# Cybersecurity, M.S.

## Degree Offered

- Master of Science, Cybersecurity (M.S.)

## Nature of the Program

The Lane Department of Computer Science and Electrical Engineering offers the Master of Science in Cybersecurity (M.S. Cybersecurity), a fully online graduate program designed to prepare students for real-world, industry-ready roles in the rapidly evolving cybersecurity landscape. Tailored for professionals and recent graduates with foundational knowledge or practical experience in computer science, computer engineering, or related fields, the program blends theoretical foundations with applied expertise in hardware and software security, secure system design, and critical infrastructure protection. With five core courses and five electives that can be customized to individual interests, students gain the ability to design, implement, test, and critically evaluate secure systems across a range of domains, including energy systems, cloud computing, and intelligent infrastructure. The flexible online structure supports full-time professionals, career changers, recent graduates, and aspiring researchers, providing a rigorous yet accessible pathway into one of the most in-demand and impactful technology fields of the future.

## Program Educational Objectives

The objective of the M.S. in Cybersecurity program is to produce graduates with the knowledge, technical expertise, and professional mindset needed for success in business, industry, research, and government roles. After completing the required core and elective courses, students will achieve proficiency in:

- Cybersecurity Principles and Methodologies, including risk assessment, threat analysis, and defensive strategies for protecting digital systems and networks.
- Application of Security Techniques across a variety of domains such as cloud computing, software systems, critical infrastructure, and embedded devices.
- Design and Implementation of Secure Systems, with the ability to architect, test, and evaluate hardware, software, and network defenses against evolving cyber threats.
- Cybersecurity Research and Innovation, including the ability to investigate emerging vulnerabilities, develop new countermeasures, AI/ML applications, and effectively communicate findings to technical and non-technical audiences.
- Ethical, Legal, and Societal Dimensions of Cybersecurity, encompassing privacy, data protection, policy, and responsible conduct in the global digital landscape.

## Admissions for 2027-2028

To be eligible for admission into the Master of Science in Cybersecurity degree program, a candidate must fulfill the following requirements:

- Submit a personal statement. Personal statements should be 750 to 1,000 words and double-spaced. This is an opportunity to tell the admissions committee more about your reasons to earn this degree and should not repeat the information on your resume.
- Submit two (2) professional and/or educational references.
- Submit official transcripts showing degree completion of a bachelor's degree in computer science, computer engineering, cybersecurity, or a closely related field from an accredited University, with a minimum cumulative grade point average of 3.0 (on a 4-point scale) or better.
- Submit a resume that reflects your education and experience.

*Students with a degree in other fields of study from accredited institutions, but having at least one year experience in cybersecurity/AI/ML may be considered for provisional admission. One year experience should be highlighted through reference letter(s) and other documents. Provisional students will be required to complete three core courses with a 'B' or above. After successful completion of three core courses, the student will move to regular graduate status.

GRE is not required but may be submitted to assist in admission decision.

International applicants must meet the WVU requirement of English language proficiency (https://graduateadmissions.wvu.edu/how-to-apply/international-graduate-applicant/).

## Curriculum in Master of Science in Cybersecurity

A candidate for the M.S. degree in cybersecurity must comply with the rules and regulations as outlined in the WVU Graduate Catalog and the specific requirements of the Statler College and the Lane Department of Computer Science and Electrical Engineering.

## Program Requirements

All M.S. degree candidates are required to follow a planned program of study. The student's faculty advisor, in conjunction with the student's Advising and Examining Committee (AEC) will be responsible for determining the plan of study appropriate to the student's needs. The underlying principle of the planned program is to provide the student with the necessary support to complete their degree and prepare them for their career.

## Curriculum Requirements

| Code | Title | Hours |
|---|---|---|
| A minimum cumulative GPA of 3.0 is required | | |
| Up to 6 credit hours can be at the 400 level | | |
| **Course Requirements** | | |
| CPE 530 | Hardware Security and Trust | 3 |
| CPE 553 | Advanced Networking Concepts | 3 |
| CYBE 510 | Advanced Cybersecurity Principles | 3 |
| CYBE 520 | Ethics in Cybersecurity | 3 |
| CYBE 660 | Engineering Secure Software | 3 |
| **Elective Courses** | | **15** |
| Select from the following: | | |
| AI 472 | Artificial Intelligence [*] | |
| or CPE 520 | Application of Neural Networks | |
| or CS 676 | Machine Learning | |
| AI 720 | Generative AI | |
| CPE 538 | Intro Computer Security Management | |
| CPE 620 | Deep Learning | |
| CYBE 467 | Ethical Hacking & Penetration Testing | |
| CYBE 564 | Software Engineering of Mobile Applications | |
| CYBE 640 | Data Analytics for Secure Cyber-Power Systems | |
| CYBE 650 | Cloud Computing and the Internet of Things | |
| **Total Hours** | | **30** |

* Students may select only one of AI 472, CPE 520, or CS 676 to fulfill one Elective Course requirement.

## Student Learning Outcomes

### CYBERSECURITY

Program learning outcomes (PLO) for students in the program will include:

1. PLO 1: Assess the security of digital systems with respect to confidentiality, integrity, and availability.
2. PLO 2: Explain hardware, software and network security threats and countermeasures
3. PLO 3: Evaluate cybersecurity vulnerabilities to critical infrastructure
4. PLO 4: Design secure hardware, software and network architectures
5. PLO 5: Compare ethical approaches to current cybersecurity issues