct digital forensics investigations and to develop and administer policy in support of digital forensic programs.

Students selecting the Network Security electives will take classes that will help to prepare them for the Cisco Certified Network Associate (CCNA) industry certification. These elective courses will place special emphasis on the knowledge and skills to implement, administer, and secure networks of various sizes.

Students selecting electives in Information Assurance will take classes that will help to prepare them with the technical knowledge, as well as the foundational leadership and management capabilities to further skills related to policy development, compliance, standards, and risk management.

Students will be taking courses in this program through several course delivery formats. Since it is imperative that students obtain hands-on experience with the various tools, technologies and techniques employed in the cybersecurity field, some courses may only be offered in a face-to-face lab environment. However, most courses in the program are available online as well as in 7-week mini-semester, and summer terms.

This program has been designated as a CAE-CDE 2Y - National Centers of Academic Excellence in Cyber Defense 2-Year Education by the National Security Agency (NSA) and Department of Homeland Security (DHS).

Professionals with a strong IT background may contact the program coordinator or chair about obtaining prerequisite waivers to take certain classes in this program.

Students may be eligible to receive Credit for Prior Learning through Certification Evaluation for up to 15 credits with any of the following current certifications: CompTIA A+, CompTIA Security+, CompTIA Linux+, CISCO CCNA, EC Council CEH, EC Council CHFI, AWS Certified Cloud Practitioner, and ISC² CISSP.

Students should meet with an advisor to discuss Certification Evaluation, transfer evaluation, or options for transfer to 4-year colleges with this program.

The maximum number of credits accepted in transfer from other institutions to this program is 45.

Career Opportunities:

information systems security technician, cybersecurity analyst, security associate, security administrator, security specialist, digital forensics investigator, security consultant, information assurance technicians, network security administrator, and security engineer

Transfer Options:

A complete list of all transfer opportunities can be found on the Transfer Services page

Student Learning Outcomes:

Students will...

1. Analyze social, professional, security, and ethical issues related to computing.
2. Apply industry standard information security practices to solve a variety of business and technical problems.

3. Demonstrate understanding of key security domain concepts (policy development, physical security, computer application security, network defense, user support, and disaster and recovery planning).
4. Secure information as it exists in networks and computer systems by applying a layered security policy.
5. Explain as well as justify, in both oral and written form, security procedures and recommendations for a non-technical audience.

Cybersecurity, AAS	
New 2020 Catalog	
General Education	
3 credits English Composition	ENG-1010 English Composition* (3)
3 credits Arts/Humanities	COM 1010 Basic Principles of Speech Communication* (3)
3-4 credits Biological/Physical Sciences	Select from Gen. Ed. Listing (3)
3 credits Social/Behavioral Sciences	Select from Gen. Ed. Listing of Courses Within Cultural & Global Awareness Course List (3)
3 credits Mathematics	MTH 1010 Quantitative Literacy and Reasoning* (3)
Other General Education (from above categories) (3 credits)	PHL-1150 – Cyber Ethics* (3)
MHEC requires a minimum of 18 credits	General Education=18
Major requirements	ITS 1050 Computing Essentials* (3) ITS 1960 Introduction to Linux* (3) ITS 2090 Computer Security * (3) ITS 2190 Microsoft Window Server Administration* (3) ITS 2511 Networking I* (3) CSC 1110 Program Design and Development* (3) ENG 2050 Business and Technical Writing* (3) ITS 2536 Network & Infrastructure Defense* (3) ITS 2516 Networking II* (3) ITS 2555 Digital Forensics I* (3) ITS 2500 Ethical Hacking* (3) ITS 2545 Information Systems Security* (3)
	Major Requirements=36
Electives	ITS 1120 Introduction to Database* (3) ITS 2560 Digital Forensics II* (3) Or ITS 2527 Enterprise Networking* (3) NEW COURSE ITS 2400 Introduction to Cloud Computing* (3) Or ITS 2160 Cybersecurity Risk Management* (3) ITS 2150 Business Continuity and Disaster Recovery* (3)
	Electives=6
	Credit total=60
*courses requiring a prerequisite	

Cybersecurity, AAS	
2019 Catalog	
General Education	
3 credits English Composition	ENG-1010 English Composition* (3)
3 credits Arts/Humanities	COM-1010 Basic Principles of Speech* (3)
3-4 credits Biological/Physical Sciences	Biological/physical sciences (3 credits) Select 3 credits from the General Education Course List
3 credits Social/Behavioral Sciences	Social/behavioral sciences (3 credits) Acceptable: Select 3 any General Education Social Behavioral Science course within the Cultural and Global Awareness course list
3 credits Mathematics	MTH-1010 Quantitative Reasoning* (3)
	Core General Education=15
Other General Education (from above categories) (3 credits)	PHL-1150 - Cyber Ethics* (3)
MHEC requires a minimum of 18 credits	General Education= 18
Major requirements	<p>ENG-2050 - Business and Technical Writing* (3)</p> <p>ITS-1050 - Computing Essentials* (3)</p> <p>ITS-1960 - Introduction to Linux* (3)</p> <p>ITS-2090 - Computer Security* (3)</p> <p>ITS-2190 – Microsoft Windows Server Administration* (3)</p> <p>ITS-2511 - Networking I* (3)</p> <p>ITS-2516 - Networking II* (3)</p> <p>ITS-2500 - Ethical Hacking & Penetration Testing* (3)</p> <p>ITS-2536 - Network & Infrastructure Defense* (3)</p> <p>ITS-2555 - Digital Forensics I* (3)</p> <p>Digital Forensics:</p> <p>CSC-1110 - Program Design and Development* (3)</p> <p>ITS-1120 – Introduction to Database* (3)</p> <p>ITS-2545 - Information Systems Security* (3)</p> <p>ITS-2560 - Digital Forensics II* (3)</p> <p>Network Security:</p> <p>CSC-1110 - Program Design and Development* (3)</p> <p>ITS-2521 - Networking III* (3)</p> <p>ITS-2526 - Networking IV* (3)</p> <p>ITS-2545 - Information Systems Security* (3)</p>
	Major Requirements=42
Electives	
	Electives= 0
	Credit total= 60
*courses requiring a prerequisite	

Our Cybersecurity AAS program has been designated as a CAE-CDE 2Y - National Centers of Academic Excellence in Cyber Defense 2-Year Education by the National Security Agency (NSA) and Department of Homeland Security (DHS). CSM's designation is valid through 2021.

Note: CSM was up for re-designation this year; however, all 2-year schools were notified in October 2019 that CAE designations will be valid one more year (through 2021) while the NSA retools their application process.

There are no specialized graduate certification requirements for this program and its students.

CSM provides information to students about our program offerings in numerous ways, including Campus Open Houses and Tours, Presentations at local high schools, Orientation and Registration sessions, and New Student Welcome events. They are provided with information about applying to CSM, college readiness, financial aid, payment policies, technical requirements, including our LMS, and the many academic support services.

Advisors are available in-person and through videoconferencing sessions. We also have a faculty advising training program to equip faculty to advise students after they have completed 30 credits towards their degree.

Other student services include learning support services such as tutoring, workshops, and learning labs, library services, counseling services, testing services on all campuses, and disability, and Veteran & Military support services.

Students are provided with a CSM email account and access to Microsoft Office software with information about our technology services support and help desk.

Our students are notified in writing of changes that may impact their program planning. Because the new elective offerings are courses that are already being offered, we do not anticipate any major challenges in implementing the proposed changes.

Our Admissions Department works closely with the Marketing Department and the Division of Academic Affairs to ensure that the recruitment and admissions materials will clearly and accurately represent our programs and services available. The Admissions Department identifies prospective students; recruits and admits new students; and provides information regarding the college to all prospective and current students and the community. The department works collaboratively with the Enrollment Management Team to support the college's efforts to attract students and assist them in defining and achieving their goals and in providing the highest quality customer service.

The goal of the Recruitment Team is to attract traditional and returning adults to the college through several avenues that include presentations to middle and high schools, civic organizations, businesses, alternative schools, college fairs and information sessions. In addition, the team is responsible for post test advising for new students in order to ensure a smooth transition into the college community. Team members are available to meet with anyone interested in learning more about the college and how it can help them realize their potential.

As the focal point of college information, the Call Center staff responds to questions on how to start the college application process, provides assistance with log-in and account restrictions, and answers many general questions about the college.

As a team, our Marketing Department completes more than 500 projects each year to support and promote the many programs and initiatives at CSM. The team provides website support and is responsible for accurately representing all of our programs and services available at CSM.

H. Adequacy of Articulation

CSM has transfer agreement with this program with these institutions:

- Capitol Technology University
- Goucher College
- Stevenson University

Copies of the articulation agreements are included with this proposal.

I. Adequacy of Faculty Resources (as outlined in COMAR 13B.02.03.11).

As described in Section G, our program faculty is comprised of both full-time and part-time faculty and come from diverse professional and academic backgrounds. Our full-time faculty include both new instructors as well as long-time tenured faculty with both academic credentials and industry certifications in the field of cybersecurity, information science, computer science, and related fields. Some of our full-time faculty have current industry experience in the cybersecurity field as well. We have full-time faculty members who are Cisco Certified Academy Instructors and others with various cybersecurity certifications such as Security + and Certified Ethical Hacking. Our adjunct faculty are current practitioners in cybersecurity, and they come with a great deal of relevant expertise to enrich their teaching and benefit our students.

Our Distance Learning and Faculty Development (DLF) division provides support to faculty in training and administration of our learning management system (LMS). All new faculty are required to complete LMS training. Other training courses are also available to all faculty, including training on teaching web-hybrid classes and refresher training.

The DLF division also provides support for faculty conference attendance and additionally hosts an annual professional development 2-day conference for both full-time and adjunct faculty. Additionally, the DLF team coordinates pre-semester professional development activities for all faculty.

Faculty Member Name	Terminal Degree	Full-time or Part-time	Courses Taught
Christopher Estes	MBA (and CISSP)	Full-time	CSC-1110, ITS-1050, ITS-1960, ITS-2090, ITS-2536, ITS-2545
Lakisha Ferebee	B.A. - Interdisciplinary Studies	Full-time	ITS-2511, ITS-2516, ITS-1050, ITS-2555, ITS-1960
Lawrence Gross	M.S. - Technology Management	Part-time	ITS-2090, ITS-2545

Ronda Jacobs	M.A. – Adult Education & Distance Learning	Full-time	ITS-1050
Eugen Leontie	Ph.D. - Computer Science	Full-time	CSC-1110, ITS-2555
Pamela Mitchell	B.S. - Data Management	Full-time	ITS-2511, ITS-2516, ITS-2521, ITS-2526, ITS-1120
Gale Pomper	D.Sc. - Information Assurance	Part-time	ITS-1960
Michael Shellem	M.S. - Computer & Software Engineering	Part-time	ITS-1960
Terrell Smith	M.S. - Information Technology: Information Assurance	Part-time	ITS-1960, ITS-1050, ITS-2090, ITS-2536
Kathleen Wallace	B.S. - Information Technology	Part-time	ITS-2555, ITS-2560, ITS-2500
Richard White	M.S. – Information Technology, Database Adm.	Full-time	CSC-1110
John Wilson	M.A. – National Security Affairs	Full-time	PHL-1150, ITS-1050, ITS-1120, ITS-2190

J. Adequacy of Library Resources (as outlined in COMAR 13B.02.03.12).

Students may borrow circulating materials from any of the three CSM library branches. Through the interlibrary loan program (ILL), students can order almost any book, periodical article, or ERIC document needed, generally available within one week of the request. Library resources also include audiovisual collections use in the library and classrooms only. Additionally, substantial material is available through online databases, including ProQuest and EBSCO.

The President assures that appropriate library resources are available to support the needs of this program.

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment (as outlined in COMAR 13B.02.03.13)

CSM is a leader among Maryland community colleges in offering courses which meet the busy schedules of our students, traditional weekday face to face courses, weekend and evening classes, Web-hybrid courses which offer a mix of online and traditional classroom face-to-face instruction and a popular online learning community. The college makes available state of the art facilities on three campuses to accomplish its mission in support of our community's academic, professional, and self-enrichment pursuits.

The Cybersecurity AAS degree program will be conducted primarily on the La Plata campus, in the ST building, home to the Business and Technology Division. Many classes will also be offered at the Leonardtown and Prince Frederick campuses. Many business classes are offered in the BU building. The ST and BU buildings house state of the art classrooms, conference rooms, faculty and administrative offices, computer labs, Student Computer Support department (help desk) and science laboratories. Additionally, we have dedicated labs at the La Plata and

Leonardtown campuses that are equipped with software and equipment to offer specialized Cybersecurity courses in digital forensics, ethical hacking, and networking courses.

The President assures that appropriate physical facilities, infrastructure, and instructional equipment are available to support the needs of this program.

L. Adequacy of Financial Resources with Documentation (as outlined in COMAR 13B.02.03.14)

TABLE 1: RESOURCES					
Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue	\$271,800	\$292,185	\$314,835	\$342,015	\$371,460
(c + g below)					
a. Number of F/T Students**	30	30	30	30	30
b. Annual Tuition/Fee Rate (\$151 x 21 credits)*	\$3,171	\$3,171	\$3,171	\$3,171	\$3,171
c. Total F/T Revenue (a x b)	\$95,130	\$95,130	\$95,130	\$95,130	\$95,130
d. Number of P/T Students***	78	87	97	109	122
e. Credit Hour Rate	\$151	\$151	\$151	\$151	\$151
f. Annual Credit Hours Rate	15	15	15	15	15
g. Total P/T Revenue	\$176,670	\$197,055	\$219,705	\$246,885	\$276,330
(d x e x f)					
3. Grants, Contracts & Other	0	0	0	0	0
External Sources					
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	\$271,800	\$292,185	\$314,835	\$342,015	\$371,460
* The credit hour rate (\$151) is based upon CSM's current tuition rate of \$123 plus 23% combined fee.					

** Full Time enrollment has been flat.

*** Part Time enrollment has been increasing at approximately 12% yearly.

TABLE 2: EXPENDITURES:					
Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000
a. # FTE	1 FT x 5 courses & 2 Existing Courses	2 FT x 5 courses & 2 Existing Courses	3 FT x 5 courses & 2 Existing Courses	4 FT x 5 courses & 2 Existing Courses	5 FT x 5 courses & 2 Existing Courses

b. Total Salary	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000
c. Total Benefits	0	0	0	0	0
2. Admin. Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	0	0	0	0	0
TOTAL (Add 1 – 7)	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000	\$ 210,000

M. Adequacy of Provisions for Evaluation of Program (as outlined in COMAR 13B.02.03.15).

CSM conducts course evaluations every semester or, more often when deemed necessary.

To address online academic rigor and faculty presence, in coordination with our Distance Learning and Faculty Development (DLF) division, our online courses undergo additional review through our internal Online Academic Rigor and Presence (OARP) process. Our OARP process is comprised of a self-review followed by peer review and remediation.

Faculty are evaluated annually according to the process outlined in CSM's "Faculty Handbook".

As described in Section G, our Academic Planning and Assessment's office's focus is the primary mission of the college: to provide quality opportunities for intellectual development that result in student learning. Our Student Learning Outcomes Assessment Plan (SLOAP) outlines the process of collecting information to determine whether CSM's academic offerings are having the appropriate educational impact on students. Student Learning Outcomes Assessment (SLOA) is defined as the systematic collection of information about academic offerings and analysis thereof, for the purpose of improving student learning.

Program Assessment at CSM is a cyclical process that includes:

1. Program Reviews conducted every five-six years, or more often as needed.
2. Academic certificate programs are included within the review of degree programs.
3. Program Monitoring conducted every other year (except in the year of a Program Review).
4. Program Assessments of Student Learning conducted on a cycle established by faculty.

N. Consistency with the State's Minority Student Achievement Goals (as outlined in COMAR 13B.02.03.05).
--

One of CSM's Values/Guiding Principles is Diversity. The Institutional Equity and Diversity Office works to "create an environment that instills an appreciation and understanding of the diverse qualities each of us brings to this campus; where our students, staff, and faculty mirror the community we serve and are free from discrimination and harassment."

Additionally, CSM defines civility as "the demonstration of respect for others through basic courtesy and the practice of behaviors that contribute toward a positive environment for learning and working."

As is true of CSM, the Cybersecurity AAS Program is open to all students with no restrictions reference to age, gender, or ethnic background. As such, any student meeting the eligibility requirements of the college admissions process is entitled to enroll in this discipline of study. Furthermore, CSM, the Business, Technology, and Public Services Division, and representatives of the Cybersecurity AAS Program all participate in events, programs, orientations, and information sessions sponsored internally or by external advocates in order to reach all students seeking information on the college's programs and the professional opportunities that result from that education and training.

CSM's marketing department is developing a comprehensive marketing plan for this new program. These resources include the designing and printing of brochures, assistance with marketing campaigns (web and traditional news media), and development of other recruitment materials. CSM is committed to ensuring new programs are marketed to diverse populations, as demonstrated by the organizational values, which include valuing diversity. Marketing plans will include activities specifically designed to market the program to the diverse population of the tri-county region.

Diversity and multiculturalism are vitally important issues for future leaders. As such, the representatives of this new program at CSM intend to contact multiple professional associations, national, regional and local employers, secondary and postsecondary institutions to create partnerships that will lead to the diversity of our student population and graduates of our programs.

O. Relationship to Low Productivity Programs Identified by the Commission:

The proposed degree is not directly related to an identified low productivity program identified by the Commission.

P. Adequacy of Distance Education Programs (as outlined in COMAR 13B.02.03.22)

This program will not be offered as a distance education program.



**Agreement Between College of Southern Maryland (CSM) and
Capitol Technology University (Capitol) for the Articulation of the A. A. S. in
Cybersecurity to Capitol Technology University B. S. in Cyber and Information Security**

PURPOSE

This agreement facilitates the transfer of College of Southern Maryland (CSM) students who graduate with an A. A. S. in Information Systems Security to the B. S. in Cyber and Information Security (BSCIS) as well as to the M.S. in Cyber and Information Security (MSCIS) at Capitol Technology University (Capitol). This agreement defines the terms of the transfer agreement. The goals inherent in the agreement are to:

1. Facilitate students' transfer from the A. A. S. in Information Systems Security at CSM to the B. S. Cyber and Information Security program at Capitol as efficiently as possible.
2. Facilitate students' admission into Capitol's MSCIS program after completing the A. A. S. in Information Systems Security at CSM and possessing Bachelor's degree from an accredited institution.
3. Establish a clear set of understandings and expectations for institutions, students, and their respective degrees.
4. Establish a pathway for CSM A. A. S. in Information Systems Security graduates to earn a B. S. in Cyber and Information Security at Capitol as a means to advance their careers in the associated field.

ARTICULATION AGREEMENT

CSM and Capitol agree to offer articulated programs leading to the award of an A. A. S. in Information Systems Security and a B. S. in Cyber and Information Security. The two institutions further agree that students from CSM, under the articulation agreement, may transfer credits earned for the A. A. S. in Information Systems Security toward the B. S. in Cyber and Information Security at Capitol. The following general principles guide the implementation of this agreement:

1. The program is designed for graduates of the A. A. S. degree in Information Systems Security at CSM to transfer specific courses in which they have earned the grade of C or higher. The number of courses transferred may not exceed 69 credit hours (half the degree per Maryland law). However, students with transfer credits from 4-year institutions may request evaluation of those credits for additional transfer. The credit hours transferred from CSM contribute to the fulfillment of the 129/131 credit hours required for baccalaureate completion (BSCIS) at Capitol.
2. The course transfer table included with this document specifies courses that will transfer from CSM to Capitol.
3. Capitol 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).

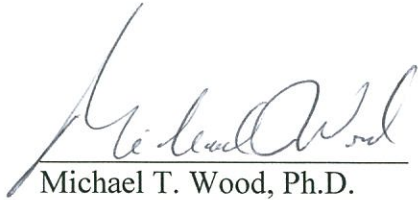
4. For a smooth transition, students at CSM may start taking courses in the Cyber and Information Security program at Capitol while they are completing the A. A. S. degree at CSM. However; students are advised to complete the A. A. S. degree prior to officially transferring to Capitol.
5. If CSM and Capitol 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. CSM students who complete the A. A. S. in Information Systems Security with a 2.5 grade point average will be automatically accepted into the bachelor's degree program at Capitol and will be given consideration for financial assistance and will be eligible to compete for academic scholarships at Capitol. Students who finish the A. A. S. degree with a GPA of 3.0 or higher and subsequently attend Capitol full-time will be considered for larger scholarship under a special program.
7. At the request of the CSM Vice President for Academic Affairs, the Capitol Academic Dean will provide general information on the academic progress of CSM students enrolled in the Capitol BSCIS program. Any feedback must adhere to FERPA.
8. CSM and Capitol agree to monitor the performance of this agreement and to revise as necessary.
9. CSM and Capitol agree to publicize this agreement.
10. The course transfer table is subject to a five-year review for updating and revising as necessary by the appropriate CSM and Capitol 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. A. S. in Information Systems Security program who are taking courses at Capitol or who have been accepted into the BSCIS at Capitol.
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.

MASTER DEGREE TRANSFER: M.S. (2+2+1):

Students who complete the A. A. S. degree in Information Systems Security at CSM, the B. S in Cyber and Information Security at Capitol and who have a GPA of 3.0 or greater will be accepted into the M.S. in Cyber and Information Security. The program can be completed in one year with student attendance on a full-time basis. Students may contact an advisor regarding eligibility for other master degrees under this program.

Authorizing Signatures

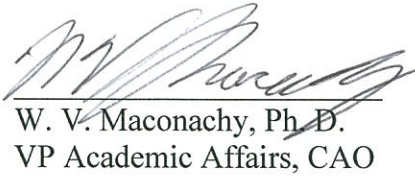
This agreement is authorized for implementation on the 24th day of November, 2015



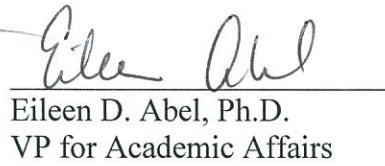
Michael T. Wood, Ph.D.
President
Capitol Technology University



Bradley M. Gottfield, Ph.D.
President
College of Southern Maryland



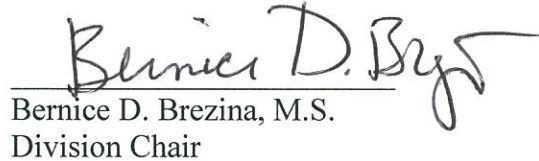
W. V. Maconachy, Ph.D.
VP Academic Affairs, CAO



Eileen D. Abel, Ph.D.
VP for Academic Affairs



Helen G. Barker, D.M.
Dean Business and Info. Sciences



Bernice D. Brezina, M.S.
Division Chair

Course Transfer Table
College of Southern Maryland A.A.S. in Information Systems Security to
Capitol Technology University B.S. in Cyber and Information Security
(129/131 Credits)

COURSE NUMBER, TITLE and NUMBER of CREDITS			COURSE NUMBER, TITLE and NUMBER of CREDITS		
Programming and Computer Courses		32 Credits	English/Humanities/Social Sciences		27/28 Credits
		Transferred Course			Transferred Course
	CS-130 Computer Science Fundamentals I (4)			FS-100 Freshman Seminar (1)	WAIVE
	CS-220 Database Management (3)			EN-101 English Communications I (3)	ENG 1010
	CS-230 Computer Science Fundamentals II (3)			EN-102 English Communications II (3)	
	CS-320 Database Administration (3)			EN-408 Writing Semi in Tech Research (3)	
	CS-418 Operating Systems (3)	ITS 1020		HU-331 or HU-332 Arts and Ideas (3)	
	CS-150 Intro to Programming using C (4)			SS-351 Ethics (3)	ITS 2940
	CT-152 Introduction to Unix (3)	ITS 1960		Arts & Humanities Elective (3)	ENG-2050
	CT-206 Scripting Languages (3)			Arts & Humanities Elective (3)	COM 1010
	CT-240 Internetworking w/Rters/Switches (3)	ITS 2516		Social Science Elective (3)	Elective
	SE-458 Senior Project (3)			Social Science Elective (3)	ITS 1015
Information Assurance Courses		27 Credits	General Electives		19-21 Credits
	IAE-201 Introduction to IA Concepts (3)	ITS 2090		ITS 2190	3
	IAE-301 Comp Cmptr/Ntwk Security (3)	ITS 2536		ITS 2526	3
	IAE-315 Secure Sys Admin & Operation (3)			ITS 2511	3
	IAE-321 Applied Wireless Ntwk Security (3)			ITS 2521	3
	IAE-325 Secure Data Commun and Crypt (3)			ITS 2545	3
	IAE-402 Intro to Inc Handling/Mal Code (3)				
	IAE-405 Malware Analysis/Reverse Engrg (3)				
	IAE-406 Forensic Investigative Processes (3)	ITS 2550			
	IAE-410 Design and Testing (3)	ITS 2500			
Mathematics and Science Courses		17 Credits			
	MA-114 Algebra and Trigonometry (4)	See NOTE 1: Mathematics			
	MA-124 Discrete Math (3)				
	MA-128 Introduction to Statistics (3)				
	MA-261 Calculus I (4)				
	Science Elective (3)	Science Elective		TOTAL CREDITS	61
Management Courses		6 Credits			
	BUS-174 Intro/Business and Management (3)				
	BUS-301 Project Management (3)				

NOTE 1: Mathematics recommendation:

MTH 1150 transfers as MA 114

MTH 1200 transfers as MA 261

MTH 2300 transfers as MA 128

NOTE 2: Recommendations for additional courses up to a total of 69 credits:

ENG 1020 transfers as EN 102

BAD 1210 transfers as BUS 174

BAD 1780 transfers as BUS 174

ECN 1015 transfers as BUS 174

ITS 2591 or ITS 2592 transfer as CS 130. If both are taken one could transfer as a CTU

General Elective.

There is an opportunity for one 100-200 level course that transfers as a CTU General Elective.

TS 2300 transfers as BUS 301

ITS 1390 transfers as CS 230

**ACADEMIC PROGRAM ARTICULATION 2+2 AGREEMENT BETWEEN
COLLEGE OF SOUTHERN MARYLAND
AND
GOUCHER COLLEGE REGARDING TRANSFER FROM THE ASSOCIATE OF
APPLIED SCIENCE AT COLLEGE OF SOUTHERN MARYLAND TO THE
BACHELOR OF PROFESSIONAL STUDIES AT GOUCHER COLLEGE**

This Academic Program Articulation Agreement (“Agreement”) is entered into by and between COLLEGE OF SOUTHERN MARYLAND (the “Sending Institution”) and GOUCHER COLLEGE (the “Receiving Institution”) (collectively, the “Institutions”) to facilitate the transfer of academic credits from the following programs at College of Southern for completion of the Bachelor of Professional Studies degree at Goucher College:

AAS PROGRAM	HEGIS	CIP	BPS TRANSFER	HEGIS	CIP
Criminal Justice	550501	430107	Criminal Justice	550505	430103
Cybersecurity	550501	430107	Criminal Justice	550505	430103
Human Services	521601	511502	Human Services	521601	511502
Massage Therapy	559920	513501	Human Services	521601	511502

A. Qualifying Students

This Agreement pertains to the transfer of “Qualifying Students”, *i.e.*, those students who:

1. Have successfully completed the AAS program at the College of Southern Maryland;
2. Are enrolled in College of Southern Maryland in good standing; and
3. Are accepted for admission at Goucher College.

B. Responsibilities of the Institutions

The Institutions agree to implement the transfer of Qualifying Students in accordance with applicable law and the following requirements and protocols:

1. A Qualifying Student may transfer from College of Southern Maryland into Goucher College for the completion of the Bachelor of Professional Studies degree.
2. Goucher College will accept the full AAS degree awarded at College of Southern Maryland in one of the ten (10) AAS programs listed above (60 credits total) as completion of the first two years of the Bachelor of Professional Studies program at Goucher.
3. The transferring student will complete an additional 60 credits at Goucher College online with no residency requirement to fulfill the third and fourth year of the BPS program. These additional courses shall consist of the following:

BPS Core Courses (30 cr)

BPS 300	Introduction to Professional Studies
BPS 330	Digital and Professional Communication
BPS 350	<i>Critical Thinking, Research & Presentation (3)</i>
BPS 370	Technology for Information-Based Orgs.
BPS 390	Ethics in Professional Life (3)
BPS 440	<i>The Legal Environment (3)</i>
BPS 450	Leadership in the Workplace (3)

BPS 460	Human Diversity in Social Contexts (3)
BPS 480	Public Advocacy and Negotiation (3)
BPS 490	Professional Internship (3)

BPS Major Courses (30 cr)

Students select one of the following three major areas:

Criminal Justice

CRJ XXX	Introduction to the Criminal Justice
CRJ XXX	Theories of Crime and Justice
CRJ XXX	Criminal Law and Criminal Procedure
CRJ XXX	Police and Society
CRJ XXX	Corrections
CRJ XXX	Research Methods in Criminal Justice
CRJ XXX	Crime Analysis and Report Writing
CRJ XXX	Ethics in Criminal Justice
CRJ XXX	Seminar: Contemporary Issues in Criminal Justice
CRJ XXX	Criminal Justice Assessment

Human Services (30 cr.)

HUS XXX	Human Services Delivery Systems (3)
HUS XXX	Chemical Dependency and Treatment Approaches (3)
HUS XXX	Mental Health and Counseling (3)
HUS XXX	Children, Family, and Community-based Services in Human Services (3)
HUS XXX	Gerontology in Human Services (3)
HUS XXX	Case Management Practice and Principles (3)
HUS XXX	Crisis Intervention and Ethics in Human Services (3)
HUS XXX	Social Policies and Advocacy in Human Services (3)
HUS XXX	Evaluation and Program Planning in Human Services (3)
HUS XXX	Field Experience and Seminar in Human Services (3)

Sports Communication Courses (30 cr.)

SPC XXX	Communication, Sport, and Society
SPC XXX	Introduction to Sports Media
SPC XXX	Sports Publications
SPC XXX	Sports Media Relations
SPC XXX	Social Media and Sports Communication
SPC XXX	Communication in Sports Organizations
SPC XXX	Sports Media Criticism
SPC XXX	The Business of Sports Promotion
SPC XXX	Advanced Sports Communication
SPC XXX	Current Topics in Sport Communication

Goucher College shall designate, and shall provide to College of Southern Maryland, the contact information for a staff person at Goucher College who is responsible for the oversight of the transfer of Qualifying Students. College of Southern Maryland shall designate, and shall provide to the Receiving Institution, the contact information for a staff person at the College of Southern Maryland who is responsible for the oversight of the transfer of Qualifying Students.

	College of Southern Maryland	Goucher College
Name of staff person responsible for oversight	Ms. Jacqui Rogers	Ms. Alexis Rudolph
Title of staff person	Coordinator of Transfer and Articulation	Assistant Director of Recruitment
Email address	jgrogers@csmd.edu	Lexi.rudolph@goucher.edu
Telephone Number	301-934-7571	410-337-6110

Should the staff person or position change, the institution will promptly provide new contact information to the partner institution and inform the Maryland Higher Education Commission of the change.

Additional contact information:

Dean or Program Director(s)	College of Southern Maryland	Goucher College
Name of person	Dr. Eileen Abel	Dr. Kathryn Doherty
Title of person	VPAA	Associate Provost
Email address	eabel@csmd.edu	kathryn.doherty@goucher.edu
Telephone Number	301-934-7846	410-337-6208

- If the Qualifying Student is using federal Title 38 VA Education Benefits (GI Bill® Education Benefits), the Institutions shall adhere to all applicable U.S. Department of Veterans Affairs' regulations, including the regulations governing the awarding of prior credit, as regulated under Title 38, Code of Federal Regulations, Sections 21.4253(d)(3) and 21.4254(c)(4).

Tuition Information:

Total Credits	60
Cost Per Credit	\$300
Technology Fee (only assessed in the fall and spring semesters)	\$275

- Each Institution shall adhere to all applicable transfer requirements set forth in the Annotated Code of Maryland and the Code of Maryland Regulations.
- Each Institution shall advise students regarding transfer opportunities under this Agreement, and shall advise students of financial aid opportunities and implications associated with the transfer.

7. Should either Institution make changes to program requirements, the institution will inform the partner institution immediately. The articulation agreement should be updated to reflect the changes and forwarded to the Maryland Higher Education Commission.

C. Term and Termination

1. This agreement shall be effective on the date that it is signed by the appropriate and authorized representatives of each Institution.
2. Either Institution may, at its sole discretion, terminate this Agreement upon delivering 90 days written notice to the other Institution and the Maryland Higher Education Commission.
3. Both Institutions agree to meet once every 5 year(s) to review the terms of this agreement.

D. Amendment

1. This Agreement constitutes the entire understanding and agreement of the Institutions with respect to their rights and obligations in carrying out the terms of the Agreement, and supersedes any prior or contemporaneous agreements or understandings.
2. This Agreement may be modified only by written amendment executed by both Institutions.

E. Governing Law

This Agreement shall be governed by, and construed in accordance with, the laws of the State of Maryland.

F. Counterparts

This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

G. Notice of Agreement

1. The Institutions agree to provide a copy of this Agreement, with any amendments, to the Maryland Higher Education Commission.
2. The Institutions agree to provide copies of this Agreement to all relevant individuals and departments of the Institutions, including but not limited to students, academic department chairs participating in the transfer, offices of the president, registrar's offices, and financial aid offices.

H. No Third-Party Beneficiaries

There are no third-party beneficiaries to this Agreement.

I. Representations and Warranties of the Parties

Both Institutions represent and warrant that the following shall be true and correct as of the Effective Date of this Agreement, and shall continue to be true and correct during the term of this Agreement:

1. The Institutions are and shall remain in compliance with all applicable federal, state, and local statutes, laws, ordinances, and regulations relating to this Agreement, as amended from time to time.
2. Each Institution has taken all action necessary for the approval and execution of this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

College of Southern Maryland

By: Eileen Abel
Eileen Abel, Ph.D.
Vice President of Academic Affairs

8-21-19
Date

Goucher College

By: Scott Sibley
Scott Sibley, PhD
Interim Provost

8-21-19
Date

**ACADEMIC PROGRAM ARTICULATION AGREEMENT BETWEEN
COLLEGE OF SOUTHERN MARYLAND (CSM)
AND
STEVENSON UNIVERSITY (SU) REGARDING TRANSFER FROM CSM'S A.A.S. IN
CYBERSECURITY TO SU'S B.S. IN CYBERSECURITY AND DIGITAL FORENSICS**

This Academic Program Articulation Agreement ("Agreement") is entered into by and between College of Southern Maryland (the "Sending Institution") and Stevenson University the "Receiving Institution") (collectively, the "Institutions") to facilitate the transfer of academic credits from the A.A.S. in Cybersecurity for the completion of the B.S. in Cybersecurity and Digital Forensics (the "Program(s)").

A. Qualifying Students

This Agreement pertains to the transfer of "Qualifying Students", *i.e.*, those students who:

1. Have successfully completed the program at the Sending Institution;
2. Are enrolled in the Sending Institution, in good standing; and
3. Are accepted for admission to the Receiving Institution

B. Responsibilities of the Institutions

The Institutions agree to implement the transfer of Qualifying Students in accordance with applicable law and the following requirements and protocols:

1. A Qualifying Student may transfer into from the Transferring Institution into the Receiving Institution for the completion of the Program.
2. Courses that the Receiving School will accept credits for towards completion of the Program include:

	Community College Degree Requirements	Stevenson Equivalency	Credits Transferred
Program Requirements	ITS-1050 - Computing Essentials	IS-140 Information Systems Architecture and Design	3
	ITS-1960 - Introduction to Linux*	CDF-240: Linux System Administration	3
	ITS-2090 - Computer Security*	CDF-110: Cybersecurity and Digital Forensics Fundamentals	3
	ITS-2190 - Microsoft Window Server Administration*	IS 235 Advanced Windows Server Architecture & Administration	3
	ITS-2511 - Networking I*	IS 231 Network Technologies	3
	ENG-2050 - Business and Technical Writing*	MGT 210 Business Writing	3

	Community College Degree Requirements	Stevenson Equivalency	Credits Transferred
	ITS-2536 - Network & Infrastructure Defense*	CDF 251 Network Security	3
	ITS-2516 - Networking II*	CDF-252: Networking II	3
	ITS-2555 - Digital Forensics I*	CDF 261 Digital Forensics	3
	ITS-2500 - Ethical Hacking & Penetration Testing*	CDF 271 Intrusion and Penetration Testing	3
	ITS-2545 - Information Systems Security*	CDF-290: Legal Aspects of Cybersecurity	3
	CSC1110 - Program Design and Development	IS 240 Programming Concepts	3
Area of Concentration	Digital Forensics <ul style="list-style-type: none"> ITS-1120 - Introduction to Database* (3) ITS-2560 - Digital Forensics II* (3) OR Network Security <ul style="list-style-type: none"> ITS-2521 - Networking III* (3) ITS-2526 - Networking IV* (3) 	Elective Elective IS 232 TCP and IP Communication Protocols for Windows and UNIX Elective	6
English Composition and literature	ENG-1010 - Composition and Rhetoric*	English 151	3
Arts and Humanities	PHL-1150 - Cyber Ethics*	Humanities Requirement	3
Arts and Humanities	COM-1010 - Basic Principles of Speech Communication*	Communication-Intensive Requirement	3
Biological and Physical Sciences	Biological/physical sciences	Scientific Reasoning Requirement	3
Mathematics	MTH-1010 - Quantitative Literacy and Reasoning*	Quantitative Reasoning Requirement	3
Social and Behavioral Sciences	Social/behavioral sciences from the list of Cultural and Global Awareness classes	Social Science Requirement	3
Total	60 Credits (Generally this should add up to 60 credits) Please note: A minimum of 60 credits are needed for the associate degree		

Remaining Courses to be taken at Stevenson

Students who complete the plan above including all recommended courses and earn the A.A.S. in Cybersecurity will take the following courses at Stevenson to meet the B.S. requirements. Students who

transfer before completing the associate degree may have more general education and program requirements to take and fewer free electives.

General Education Requirements: 22 Credits

Freshman Composition II (3 credits)

Humanities (9 credits)

Fine Arts (3 credits)

Social Science (3 credits)

Scientific Reasoning Lab (4 credits)

Major Requirements (27-30 credits)

CDF 281 Advanced Network Defense 3 credits

CDF 391 Incident Response and Investigation 3 credits

CDF 392 Information Systems Forensic Internals – Auditing 3 credits

CDF 393 Forensic Evidence Collection Tools and Techniques 3 credits

CDF 475 Advanced Digital Forensics 3 credits

CDF 480 Cybersecurity and Digital Forensics Capstone 3 credits

IS 232 TCP and IP Communication Protocols for Windows and UNIX 3 credits (unless Network Security Concentration is completed at CSM) 3 credits

IS 331 CISCO TCP and IP Routing 3 credits

IS 365 Writing for IS Applications 3 credits

IS 432 Network Security-Firewalls, IDS, and Counter Measures 3 credits

Additional Credits Needed: 8-11 credits of general electives if need to reach a minimum of 120.

Total credits to be taken at SU: 60

Suggested Course Sequence

Suggested Course Sequence				
YEAR 3				
SEMESTER	FALL		SPRING	
RECOMMENDED COURSES	English 152: Introduction to Literature	3	CDF 475 Advanced Digital Forensics	3
	CDF 391 Incident Response and Investigation	3	CDF 281 Advanced Network	3
	Elective	3	IS 365 Writing for IS Applications	3
	Elective	3	IS 232 TCP and IP Communication Protocols for Windows and UNIX or elective	3
	CDF 392 Information Systems Forensic Internals – Auditing	3	CDF 393 Forensic Evidence Collection Tools and Techniques	3
CREDITS	15 CREDITS		15 CREDITS	
YEAR 4				

SEMESTER	FALL	SPRING
RECOMMENDED COURSES	Humanities 3	Social Science 3
	Humanities 3	Fine Arts 3
	Electives (if needed to reach 120) 3	IS 331 CISCO TCP and IP Routing 3
	IS 432 Network Security-Firewalls, IDS, and Counter Measures 3	CDF 480 Cybersecurity and Digital Forensics 3
	Lab Science 3	Humanities 3
CREDITS	15 CREDITS	X CREDITS

3. Additional Provisions

- Courses that fulfill program requirements are only eligible for transfer if students have earned a grade of "C" or better. Courses used to fulfill only general education requirements are eligible for transfer if students have earned a grade of "D" or better.
- Students must maintain a (a 2.5) cumulative grade point average in order to transfer.
- Stevenson University will accept up to 70 credits from 2-year institutions. Up to 90 credits can be applied to degree requirements from a combination of 2-year institutions, 4-year institutions, and non-direct classroom instruction (including CLEP, AP, and other nationally recognized standardized examination scores). For additional information about credit transfer, please see: <http://www.stevenson.edu/admissions-aid/getting-started/transfer-students/transfer-credit-evaluation/>
- For non-direct classroom instruction, an appropriate score is determined by Stevenson University, and student must submit original test scores/results to Stevenson University. Tech Prep credits will/will not transfer. Credit awarded for prior learning ("life experience") is not recognized by, and is not transferable to, Stevenson University.
- Students intending to transfer should complete the admission application for Stevenson University following the third semester of their Associate Degree program. Students should contact the Financial Aid Office at Stevenson University as soon as possible in regard to college deadlines for financial aid. Students who have completed an associate degree at a Maryland community college are guaranteed admissions to Stevenson.

4. The Receiving Institution shall designate, and shall provide to the Sending Institution, the contact information for a staff person at the Receiving Institution who is responsible for the oversight of the transfer of Qualifying Students. The Sending Institution shall designate, and shall provide to the Receiving Institution, the contact information for a staff person at the Sending Institution who is responsible for the oversight of the transfer of Qualifying Students.

	Sending Institution	Receiving Institution
--	---------------------	-----------------------

Name of staff person responsible for oversight	Jacqui Rogers	Dave Copenhaver
Title of staff person	Coordinator of Transfer and Articulation	Assistant Director of Transfer Admissions
Email address	jrogers@csmd.edu	wcopenhaver@stevenson.edu
Telephone Number	301-934-7571	(443)352-4409

Should the staff person or position change, the institution will promptly provide new contact information to the partner institution and inform the Maryland Higher Education Commission of the change.

Additional contact information:

[Role & Responsibilities of persons listed here]	Sending Institution	Receiving Institution
Name of person	Chris Estes	Bridget Brennan
Title of person	Cybersecurity Program Coordinator	AVP, Academic Affairs
Email address	CAEstes@csmd.edu	bhbrennan@stevenson.edu
Telephone Number	443-550-6156	443-352-5445

5. If the Qualifying Student is using federal Title 38 VA Education Benefits (GI Bill® Education Benefits), the Institutions shall adhere to all applicable U.S. Department of Veterans Affairs' regulations, including the regulations governing the awarding prior credit, as regulated under Title 38, Code of Federal Regulations, Sections 21.4253(d)(3) and 21.4254(c)(4).
 - For scholarship information please see the "Paying for College" page on: <http://www.stevenson.edu/transfer>
6. Each Institution shall adhere to all applicable transfer requirements set forth in the Annotated Code of Maryland and the Code of Maryland Regulations.
7. Each Institution shall advise students regarding transfer opportunities under this Agreement, and shall advise students of financial aid opportunities and implications associated with the transfer.
8. Should either Institution make changes to program requirements, the institution will inform the partner institution immediately. The articulation agreement should be updated to reflect the changes and forwarded to the Maryland Higher Education Commission.

C. Term and Termination

1. This agreement shall be effective on the date that it is signed by the appropriate and authorized representatives of each Institution.

2. Either Institution may, at its sole discretion, terminate this Agreement upon delivering 60 days written notice to the other Institution and the Maryland Higher Education Commission.
3. Both Institutions agree to meet once every 2 year(s) to review the terms of this agreement.

D. Amendment

1. This Agreement constitutes the entire understanding and agreement of the Institutions with respect to their rights and obligations in carrying out the terms of the Agreement, and supersedes any prior or contemporaneous agreements or understandings.
2. This Agreement may be modified only by written amendment executed by both Institutions.

E. Governing Law

This Agreement shall be governed by, and construed in accordance with, the laws of the State of Maryland.

F. Counterparts

This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

G. Notice of Agreement

1. The Institutions agree to provide a copy of this Agreement, with any amendments, to the Maryland Higher Education Commission.
2. The Institutions agree to provide copies of this Agreement to all relevant individuals and departments of the Institutions, including but not limited to students, academic department chairs participating in the transfer, offices of the president, registrar's offices, and financial aid offices.

H. No Third-Party Beneficiaries

There are no third-party beneficiaries to this Agreement.

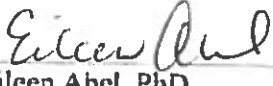
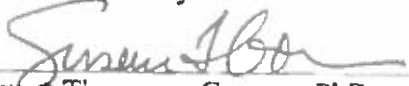
I. Representations and Warranties of the Parties

Both Institutions represent and warrant that the following shall be true and correct as of the Effective Date of this Agreement, and shall continue to be true and correct during the term of this Agreement:

1. The Institutions are and shall remain in compliance with all applicable federal, state, and local statutes, laws, ordinances, and regulations relating to this Agreement, as amended from time to time.

2. Each Institution has taken all action necessary for the approval and execution of this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

College of Southern Maryland	Stevenson University
By: 	By: 
Eileen Abel, PhD Vice President of Academic Affairs	Susan Thompson Gorman, PhD EVP Academic Affairs and Provost
Date: <u>June 26, 2019</u>	Date: <u>06/19/19</u>

