Cybersecurity, B.S.

Degree Offered

- Bachelor of Science

Nature of the Program

Students will be able to recognize the relevant issues in cybersecurity and have knowledge in the areas: data security, software security, system security, human security, organizational security and societal security. Students will be able to apply the ethical aspects and cyber laws in each cybersecurity area. The Bachelor of Science degree in cybersecurity is accredited by the Computing Accreditation Commission of ABET, http://www.abet.org, under the General Criteria and the Program Criteria for Cybersecurity

Program Educational Objectives

The objective of the bachelor's degree program in Cybersecurity (CYBE) at West Virginia University is to produce graduates who have the attitudes that will ensure success in professional positions in business, industry, research, governmental service, or graduate study or professional school.

Curriculum in Cybersecurity

General Education Foundations

Please use this link to view a list of courses that meet each GEF requirement. **(**http://registrar.wvu.edu/gef/**)**

NOTE: Some major requirements will fulfill specific GEF requirements. Please see the curriculum requirements listed below for details on which GEFs you will need to select.

Code	Title	Hours
General Education Foundations		
F1 - Composition & Rhetoric		3-6
ENGL 101 & ENGL 102	Introduction to Composition and Rhetoric and Composition, Rhetoric, and Research	
or ENGL 103	Accelerated Academic Writing	
F2A/F2B - Science & Technology		4-6
F3 - Math & Quantitative Reasoning		3-4
F4 - Society & Connections		3
F5 - Human Inquiry & the Past		3
F6 - The Arts & Creativity		3
F7 - Global Studies & Diversity		3
F8 - Focus (may be satisfied by completion of a minor, double major, or dual degree)		9
Total Hours		31-37

Please note that not all of the GEF courses are offered at all campuses. Students should consult with their advisor or academic department regarding the GEF course offerings available at their campus.

Degree Requirements

Students must meet the following criteria to qualify for a Bachelor of Science with a major in Cybersecurity degree:

- Complete a minimum of 122 credit hours
- Satisfy WVU's undergraduate degree requirements
- Satisfy Statler College's undergraduate degree requirements (http://catalog.wvu.edu/undergraduate/collegeofengineeringandmineralresources/#policiestext)
- Complete all courses listed in the curriculum requirements with the required minimum grades
- Attain an overall grade point average of 2.00 or better
- Attain a WVU grade point average of 2.00 or better
- Attain a Statler grade point average of 2.00 or better
- A maximum of one math or science courses with a grade D+, D-, or D may apply towards a Statler College degree.

- Complete a survey regarding their academic and professional experiences at WVU, as well as post-graduation job placement or continuing education plans.

The Statler GPA is computed based on all work taken at WVU with a subject code within Statler College (BIOM, BMEG, CE, CHE, CPE, CS, CSEE, CYBE, EE, ENGR, ENVE, ETEC, IENG, IH&S, MAE, MINE, PDA, PNGE, ROBE, SAFM, SENG) excluding ENGR 140, ENGR 150, and CS 101. The WVU GPA is computed based on all work taken at WVU. The Overall GPA is computed based on all work taken at WVU and transfer work.

Curriculum Requirements

Code	Title	Hours
University Requirements		19
Fundamentals of Engineering Requirements		2
Math and Science Requirements		22
Cybersecurity Program Requirements		79
Total Hours		122

University Requirements

Code	Title	Hours
General Education Foundations (GEF) 1, 2, 3, 4, 5, 6, 7, and 8 (31-37 Credits)		
Outstanding GEF Requirements 1, 4, 5, 6, and 7		18
ENGR 191	First-Year Seminar	1
Total Hours		19

Fundamentals of Engineering Requirements

Code	Title	Hours
A minimum grade of C- is required in all Fundamentals of Engineering courses.		
ENGR 101	Engineering Problem Solving 1	2
Total Hours		2

Math and Science Requirements

Code	Title	Hours
A minimum grade of C- is required in all Math and Science courses.		
MATH 155	Calculus 1 (GEF 3)	4
MATH 156	Calculus 2 (GEF 8)	4
MATH 373	Introduction to Cryptography	3
STAT 215	Introduction to Probability and Statistics	3
Lab Science Electives I (GEF 2B) & II (GEF 8): Select two GEF 2B courses and accompanying labs		8
Total Hours		22

Cybersecurity Program Requirements

Code	Title	Hours
CYBE 266	Foundations of Cybersecurity	3
CYBE 366	Secure Software Development	3
CYBE 435	Computer Incident Response	3
CYBE 460	Foundation of Cybersecurity 2	3
CYBE 466	Host Based Cyber Defense	3
CYBE 467	Ethical Hacking & Penetration Testing	3
CPE 271 & 271L	Introduction to Digital Logic Design and Digital Logic Laboratory	4
CPE 310	Microprocessor Systems	3
CPE 453	Data and Computer Communications	3
CS 110 & 110L	Introduction to Computer Science and Introduction to Computer Science Laboratory	4

CS 111 & 111L	Introduction to Data Structures and Introduction to Data Structures Laboratory	4
CS 210	File and Data Structures	4
CS 220	Discrete Mathematics	3
CS 330 & 330L	Introduction to Software Engineering and Introduction to Software Engineering Laboratory	4
CS 350	Computer System Concepts	3
CS 450	Operating Systems Structure	4
CSEE 380	Engineering for Societal Impact	2
CSEE 480S	Capstone Project - Design	2
or CSEE 480	Capstone Project - Design	
CSEE 481S	Capstone Project - Implementation	3
or CSEE 481	Capstone Project - Implementation	
BETH 357	The Ethics of Information Technology	3
CRIM 431	Cybercrime	3
SOC 101	Introduction to Sociology (GEF 8)	3
CS/CYBE Electives (400-level or higher courses in CS or CYBE subject codes) *		6
Lane Department Elective (400-level or higher course in BIOM, CPE, CS, CSEE, CYBE, EE, or ROBE subject codes) *		3
Total Hours		79

*

Excludes CYBE 465

Suggested Plan of Study

It is important for students to take courses in the order specified as closely as possible; all prerequisites and concurrent requirements must be observed. A typical B.S. degree program that completes degree requirements in four years is as follows.

First Year

Fall	Hours	Spring	Hours
CS 110 & 110L	4	CS 111 & 111L	4
ENGR 101	2	ENGL 101 (GEF 1)	3
ENGR 191	1	MATH 156 (GEF 8)	4
MATH 155 (GEF 3)	4	Lab Science II	4
Lab Science I (GEF 2)	4		
	15		15

Second Year

Fall	Hours	Spring	Hours
CYBE 266	3	CPE 271 & 271L	4
CS 210	4	CS 350	3
CS 220	3	MATH 373	3
ENGL 102 (GEF 1)	3	SOC 101 (GEF 8)	3
GEF 4	3	STAT 215	3
	16		16

Third Year

Fall	Hours	Spring	Hours
CPE 310	3	CYBE 366	3
CPE 453	3	CYBE 460	3
CS 330 & 330L	4	CS 450	4
CRIM 431	3	BETH 357	3
CSEE 380	2	GEF 6	3
	15		16

Fourth Year			
Fall	**Hours**	**Spring**	**Hours**
CYBE 435	3	CYBE 467	3
CYBE 466	3	CSEE 481S	3
CSEE 480S	2	CS/CYBE Elective	3
CS/CYBE Elective	3	Lane Department Elective	3
GEF 7	3	GEF 5	3
	14		15

Total credit hours: 122

Area of Emphasis

- Artificial Intelligence

AREA OF EMPHASIS IN ARTIFICIAL INTELLIGENCE

Code	Title	Hours
CS 472	Artificial Intelligence	3
CS 474	Introduction to Responsible and Safe AI	3
Select two of the following:		6
CPE 420	Introduction to Neural Networks	
CS 460	Introduction to Big Data Engineering	
CS 473	Introduction to Data Mining	
CS 476S	Applied Artificial Intelligence Studio	
EE 465	Introduction to Digital Image Processing	
Total Hours		12

Lane Department Dual Degree Programs

Students can simultaneously pursue two bachelor's degrees in the Lane Department. To successfully complete both degrees, students must meet all requirements of both programs and complete a minimum of 150 credit hours. As part of those 150 credit hours, 30 credit hours must be unique from the primary degree course requirements. Exact credit hours and classes will vary per student based on their choice of technical electives and emphasis courses.

The most common Lane Department major combinations are:

- Computer Engineering and Electrical Engineering
- Computer Engineering and Computer Science

Please refer to the catalog descriptions of each individual program for course and academic requirements which can include minimum grades and GPA, and elective choices.

Program Educational Objectives

The objective of the bachelor's degree program in Cybersecurity (CYBE) at West Virginia University is to produce graduates who have the attitudes that will ensure success in professional positions in business, industry, research, governmental service, or graduate study or professional school

Major Learning Outcomes

CYBERSECURITY

Students will be able to recognize the relevant issues in cybersecurity and have knowledge in the areas: data security, software security, system security, human security, organizational security and societal security. Students will be able to apply the ethical aspects and cyber laws in each cybersecurity area.

Upon graduation, all students obtaining a major in cybersecurity will be able to:

1. Identify a range of current problems and threats in cybersecurity.
2. Detect and analyze cybersecurity attack and practice defense strategies against them.
3. Write secure software.

4. Analyze networks and network security.
5. Plan, implement, and assess security protection mechanisms in computer systems and networks.