Cybersecurity (BS)

Students may be admitted to the major after consultation with an adviser in the Department of Computer Science or with an advisor in Tykeson Hall. Students should seek admission to this major early in their career at the university as the requirements have a number of course dependencies.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Learn essential knowledge and up-to-date techniques in cybersecurity, including those in the main areas of fundamental security concepts and principles, applied cryptography, program security, and system and network security.
- Hone hands-on skills in cybersecurity via computer and network security lab courses and field studies.
- Be able to draw on a broad knowledge and hands-on skills of cybersecurity to design, implement, and test solutions to cybersecurity tasks.
- Understand the wide-ranging effects and interdisciplinary aspects of cybersecurity while attaining proficiency in one or multiple subdomains within the field of cybersecurity.
- Apply and expand foundational knowledge and skills to new problem domains and emerging technologies.
- Possess effective communication and collaboration abilities and express ideas clearly and concisely both orally and in written form.
- Adhere to ethical principles and make well-informed decisions in the field of cybersecurity.

Cybersecurity Major Requirements

Code	Title	Credits
Stage 1	**All courses must be taken graded.**	
CS 102	Fundamentals of Computer and Information Security	4
CS 210	Computer Science I	4
CS 211	Computer Science II	4
CS 212	Computer Science III	4
MATH 231	Elements of Discrete Mathematics I	4
MATH 232	Elements of Discrete Mathematics II	4
Stage 2	**All courses must be taken graded except for 332.**	
CS 313	Intermediate Data Structures	4
CS 314	Computer Organization	4
CS 315	Intermediate Algorithms	4
CS 330	C/C++ and Unix	4
CS 332	(System and Security Administration Lab) to be submitted for approval soon	4
CS 333	Applied Cryptography	4
Stage 3	**All courses must be taken graded except for 437.**	
CS 415	Operating Systems	4
CS 422	Software Methodology I	4
CS 425	Principles of Programming Languages	4
CS 432	Introduction to Networks	4
CS 433	Computer and Network Security	4
CS 437	(Computer and Network Security Practicum) to be submitted for approval soon	4
Stage-3 depth courses		**8**
CS 434	Computer and Network Security II	
CS 436	Secure Software Development	
J 431	Media Structures and Regulation: [Topic] (Computer Crime Law)	
Breadth Courses	**A maximum of 8 credits may be taken Pass/No Pass.**	**16**
Any additional stage-3 depth courses		
Any 400-level CS courses and 399		
A maximum number of 8 credits from courses 399, 400M, and 410 may be counted toward the degree		
A maximum number of 8 credits from 403 may be counted toward the degree		
A maximum number of 4 credits from courses 405 and 407 may be counted toward the degree		
CIS 405, 407, 399, 410 repeatable only with different subtitles		
Writing Requirement: one of the two	**The course may be taken Pass/No Pass or Graded.**	**4**
WR 320	Scientific and Technical Writing	
WR 321	Business Communications	
Field Study	**Over one or multiple terms with totally four (4) credits. The course may be taken Pass/No Pass or Graded.**	**4**
CS 401	Research: [Topic]	
CS 404	Internship: [Topic]	
CS 406	Practicum: [Topic]	
Total Credits		**104**

24 credits from the Computer Science department must be earned in residence at the University of Oregon.