Courses Required for the AAS in Cybersecurity
Courses Grouped By Category

General Education and Program-Related Requirements (24 credits)

ENG 111	College Composition I	3
ENG 112	College Composition II	3
MTH 151	Mathematics for Liberal Arts I or higher level course	3
SDV 101	Orientation to IT Professions	1
	Humanities/Fine Arts Elective	3
	Social Science Elective	3
PED	Physical Education and Health Elective	1
CST 110	Introduction to Communications	3
_____	Natural Science w/Lab	4

Program Requirements (43 credits)

ITN 100	Introduction to Telecommunications	3
ITP 100	Software Design	3
ITE 221	PC Hardware and OS Architecture	3
ITN 200	Administration of Network Resources	3
ITP	Programming Elective	4
ITN 260	Network Security Basics	3
ITN 170	Linux System Administration	3
ITN 261	Network Attacks, Computer Crime, and Hacking	3
ITN 262	Network Communications, Security and Authentication	3
ITN 263	Internet/Intranet Firewalls and E-Commerce Security	3
ITN 266	Network Security Layers	3
ITN 267	Legal Topic in Network Security	3
ITN 276	Computer Forensics I	3
ITN/ITP	Networking/Programming Elective	3

Minimum Credits Required 67

Course Descriptions

CST 110 – Introduction to Communications 3 Credits

Examines the elements of affecting speech communication at the individual, small group and public communication levels with emphasis on practice of communication at each level. Lecture 3 hours per week.

ENG 111 – College Composition I 3 Credits

Introduces students to critical thinking and the fundamentals of academic writing. Through the writing process, students refine topics; develop and support ideas; investigate, evaluate, and incorporate appropriate resources; edit for effective style and usage; and determine appropriate approaches for a variety of contexts, audiences, and purposes. Writing activities will include exposition and argumentation with at least one researched essay. Lecture 3 hours per week.

ENG 112 – College Composition II 3 Credits

Continues to develop college writing with increased emphasis on critical essays, argumentation, and research, developing these competencies through the examination of a range of texts about the human experience. Requires students to locate, evaluate, integrate, and document sources and effectively edit for style and usage. Prerequisite: Students must successfully complete ENG 111 or its equivalent, and must be able to use word processing software. Lecture 3 hours per week.

Humanities/Fine Arts Elective 3 Credits

ITE 221 – PC Hardware and OS Architecture 3 Credits

Covers instruction about processors, internal functions, peripheral devices, computer organization, memory management, architecture, instruction format, and basic OS architecture. Lecture 3 hours per week.

ITN 100 – Introduction to Telecommunications 3 Credits

Surveys data transmission systems, communication lines, data sets, network, interfacing, protocols, and modes of transmission. Emphasizes network structure and operation. Lecture 3 hours per week.

ITN 170 – Linux System Administration 3 Credits

Focuses instruction on the installation, configuration and administration of the Linux operating system and emphasizes the use of Linux as a network client and workstation. Lecture 3 hours per week.

ITN 200 – Administration of Network Resources 3 Credits

Focuses on the management of local area network servers. Teaches proper structuring of security systems. Explains print queues, disk management, and other local area network (LAN) issues. Presents concerns and issues for the purchase and installation of hardware and software upgrades. The course can be taught using any network operating system or a range of operating systems as a delivery tool. Lecture – 3 hours per week.

ITN 260 – Network Security Basics 3 Credits

Explores the basics of network security in depth. Includes security objectives, security architecture, security models and security layers. Discusses risk management, network security policy, and security training. Discusses the five security keys: confidentiality, integrity, availability, accountability, and auditability. Lecture 3 hours per week.

ITN 261 – Network Attacks, Computer Crime, and Hacking 3 Credits

Provides an in-depth exploration of various methods for attacking and defending a network. Explores network security concepts from the point of view of hackers and their attack methodologies. Discusses hackers, attacks, Intrusion Detection Systems (IDS), malicious code, computer crime, and industrial espionage. Lecture 3 hours per week.

ITN 262 – Network Communications, Security, and Authentication 3 Credits

Provides an in-depth exploration of various communication protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker in order to highlight protocol weaknesses. Discusses Internet architecture, routing, addressing, topology, fragmentation, and protocol analysis. Includes the use of various utilities to explore TCP/IP. Lecture 3 hours per week.

ITN 263 – Internet/Intranet Firewalls and E-Commerce Security 3 Credits

Provides an in-depth exploration of firewalls, Web security, and e-commerce security. Explores firewall concepts, types, topology, and the firewall's relationship to the TCP/IP protocol. Explores client/server architecture, the Web server, HTML, and HTTP in relation to Web security. Discusses digital certification, 7D.509, and Public Key Infrastructure (PKI). Lecture 3 hours per week.

ITN 266 – Network Security Layers 3 Credits

Provides an in-depth exploration of various security layers needed to protect the network. Explores Network Security from the viewpoint of the environment in which the network operates and the necessity to secure that environment to lower the security risk to the network. Includes physical security, personnel security, operating system security, software security and database security. Lecture 3 hours per week.

ITN 267 – Legal Topics in Network Security 3 credits

Conveys an in-depth exploration of the civil and common law issues that apply to network security. Explores statutes, jurisdictional, and constitutional issues related to computer crimes and privacy. Includes rules of evidence, seizure and evidence handling, court presentation and computer privacy in the digital age.

Lecture 3 hours per week.

ITN 276 – Computer Forensics I 3 Credits

Teaches computer forensic investigation techniques for collecting computer-related evidence at the physical layer from a variety of digital media (hard drives, compact flash and PDAs) and performing analysis at the file system layer. Lecture 3 hours per week

ITP 100 – Software Design 3 Credits

Introduces principles and practices of software development. Course content includes instruction in critical thinking, problem solving skills, and essential programming logic in structured and object-oriented design using contemporary tools. Lecture 3 hours per week.

ITP – Programming elective 4 Credits

ITN/ITP – Networking/Programming elective 3 credits

MTH 151 – Mathematics for Liberal Arts I 3 Credits

Presents topics in sets, logic, numeration systems, geometric systems, and elementary computer concepts. The general purpose of this course is to give the student an appreciation for the uses of mathematics in the contemporary world and to develop ability by the student to solve certain mathematical problems in a logical manner. Lecture 3 hours per week.

PED - Physical Education or Health Elective 1 Credit

SDV 101 – Orientation to IT professions 1 Credit

Introduces students to the skills which are necessary to achieve their academic goals, to services offered at the college and to the discipline in which they are enrolled. Covers topics such as services at the college including the learning resources center; counseling, and advising; listening, test taking, and study skills; and topical areas which are applicable to their particular discipline. Lecture 1 hour per week.

Social Science Elective 3 Credits

Natural Science with Lab 4 Credits

Catalog Layout

Cybersecurity **MIDD, FAUQ**
Associate of Applied Science Degree

PURPOSE: This curriculum is designed for those who seek employment in the field of cybersecurity (information assurance), for those who are presently in IT or a security field and who desire to increase their knowledge and update their skills, and for those who must augment their abilities in other fields with knowledge and skills in information security. The curriculum is mapped to the NSA/DHS Knowledge Units necessary for LFCC's designation as a Center of Academic Excellence – Two Year.

OCCUPATIONAL OBJECTIVES: The degree prepares students for careers in business, government and industry as information security specialists, cybersecurity analysts, cyber-defense penetration testers and entry-level digital forensics specialists.

TRANSFER GUIDELINES: Transfer is not the primary purpose of an A.A.S. program, but a transfer pathway is a component under the CAECD 2Y designation. LFCC has transfer arrangements that facilitate the transfer of this degree to selected senior institutions. Students interested in transfer should contact their academic advisor early in the program for specific course requirements. However, certain requirements are as follows:

1. Student transferring to the BAS in Cybersecurity at GMU should take the following courses external to this degree program before transferring:
    - ITE 115 (Variable credit corresponding to GMU IT 194: see advisor);
        - It is recommended that this course is completed prior to entry into the degree program
    - ENG 241 Literature (Meet GMU's Literature requirement)
    - Two social science electives from approved list on page 41 (See note 4)
    - Science w/o lab requirement will need to be satisfied at GMU
2. Students transferring to the BPS in Cybersecurity at GWU should take the following course external to this degree program before transferring:
    - One social science elective from approved list on page 41

PROGRAM REQUIREMENTS: The student must possess strong analytical problem-solving skills, strong written and verbal communications skills and must have good interpersonal skills. The curriculum contains highly technical courses consisting of theoretical concepts and practical applications applicable to the cybersecurity industry and government environment. Upon satisfactory completion of the program, the graduate will be awarded the Associate of Applied Science in Cybersecurity.

Course		Title	Credits
1st Semester			
ENG	111	College Composition I	3
ITE	221	PC Hardware and OS Architecture	3
ITN	100	Intro to Telecommunications	3
ITP	100	Software Design	3
MTH	151	Mathematics for Liberal Arts I or higher-level math[1]	3
SDV	101	Orientation to IT Professions	1
Total			**16**
2nd Semester			
ENG	112	College Composition	3
CST	110	Intro to Speech Communication	3
ITP		Programming Elective[2]	4
ITN	170	Linux Administration	3
ITN	260	Network Security Basics	3
PED		PED Elective	1
Total			**17**
3rd Semester			
____		Approved Humanities/Fine Arts Elective[3]	3
____		Approved Social Science Elective[4]	3
ITN	200	Administration of Network Resources	3
ITN	261	Network Attacks, Computer Crime and Hacking	3
ITN	262	Network Communications, Security and Authentication	3
ITN	266	Network Security Layers	3
Total			**18**
4th Semester			
ITN	263	Internet/Intranet Firewalls and E-Commerce	3
ITN	267	Legal Topics in Network Security	3
ITN	276	Computer Forensics I	3
——		Natural Science w/Lab[5]	4
ITN/ITP		Networking/Programming Elective[6]	3
Total			**16**
Total credits for the Cybersecurity A.A.S.=67			

IT courses used for this program may not be more than 6 years old, unless approved by division dean.

[1]Students planning to transfer to another four-year college are encouraged to see advisor prior to math selection so as to ensure proper math required for the student's transfer institution. GWU requires math course to achieve a C or better.

[2] GMU requires Java language for programming courses (ITP 120, ITP 220)

[3]Students may select humanities elective from approved list. *Students pursuing the Bachelors of Professional Studies in Cybersecurity at George Washington University are encouraged to take HIS, PHI, REL, ENG 200-level literature courses and Foreign Language 200-level courses; . Students pursuing the*

Bachelors of Applied Science in Cybersecurity at George Mason University are encouraged to take ART100, ART 101, ART 102 (Fine Arts)

[4]Students may select social science elective from approved list on Page 41. *Students pursuing the Bachelor of Applied Science degree at George Mason University are encouraged to take HIS 101, HIS 102, or HIS 112 as their LFCC social science elective. However, HIS 111 is transferrable as Global Understanding at GMU. Students pursuing the Bachelors of Professional Studies in Cybersecurity at George Washington University are encouraged to take HIS 101, HIS 102, HIS 111 or HIS 112 as their LFCC social science elective. For this requirement, it is best for the student to see an LFCC advisor to ensure proper sequencing.*

[5]If transferring to GMU/GWU, students may select Science with Laboratory 4 credit elective from the approved list on page 41 except for BIO 141-142 (Human Anatomy and Physiology)

[6]Students may select one of the following courses: ITP 120, ITP 220, ITP 251, ITN 124, ITN 208; if transferring to GMU, select one of the following: ITP 120, ITP 220, ITN 106, ITN 208.

NOTES:

Students planning on transferring to GMU's BAS in Cybersecurity must have completed the AAS in Cybersecurity degree with a minimum 2.0 GPA. GMU has waived the age requirements for the BAS in Cybersecurity degree. Students should meet with the GMU academic advisor to sign the BAS Age Waiver form.

GWU requires that all transfer credits have a C or better and the GPA to be at least 2.7.

∞

This does not constitute a guarantee of admission or of transferability, as this is a guideline based on the most recent information provided to us by our senior institution partners, Students should check with the advisors at the senior institution into which they intend to transfer prior to applying for admission.