



# OLD DOMINION UNIVERSITY®

## School *of* Cybersecurity

### **Undergraduate Student Handbook**

#### **Director's Welcome**

Welcome to the School of Cybersecurity at Old Dominion University. Our mission is to prepare the next generation of cybersecurity professionals with the knowledge, skills, and real-world experiences needed to protect the world's information systems.

The School of Cybersecurity provides interdisciplinary, hands-on education spanning technical, managerial, social, and policy dimensions of cybersecurity. Our programs align with federal designations as a Center of Academic Excellence in Cyber Defense and Cyber Operations. To explore the complete mission, vision, and academic approach,

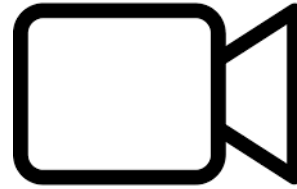
The Director's full message is maintained online and updated regularly. For the most current version, refer to the [School of Cybersecurity's Mission Statement](#).

#### **Multi-Media Resources**

Below are multi-media resources describing the ODU School of Cybersecurity's programs and teaching approach.



## [Podcast](#)



## [Video](#)

### **Meet the Team**

Our faculty brings a truly global perspective to cybersecurity, representing countries and research traditions from around the world. Faculty members come to ODU with deep experience across commercial industries, government agencies, and international research labs. This mix of backgrounds ensures students learn from experts who have defended real systems, shaped policies, and worked on emerging challenges at national and global levels.

Please visit the [faculty directory](#) for a complete list of ODU's School of Cybersecurity Faculty.

### **An Interdisciplinary Approach to Cybersecurity**

At ODU, we take an interdisciplinary approach to the field of cybersecurity. Students receive not only a robust technical education but are exposed to a number of other fields necessary to succeed in the rapidly evolving world of cybersecurity.

### **The Nature of Modern Cyber Threats**

Cyber threats have evolved into complex, interconnected challenges that demand far more than a purely technical response.

- Cybersecurity problems are no longer just technical glitches.
- Attacks now intersect with human behavior, business decisions, legal requirements, and global politics.
- No single discipline can fully address threats that span technology, privacy, economics, and national security.

### **Why We Teach Cybersecurity Through Many Lenses**

Because today's threats span people, organizations, and nations, students need insight from multiple fields to fully understand how attacks happen—and how to prevent them.

**Technology & Computer Science:** Build and secure the systems that run our world.

**Business & Risk Management:** Understand financial impact, risk, and organizational decision-making.

**Humanities & Social Sciences:** Explore ethics, psychology, communication, and human factors that drive real-world vulnerabilities.

**Law & Government:** Navigate regulations, digital rights, and the growing role of government in protecting critical infrastructure.

### The Result for Students

This interdisciplinary foundation equips students with a broader, more agile way of thinking that directly translates to real-world capability.

- ODU Graduates can analyze problems from multiple angles rather than relying on a single technical answer.
- As a future professional, you will collaborate across teams—IT, policy, leadership, and operations—to create resilient, practical solutions.
- You will have skills that remain adaptable in a constantly evolving field where the next challenge may be technical, legal, ethical, or global.

### Undergraduate Programs

ODU offers multiple undergraduate pathways in cybersecurity designed to meet a wide range of student interests—technical, managerial, operational, and interdisciplinary. These majors, as well as the Cybersecurity minor, emphasize practical skill development, emerging threat awareness, and workforce readiness.

- [B.S. Cybersecurity](#)
- [B.S. Cyber Operations](#)
- [B.S. Cyber Risk Management](#)
- [B.S. AI for Cybersecurity](#)
- [Cybersecurity Interdisciplinary Minor](#)

For current degree requirements, sample four-year plans, and course lists, visit our [Program Description Page](#).

Need sample 4 year plans - From website

## Available Cybersecurity Courses

The School of Cybersecurity offers over 30 courses designed to prepare students for a dynamic, in-demand, and rapidly changing field. Courses range from introductory concepts to the application of Machine Learning and Artificial Intelligence, to Cyber Warfare. For a complete listing of available courses please refer to the [School of Cybersecurity Undergraduate Catalog Course Listing](#).

## Graduation Requirements

Successful completion of 120 credit hours is required to complete your degree. These credit hours are divided into the following categories.

Category	# Courses	Hours
<b>General Education</b>	18	53
<b>Core Cybersecurity Courses</b>	8	24
<b>Principle Cybersecurity Courses</b>	3	9
<b>Application Cybersecurity Courses</b>	3	9
<b>Capstone Courses, including internship</b>	2	6
<b>General Electives (Your choice)</b>	6 – 7	19

Refer to the [School of Cybersecurity Program Requirements](#) page for an UpToDate list of current course offerings and categories.

## Linked & Accelerated Programs

High-performing undergraduates may apply to a linked BS-to-MS program, allowing students to complete graduate-level coursework while finishing their bachelor's degree. This pathway reduces both time and tuition cost toward a master's degree. Full details on eligibility, application timelines, and program options can be found on the [Linked Programs Page](#).

## Admissions Overview

Students interested in joining the cybersecurity undergraduate program should follow the university's standard admissions process, which includes meeting academic requirements, submitting transcripts, and completing application components through the ODU Undergraduate Admissions office. For the most current undergraduate admissions requirement visit [ODU's General Admissions Page](#).

## Student Resources

The school provides extensive support services including tutoring, student organizations, career readiness workshops, cybersecurity competitions, and professional development events. Resources are updated throughout the year; refer to the [Student Resources Page](#) for a complete list of available opportunities for ODU Cybersecurity Majors.

## Career Pathways

Cyber career pathways help students understand how the cybersecurity workforce is structured and how to enter and move within it. The pathways below show...

- How roles relate, overlap, and progress
- Identify the skills, competencies, and tasks tied to each job family
- Link academic preparation to workforce expectations
- Support informed decision-making about specialization and advancement
- Provide a common language used by universities, industry, and government

Together, these pathway resources give learners a clear, scalable view of where they can begin, how they can grow, and what expertise the modern cyber workforce demands.

Here are a few popular career pathways students can use to provide general guidance on fields of interest.

### [ODU School of Cybersecurity Career Pathways](#)

A guide showing how cybersecurity roles connect to real-world skills and your academic plan.

- Highlights industry-aligned job families
- Links coursework to employability
- Clarifies steps from classroom to career

### [CISA Cyber Career Pathways Tool](#)

A national map of how cybersecurity roles relate, evolve, and build on shared competencies.

- Visualizes role progression across specialties
- Identifies required skills and tasks
- Supports exploration using federal workforce data

### [NIST NICE Framework](#)

A standardized model defining cybersecurity work across government, industry, and education.

- Establishes a common language for roles and skills
- Breaks down tasks, knowledge, and competencies

- Helps align learning to professional expectations

### [DoD Cyber Workforce Pathways](#)

A mission-focused roadmap describing career options within the Department of Defense cyber workforce.

- Outlines specialized military and civilian roles
- Shows advancement routes across mission areas
- Clarifies how DoD cyber careers differ from industry paths

### **Academic Advising**

Advising ensures students stay on track for graduation, understand prerequisites, and plan for internships or accelerated programs. Advisors assist with academic planning, course selection, and university navigation. For advisor contacts and scheduling:

<https://www.odu.edu/cyber/student-opportunities>

If you have questions related to academic advising, or are not sure who your advisor is, please reach out to [IDSchoolsAdvising@odu.edu](mailto:IDSchoolsAdvising@odu.edu).

### **Experiential Learning**

Internships are strongly encouraged and often required depending on the degree track. The school partners with regional employers, defense organizations, and private-sector companies to provide students with hands-on cybersecurity experience. Up-to-date internship guidance visit the [ODU School of Cybersecurity Internship Page](#).

### **Internships**

### **Cybersecurity Competitions**

### **Student run SOC**

### **Study Abroad Opportunities**

The School of Cybersecurity encourages students to broaden their perspective through international study that strengthens both technical ability and cultural awareness.

As part of the BS in Cybersecurity, students are required to complete **19 credit hours of electives**, and these credits may be fulfilled through approved coursework taken at one of ODU's partner universities abroad. ODU's bilateral exchange programs allow cybersecurity

majors to spend a semester or full academic year abroad while *paying standard ODU tuition and retaining eligibility for financial aid.*

Students can complete cybersecurity, computer science, or elective coursework at partner universities in Australia, the United Kingdom, Ireland, South Korea, and Japan. These programs give future cybersecurity professionals exposure to global infrastructures, diverse threat landscapes, and international collaboration—key competencies in an increasingly interconnected security environment.

For the most current program details, students should visit [ODU's Office of Study Abroad](#).

### **Third-Party Certification for Credit**

Students may earn academic credit, up to six hours, for select industry certifications, allowing them to accelerate progress toward their degree while building workforce-relevant credentials. Accepted certifications and submission procedures are maintained online at the [ODU Third Party Certification for Credit Program](#).

### **Computer Hardware Requirements**

- If budget allows, 16 GB RAM + 512 GB SSD
- Acceptable minimum: 8 GB RAM + 256 GB SSD
- Avoid ultra-budget models with 4 GB RAM and <128 GB storage
- Other Considerations: Good battery life – 8 hours preferred, portability (weight)

### **Contact Information**

School of Cybersecurity  
Old Dominion University  
Constant Hall, Norfolk, VA 23529  
Phone: 757-683-XXXX  
Email: [cyber@odu.edu](mailto:cyber@odu.edu)

This page is kept current at [https://www.odu.edu/cyber/Undergraduate\\_Handbook](https://www.odu.edu/cyber/Undergraduate_Handbook)