CYBER AND INFORMATION SECURITY - ASSOCIATE OF APPLIED SCIENCE

Curriculum Code #6470

Effective May 2024

Division of Engineering, Business and Information Technologies (http://catalog.lorainccc.edu/academic-programs/engineering-business-information-technologies/)

The Associate of Applied Science degree program in Cyber and Information Security prepares students for employment in a variety of careers in Cyber Security. Examples of positions can include such titles as network security specialist, information security technician, and cybersecurity specialist. In addition to basic computer and networking skills, this degree provides a solid foundation in information assurance, cybercrime investigation, ethical hacking, digital forensics, network forensics, cyber operations, Internet of Things, data collection, software exploitation, analysis of malicious code, reverse engineering, data integrity, risk assessment and mitigation techniques. Lab work and assignments will present real world cyber security scenarios encountered in the work place. Industry standard software will be used for digital forensics studies. Lorain County Community College has articulation agreements with colleges and universities including programs offered by Lorain County Community College's University Partnership.

First Year		
Fall Semester		**Hours**
CMNW 101	A+ CERTIFICATION PREPARATION I	4
CISS 125 or CMNW 201	OPERATING SYSTEM INTERFACES [1, 2] or A+ CERTIFICATION PREP II	3-4
ENGL 161	COLLEGE COMPOSITION I	3
MTHM 158 or PHLY 171	QUANTITATIVE REASONING [3] or INTRODUCTION TO LOGIC	3
SDEV 101	INTRODUCTION TO THE LCCC COMMUNITY [4]	1
	Hours	**14-15**
Spring Semester		
CISS 145 or CMNW 145	LOCAL AREA NETWORKS [1] or NETWORK INSTALLATION/ DIAGNOSTICS	4
CMNW 120	CYBER-FOREN CYBER CRIME THE LAW	4
ENGL 164	COLLEGE COMPOSITION II WITH TECHNICAL TOPICS [1]	3
PHLY 161	INTRODUCTION TO ETHICS	3
PSYH 151	INTRODUCTION TO PSYCHOLOGY	3
	Hours	**17**
Second Year		
Fall Semester		
BIOG 164	EXPLORATIONS IN FIELD SCIENCE	3
CISS 165	CISCO CCNA V7 INTRODUCTION TO NETWORKING	3
CMNW 223	NETWORK FORENSICS AND INVESTIGATIVE TECHNIQUES	4
CYBR 220	PYTHON SCRIPTING AND PROGRAM CONCEPTS	3
CYBR 231	ETHICAL HACKING AND COUNTERMEASURES	4
CYBR 287	WORK-BASED LEARNING I - CYBR	1
	Hours	**18**
Spring Semester		
CYBR 110	FUNDAMENTALS OF INTERNET OF THINGS (IOT)	4
CYBR 244	CYBERSECURITY STANDARDS, REGULATIONS AND COMPLIANCE	3
CYBR 251	CYBER DEFENSE METHODS [1]	3
CYBR 252	IT SECURITY CONCEPTS	4
CYBR 288	WORK-BASED LEARNING II - CYBR	1
	Hours	**15**
	Total Hours	**64-65**

1

Indicates that this course requires a college level prerequisite.

2

Students pursuing the Cyber and Information Security degree program have divisional approval to take CISS 125 without having completed CISS 121.

3

MTHM 158 or PHLY 171 is preferred. An Ohio Transfer Module mathematics course will also satisfy the requirement but any college level math course will be accepted.

4

A student must register for the orientation course when enrolling for more than six credit hours per semester or any course that would result in an accumulation of thirteen or more credit hours.

5

The cyber core courses in this program may be earned through a competency-based education option. See your advisor for more information.

Program Contact(s):

Lawrence Atkinson
440-366-7050
latkinso@lorainccc.edu

For information about admissions, enrollment, transfer, graduation and other general questions, please contact your advising team (https://www.lorainccc.edu/admissions-and-enrollment/advising-and-counseling/).

More program information can be found on our website. (https://www.lorainccc.edu/it/associate-applied-science-cyber-information-security/)

Credit for Prior Learning (PLA) options may be available for your program. For more information, please visit our website: www.lorainccc.edu/PLA (http://www.lorainccc.edu/PLA/)

1. Describe methods for investigating both domestic and international cybersecurity incidents.
2. Develop short and long-term organizational cybersecurity strategies and policies.

3. Implement cyber security goals, metrics, and safeguards consistent with industry best practices.
4. Conduct security assessments to identify vulnerabilities in critical infrastructure systems.
5. Evaluate a variety of cybersecurity tools.