CYBERSECURITY (B.S.)

Required course work includes the university requirements (see regulation J-3 (https://catalog.uidaho.edu/general-requirements-academic-procedures/j-general-requirements-baccalaureate-degrees/)) and:

Code	Title	Hours
COMM 101	Fundamentals of Oral Communication	3
CYB 110	Cybersecurity and Privacy	3
CYB 210	Cybersecurity Architectures and Management	3
CYB 220	Secure Coding and Analysis	3
CYB 310	Cybersecurity Technical Foundations	3
CYB 330	Networking Fundamentals	3
CYB 340	Network Defense	3
CYB 350	Operating System Defense	3
CYB 380	Cybersecurity Lab I	3
CYB 381	Cybersecurity Lab II	3
CYB 401	Cybersecurity as a Profession	1
CYB 420	Digital Forensics	3
CYB 440	Software Vulnerability Analysis	3
CYB 480	Cybersecurity Senior Capstone Design I	3
CYB 481	Cybersecurity Senior Capstone Design II	3
CS 112 or CS 212 or ENGR 212	Computational Thinking and Problem Solving Practical Python Python Programming Essentials	3
CS 120	Computer Science I	4
CS 121	Computer Science II	3
CS 150	Computer Organization and Architecture	3
CS 240	Computer Operating Systems	3
CS 270	System Software	3
CS 383	Software Engineering	4
ENGL 317	Technical Writing II	3
MATH 160 or MATH 170	Survey of Calculus Calculus I	4
MATH 176	Discrete Mathematics	3
PHIL 103 or PHIL 208	Introduction to Ethics Business Ethics	3
STAT 251 or STAT 301	Statistical Methods Probability and Statistics	3
Total Hours		**82**

Courses to total 120 credits for this degree

Fall Term 1		**Hours**
CYB 110	Cybersecurity and Privacy	3
CS 112 or CS 212 or ENGR 212	Computational Thinking and Problem Solving or Practical Python or Python Programming Essentials	3
MATH 143	College Algebra	3
ENGL 101	Writing and Rhetoric I	3
PHIL 103 or PHIL 208	Introduction to Ethics or Business Ethics	3
	Hours	**15**
Spring Term 1		
CS 120	Computer Science I	4
MATH 176	Discrete Mathematics	3
COMM 101	Fundamentals of Oral Communication	3
ENGL 102	Writing and Rhetoric II	3
Scientific Ways of Knowing Course		4
	Hours	**17**
Fall Term 2		
CS 121	Computer Science II	3
CS 150	Computer Organization and Architecture	3
CYB 210	Cybersecurity Architectures and Management	3
Humanistic and Artistic Ways of Knowing Course		3
MATH 160 OR MATH 170		3
	Hours	**15**
Spring Term 2		
CS 240	Computer Operating Systems	3
CS 270	System Software	3
CYB 220	Secure Coding and Analysis	3
Scientific Ways of Knowing Course		4
STAT 251 OR STAT 301		3
	Hours	**16**
Fall Term 3		
CYB 310	Cybersecurity Technical Foundations	3
CYB 330	Networking Fundamentals	3
CYB 380	Cybersecurity Lab I	3
ENGL 317	Technical Writing II	3
Social and Behavioral Ways of Knowing Course		3
	Hours	**15**
Spring Term 3		
CS 383	Software Engineering	4
CYB 340	Network Defense	3
CYB 350	Operating System Defense	3
CYB 381	Cybersecurity Lab II	3
American Diversity Course		3
	Hours	**16**
Fall Term 4		
CYB 401	Cybersecurity as a Profession	1
CYB 420	Digital Forensics	3
CYB 480	Cybersecurity Senior Capstone Design I	3
Social and Behavioral Ways of Knowing Course		3
Elective Course		3
	Hours	**13**
Spring Term 4		
CYB 440	Software Vulnerability Analysis	3
CYB 481	Cybersecurity Senior Capstone Design II	3
International Course		3
Elective Course		3
Elective Course		1
	Hours	**13**
	Total Hours	**120**

The degree map is a guide for the timely completion of your curricular requirements. Your academic advisor or department may be contacted for assistance in interpreting this map. This map is not reflective of your academic history or transcript and it is not official notification of completion of degree or certificate requirements. Please contact the Registrar's Office regarding your official degree/certificate completion status.

Graduates of the program will have an ability to:

1. Analyze a complex computing and information management problems and to apply principles of cybersecurity, and other relevant disciplines to identify solutions.

2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of cyber security.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to cybersecurity.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.