جامعة الفيصل
Alfaisal University

BS in Cybersecurity Program

Alfaisal University, College of Engineering & Advanced Computing

Effective: Fall 2025

Approved: April 2025

Curriculum Structure and Study Plan

The Cybersecurity curriculum is composed of **132** Credit Hours (CRHs) divided as follows:

I. General Education Requirements (43 CRHs)
1. Mathematics & Statistics (21 CRHs)
2. Basic Sciences (8 CRHs)
3. Humanities (14 CRHs)

II. Core Requirements (89 CRHs)
1. Software Engineering Courses (79 CRHs)
2. College of Engineering & Advanced Computing Courses (4 CRHs)
3. Technical Electives (6 CRHs)
4. Summer Internship (0 CRHs)

I. General Education Requirements (43 CRHs)

1. Mathematics & Statistics (21 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect.	Lab	Tut		
MAT 101	Calculus I	3	3	0	1		
MAT 112	Calculus II	3	3	0	0	MAT 101	
MAT 211	Calculus III	3	3	0	0	MAT 112	
MAT 212	Linear Algebra	3	3	0	0	MAT 112	
MAT 213	Differential Equations	3	3	0	0	MAT 112	
MAT 224	Numerical Methods	3	3	0	0	MAT 112	
STA 212	Probability and Statistics for Engineers	3	3	0	0	MAT 112	

2. Basic Sciences (8 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect	Lab	Tut		
PHU 103	Mechanics and Waves for Engineers	3	3	0	1		MAT 101, PHU 103L
PHU 103 L	Mechanics and Waves for Engineers Lab	1	0	2	0		PHU 103
PHU 124	Electromagnetism and Optics for Engineers	3	3	0	1	PHU 103	PHU 124L
PHU 124 L	Electromagnetism and Optics for Engineers Lab	1	0	2	0		PHU 124

3. Humanities (14 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect	Lab	Tut		
ENG 101	University Writing	3	3	0	0		
ENG 222	Technical Writing	3	3	0	0	ENG 101	
ISL 101	Islamic Studies I	2	2	0	0		
ARB 101	Arabic Language and Literature I	2	2	0	0		
GE _ _ _	General Education Elective I	2	2	0	0		
GE _ _ _	General Education Elective II	2	2	0	0		

II. Core Requirements (91 CRHs)

1. Software Engineering Courses (81 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect	Lab	Tut		
SE 100	Programming for Engineers	3	3	0	0		SE 100L
SE 100 L	Programming for Engineers Lab	1	0	2	0		SE 100
SE 120	Object-Oriented Programming I	3	3	0	0	SE 100	SE 120L
SE 120 L	Object-Oriented Programming I Lab	1	0	2	0		SE 120
SE 151	Discrete Mathematics	3	3	0	0	SE 100	
DSE 200	Introduction to Data Science	3	3	0	0	SE 120	STA 212
SE 201	Introduction to Software Engineering	3	3	0	0	SE 120	
AI 213	Introduction to Artificial Intelligence	3	3	0	0	SE 215	
SE 215	Data Structures	3	3	0	0	SE 120	SE 215L
SE 215 L	Data Structures Lab	1	0	2	0		SE 215
CSE 230	Programming in C	3	3	0	0	SE 120	CSE 230L
CSE 230 L	Programming in C Lab	1	0	2	0		CSE 230
SE 239	Computer Networks	3	3	0	0		EE 210
SE 252	Database Management Systems	3	3	0	0	SE 215	SE 252L
SE 252 L	Database Management Systems Lab	1	0	2	0		SE 252
SE 254	Operating Systems	3	3	0	0	SE 215	SE 254L
SE 254 L	Operating Systems Lab	1	0	2	0		SE 254
CSE 310	Linux System Administration	3	3	0	0	SE 254, CSE 230	
CSE 312	Computer Architecture	3	3	0	0	EE 210	

CSE 330	Introduction to Cybersecurity	3	3	0	0	SE 239	SE 254
CSE 350	Cryptography and Data Privacy	3	3	0	0	CSE 330, STA 212	
CSE 360	Digital Forensics	3	3	0	0	SE 254, CSE 330	
CSE 370	Database Security	3	3	0	0	SE 252, CSE 330	
CSE 380	Operating System Security	3	3	0	0	SE 254, CSE 330	
SE 400	Theory of Computation	3	3	0	0	SE 151, CSE 350	
CSE 410	Security Architecture	3	3	0	0	SE 201, CSE 330	
CSE 442	Network Security	3	3	0	0	CSE 350	
CSE 443	Cybersecurity Risk Management and Control	3	3	0	0	CSE 330, STA 212	
SE 481	Ethical and Professional Development	1	1	0	0	CSE 495	
CSE 495	Capstone Project I	3	0	6	0	CSE 350, CSE 360, CSE 370, CSE 380	
CSE 496	Capstone Project II	3	0	6	0	CSE 495	

2. College of Engineering & Advanced Computing Courses (4 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect	Lab	Tut		
EE 210	Digital Logic Design	3	0	0	0	PHU 124	EE 210L
EE 210 L	Digital Logic Design Lab	1	0	2	0		EE 210

3. Technical Electives (6 CRHs)

Select from the following courses:

Course Code	Course-Title	Credit Hours (CRHs)				Pre-Requisite Course Code	Co-Requisite Course Code
		Total-CRHs	Lect	Lab	Tut		
CSE 444	Technical Elective 1 (Web and mobile security)	3	3	0	0	SE 252, CSE 330	
CSE 451	Technical Elective 4 (Secure Software Engineering)	3	3	0	0	CSE 410	
CSE 454	Technical Elective 3 (Ethical hacking)	3	3	0	0	CSE 442	
CSE 472	Technical Elective 2 (Penetration Testing)	3	3	0	0	CSE 442	

4. Summer Internship (0 CRHs)

Course Code	Course-Title	Credit Hours (CRHs)	Pre-Requisite Course Code	Co-Requisite Course Code
CSE 390	Software Engineering Summer Internship	0	Department approval	

Typical Study Plan-Cybersecurity Program

4-Year Curriculum: ***132 Credit Hours Total***

Each course below follows the following format:
Course code, Course Title, and Course Credit Hours (Lecture contact hours – Lab contact hours – Tutorial contact hours)

1st Year			
Fall	Course Code	Course-Title	CRHs
	SE 100	**Programming for Engineers**	**3 (3-0-0)**
	SE 100 L	**Programming for Engineers Lab**	**1 (0-2-0)**
	MAT 101	**Calculus I**	**3 (3-0-2)**
	PHU 103	**Mechanics and Waves for Engineers**	**3 (3-0-1)**
	PHU 103 L	**Mechanics and Waves for Engineers Lab**	**1 (0-2-0)**
	ENG 101	**University Writing**	**3 (3-0-0)**
	ISL 101	**Islamic Studies I**	**2 (2-0-0)**
	ARB 101	**Arabic Language and Literature I**	**2 (2-0-0)**
		Total	**18**
Spring	Course Code	Course-Title	CRHs
	SE 120	**Object-Oriented Programming I**	**3 (3-0-0)**
	SE 120 L	**Object-Oriented Programming I Lab**	**1 (0-2-0)**
	SE 151	**Discrete Mathematics**	**3 (3-0-0)**
	MAT 112	**Calculus II**	**3 (3-0-2)**
	PHU 124	**Electromagnetism and Optics for Engineers**	**3 (3-0-1)**
	PHU 124 L	**Electromagnetism and Optics for Engineers Lab**	**1 (0-2-0)**
	ENG 222	**Technical Writing**	**3 (3-0-0)**
		Total	**17**

2nd Year			
Fall	Course Code	Course-Title	CRHs
	SE 215	**Data Structures**	**3 (3-0-0)**
	SE 215 L	**Data Structures Lab**	**1 (0-2-0)**
	CSE 230	**Programming in C**	**3 (3-0-0)**
	CSE 230 L	**Programming in C Lab**	**1 (0-2-0)**
	SE 239	**Computer Networks**	**3 (3-0-0)**
	EE 210	**Digital Logic Design**	**3 (3-0-0)**
	EE 210 L	**Digital Logic Design Lab**	**1 (0-2-0)**
	STA 212	**Probability and Statistics**	**3 (3-0-0)**
		Total	**18**
Spring	Course Code	Course-Title	CRHs
	SE 252	**Database Management Systems**	**3 (3-0-0)**
	SE 252 L	**Database Management Systems Lab**	**1 (0-2-0)**
	SE 254	**Operating Systems**	**3 (3-0-0)**
	SE 254 L	**Operating Systems Lab**	**1 (0-2-0)**
	DSE 200	**Introduction to Data Science**	**3 (3-0-0)**
	AI 213	**Introduction to Artificial Intelligence**	**3 (3-0-0)**
	CSE 330	**Introduction to Cybersecurity**	**3 (3-0-0)**
		Total	**17**

3rd Year			
Fall	Course Code	Course-Title	CRHs
	SE 201	**Introduction to Software Engineering**	**3 (3-0-0)**
	CSE 310	**Linux System Administration**	**3 (3-0-0)**
	CSE 312	**Computer Architecture**	**3 (3-0-0)**
	MAT 211	**Calculus III**	**3 (3-0-0)**
	MAT 212	**Linear Algebra**	**3 (3-0-0)**
	MAT 224	**Numerical Methods**	**3 (3-0-0)**
		Total	**18**
Spring	Course Code	Course-Title	CRHs
	CSE 350	**Cryptography and Data Privacy**	**3 (3-0-0)**
	CSE 360	**Digital Forensics**	**3 (3-0-0)**
	CSE 370	**Database Security**	**3 (3-0-0)**
	CSE 380	**Operating System Security**	**3 (3-0-0)**
	MAT 213	**Differential Equations**	**3 (3-0-0)**
			15

Summer	Course Code	Course-Title	CRHs
	CSE 390	**Internship**	**0**
		Total	**0**

4th Year			
Fall	Course Code	Course-Title	CRHs
	SE 400	**Theory of Computation**	**3 (3-0-0)**
	CSE 410	**Security Architecture**	**3 (3-0-0)**
	CSE 442	**Network Security**	**3 (3-0-0)**
	SE 495	**Software Engineering Capstone Project I**	**3 (0-6-0)**
	GE _ _ _	**General Education Elective I**	**2 (2-0-0)**
		Total	**14**
Spring	Course Code	Course-Title	CRHs
	CSE 443	**Cybersecurity Risk Management and Control**	**3 (3-0-0)**
	CSE 4_ _	**Technical Elective 1**	**3 (3-0-0)**
	CSE 4_ _	**Technical Elective 2**	**3 (3-0-0)**
	SE 481	**Ethical and Professional Development**	**1 (3-0-0)**
	CSE 496	**Software Engineering Capstone Project II**	**3 (0-6-0)**
	GE _ _ _	**General Education Elective II**	**2 (2-0-0)**
		Total	**15**

Course Descriptions

In this section, we give brief descriptions of courses in the Cybersecurity program. Each course below follows the following format:

Course code: Course Title Course credit hours (Lecture contact hours – Lab contact hours – Tutorial contact hours)

Course Description

Prerequisite(s)

Co-requisites

Core Courses

SE 100: Programming for Engineers 3 (3-0-0)

The course introduces the students to basic notions of computers and computing and then introduces them to programming starting from abstract ways like flowcharts and pseudocode and finally using a typical programming language. The students will be introduced to the basic concepts of data types and structures, operators, and the different ways of data storage, manipulation, and representation.
Emphasis is on problem-solving and structured program design methodologies.
Prerequisite(s): None
Co-requisites: SE 100L

SE 100 L: Programming for Engineers Lab 1 (0-2-0)

This course constitutes the lab component of the Programming for Engineer course (SE 100). The purpose of this lab is to provide hands-on training on programming concepts, technologies and techniques introduced during lectures.
Prerequisite(s): None
Co-requisites: SE 100

SE 120: Object-Oriented Programming I 3 (3-0-0)

After completing this course, students will be equipped with the necessary skills and tools to write programs in Java based on a procedural and object-oriented approach. Topics of focus will include basic Java programming, conditional statements, strings, iteration, methods, arrays, creating classes, encapsulation, inheritance and polymorphism, abstract classes, packages, principles of object-oriented design, as well as exceptions and interfaces.
Prerequisite(s): SE 100
Co-requisites: SE 120L

SE 120 L: Object-Oriented Programming I Lab 1 (0-2-0)

This course constitutes the lab component of the Object-Oriented Programming I course (SE 120). The purpose of this lab is to provide hands-on training on the basics of Java and advanced object-oriented programming. Topics covered include data types and operators, logical expressions, control structures, methods, arrays, inheritance; polymorphism; abstract classes and interfaces. be covered.
Prerequisite(s): None
Co-requisites: SE 120

SE 151: Discrete Structures for Software Engineers **3 (3-0-0)**
This course covers the mathematical elements of computer science including formal logic, propositional logic, predicate logic, logic in mathematics, sets, functions and relations, recursive thinking, mathematical induction, counting, combinatorics, algorithms, matrices, graphs, trees, and Boolean logic. Students will learn to recognize and express mathematical ideas graphically, numerically, symbolically, and in writing.
Prerequisite(s): SE 100

SE 201: Introduction to Software Engineering **3 (3-0-0)**
This course is designed to present students with several principles relevant to Software Engineering. Students will gain insights into various software process models throughout the course. The curriculum strongly emphasizes the agile software development approach, highlighting the importance of adaptability and collaborative teamwork. Students will acquire knowledge and skills in requirements engineering. The course covers systems modeling and project management strategies. It addresses the value of software reuse and introduces students to human computer interaction and software testing. The final segment of the course focuses on configuration management.
Prerequisite(s): SE 120

AI 213: Introduction to Artificial Intelligence **3 (3-0-0)**
This course introduces students to the fundamental concepts, techniques, and tools used in artificial intelligence (AI). Topics include perception, reasoning, learning, and search algorithms (informed and uninformed). Students will gain skills in applying AI techniques to real-world problems.
Prerequisite(s): SE 215

SE 215: Algorithms and Data Structures **3 (3-0-0)**
The course involves the study of important data structures and sorting methods commonly encountered in object-oriented software engineering. It covers the design, performance analysis, and implementation of the related algorithms, stressing their practical use and performance.
Prerequisite(s): SE 120
Co-requisites: SE 215L

SE 215 L: Algorithms and Data Structures Lab **1 (0-2-0)**
Survey of important computer algorithms and related data structures used in object-oriented software engineering. Design, performance analysis and implementation of such algorithms, stressing their practical use and performance certification of large software applications. Understand how to "seal" designs to guarantee performance goals and ensure that all error conditions are caught. Laboratory experiments dealing with Algorithms and Data Structures.
Prerequisite(s): None
Co-requisites: SE 215

SE 239: Computer Networks **3 (3-0-0)**
The course teaches the fundamental concepts of communication networks and is concerned specifically with network architectures and protocols. The objective of the course is to allow students to develop a thorough understanding of the architectures of networks and the basic principles and protocols that allow the transmission of data over networks.
Prerequisite(s): None?
Co-requisites: EE 210

SE 252: Database Management Systems **3 (3-0-0)**
The focus is to teach database fundamentals required in the development and evolution of most software applications by providing a basic introduction to the principles of relational database management systems such as Entity-Relationship approach to data modeling, relational model of database management systems and the use of query languages.
Prerequisite(s): SE 215
Co-requisites: SE 252 L

SE 252 L: Database Management Systems Lab **1 (0-2-0)**
Laboratory experiments dealing with database management systems.
Prerequisite(s): None
Co-requisites: SE 252

SE 254: Operating Systems **3 (3-0-0)**
Theory and construction of operating systems, including real-time and embedded systems aspect from an engineering point of view, stressing performance measurement and metrics. Quality of Service issues leading to certification that an operating system will satisfy hard real-time constraints.
Prerequisite(s): SE 215
Co-requisites: SE 254 L

SE 254 L: Operating Systems Lab **1 (0-2-0)**
Laboratory experiments dealing with Operating Systems.
Prerequisite(s): None
Co-requisites: SE 254

CSE 310: Linux System Administration **3 (3-0-0)**
This course lays a strong foundation in managing Linux-based systems within professional, security conscious environments. Students learn to configure and optimize key services, administer file systems and user accounts, and automate tasks with scripting. Beyond the basics, the course covers advanced security mechanisms such as SELinux, AppArmor, and mandatory access controls to mitigate threats. Students also explore containerization (e.g., Docker, Podman), virtualization techniques, and system monitoring tools to ensure performance and compliance with security policies. By the end of the course, students will be equipped to maintain resilient, efficient, and secure Linux infrastructures in dynamic organizational settings.
Prerequisite(s): SE 254, CSE 230

CSE 312: Computer Architecture **3 (3-0-0)**
Students will learn the low-level design of a computer. Topics will include cache hierarchies, main memory layout, addressing schemes, virtual memory, virtualization, data storage, accelerators, etc. They will conduct experiments simulating multi-threading and multi-core processing.
Prerequisite(s): EE 210

CSE 330: Introduction to Cybersecurity **3 (3-0-0)**

This course provides an overview of core cybersecurity concepts, emphasizing the fundamental principles, tools, and procedures used to secure information systems. Students will employ the CIA triad as a guiding framework, explore prevalent threats, and examine various information security solutions. The course focuses on security and risk management, business impact analysis (BIA), asset security, vulnerabilities, threats and countermeasures, identity and authentication management, incident response and BCP/DRP, as well as key compliance and regulatory issues. By the end of the course, students will have broad, practical knowledge of cybersecurity, including the ability to identify security risks, implement effective defensive measures, and approach cybersecurity challenges with strategic thinking. Computer Networks and Operating Systems are prerequisites for this course.

Prerequisite(s): SE 239

Co-requisites: SE 254

CSE 350: Cryptography and Data Privacy **3 (3-0-0)**

This course offers a comprehensive introduction to the mathematical foundations, fundamental primitives, and modern techniques of cryptography, as well as the essential principles of data privacy. Students will learn both symmetric and asymmetric encryption, hashing, digital signatures, message authentication codes (MAC), and other critical tools for protecting data and ensuring privacy, while simultaneously developing the necessary mathematical background in number theory and algebraic structures. The course also explores modern cryptographic schemes—such as zero-knowledge proofs and homomorphic encryption—and examines their applications in current research areas. Additionally, students will study privacy-preserving methodologies, learning how to apply cryptographic techniques to safeguard sensitive information and maintain user privacy. By the end of the course, students will possess a solid understanding of cryptography and privacy theory, enabling them to apply these concepts in real-world contexts and research. Introduction to Probability and Statistics and Introduction to Cybersecurity are prerequisites for this course.

Prerequisite(s): CSE 330, STA 212

CSE 360: Digital Forensics **3 (3-0-0)**

This course introduces students to the core principles and practices involved in investigating digital assets (e.g., mobile phones, laptops, workstations) and cyber incidents. By examining methods for collecting, preserving, analysing, and presenting digital evidence, students will gain a practical understanding of forensic tools and techniques (e.g., FTK Imager, Autopsy, EnCase). Topics include chain of custody, evidence handling, imaging, file system analysis, investigations, and the use of industry-standard forensic software. Upon completing this course, students will be better prepared to conduct thorough, methodical examinations of digital devices and networks in support of security investigations.

Prerequisite(s): SE 254, CSE 330

CSE 370: Database Security **3 (3-0-0)**

This course focuses on safeguarding data at rest and in transit within various database environments. Students explore the principles of secure database design, learn to implement robust access controls, and detect and mitigate threats such as SQL injection. The curriculum covers secure database architectures, hardened configurations, and DevOps integration for continuous security testing and validation. Students also analyze case studies of large-scale data breaches to understand evolving threat patterns and compliance obligations. By the end of the course, participants will have the foundational skills required to maintain data integrity, confidentiality, and availability in diverse database systems.

Prerequisite(s): SE 252, CSE 330

CSE 380: Operating System Security **3 (3-0-0)**

In this course, students explore how operating systems manage resources, enforce security policies, and prevent unauthorized activity. Through hands-on exercises, they learn about file permissions, authentication mechanisms, secure configuration, patch management, and system hardening. By examining both traditional and emerging operating systems, students gain the skills to identify vulnerabilities and implement measures that strengthen a system's defenses against internal and external threats.

Prerequisite(s): SE 254, CSE 330

CSE 390: Software Engineering Summer Internship **(0 CRHs)**

An internship is an important aspect of the Cybersecurity Engineering curriculum that provides the student with hands-on experience and a good sense of what an actual job in an organization will be like. Students are required to join an IT department in a government or private organization for a summer period of at least 8 weeks in the last summer prior to student graduation. Students should be able to relate the internship experience to the knowledge that he or she has gained through the CSE program courses.

Prerequisite(s): Department approval

SE 400: Theory of Computation **3 (3-0-0)**

This course introduces fundamental concepts in the theory of computation. Students will be introduced to formal languages, automata, computability and computational complexity. These include finite automatons, Turing machines, grammars, decidable problems, reductive procedures and different kinds of computational problems. The course aims to explore these theoretical concepts to apply on practical issues of interest to software engineering, data science, and AI, for instance, natural language processing, algorithmic development and evaluation of computational efficiency. By the end of this course, students will be able to assess the performance bounds of computing models and their applicability towards modern computing problems.

Prerequisite(s): SE 151, CSE 350

CSE 410: Security Architecture **3 (3-0-0)**

This course provides a comprehensive overview of designing and evaluating robust security architectures within enterprise environments. Students move beyond foundational concepts to explore layered defense models, identity and access management frameworks, and Zero Trust Network Access (ZTNA). Topics include integrating cryptographic controls, establishing secure communication channels, leveraging threat intelligence, and applying architecture frameworks such as SABSA or TOGAF. Students will also assess emerging technologies and evolving regulatory requirements to ensure that architectures remain adaptive and forward-looking. Upon completion, they will be able to create strategic, standards-based security designs that protect complex systems against diverse threats.

Prerequisite(s): SE 201, CSE 330

CSE 442: Network Security **3 (3-0-0)**

This course explores the strategies, tools, and standards used to secure data as it traverses networks. It covers intrusion detection and prevention systems, advanced firewall orchestration, zero-trust network segmentation, and the integration of software-defined networking (SDN) security controls. Students will also work with network traffic analysis tools, threat intelligence platforms, and network forensics techniques to identify advanced persistent threats and devise mitigation strategies. By the end of the course, students will have the analytical and technical skills to implement scalable security architectures and maintain secure communication channels in dynamic, distributed networks.

Prerequisite(s): CSE 350

CSE 443: Cybersecurity Risk Management and Control **3 (3-0-0)**
This course focuses on identifying, assessing, and managing security risks within organizational settings. Students will explore frameworks such as NIST and ISO, perform both quantitative and qualitative risk analyses, prioritize mitigation measures, and ensure alignment with compliance requirements and regulatory guidelines. Topics include vendor risk management, third-party audits, continuous monitoring, cyber insurance considerations, and integrating risk metrics into strategic decision-making. By the end of the course, students will be equipped to shape security governance, effectively communicate risk to stakeholders, and foster a responsive risk management culture within organizations.
Prerequisite(s): CSE 330, STA 212

SE 481: Ethics for Engineers **1 (1-0-0)**
This course will explore the effects of technology on society. Especially the ethical questions that arise when technology interacts with humans. Topics will include secrecy of data, privacy issues, legal obligations, and protecting the society by limiting the reach of technology.
Prerequisite(s): CSE 495

CSE 495: Capstone Project I **3 (0-6-0)**
In this first part of the capstone sequence, students embark on a comprehensive, team-based project to address real-world cybersecurity engineering. The focus of this course is on problem identification, requirements analysis, and solution design. Students will define the project scope, conduct a literature review, and create a detailed project proposal. Emphasis is placed on applying knowledge from previous coursework to develop innovative and practical solutions. By the end of this course, students will have a clear roadmap for implementation of a cybersecurity engineering solution.
Prerequisite(s): CSE 350, CSE 360, CSE 370, CSE 380

CSE 496: Capstone Project II **3 (0-6-0)**
Building on the groundwork laid in CSE 495, this course focuses on implementing and completing the capstone project. Students will execute their proposed solutions. Teams will utilize industrystandard tools and techniques to develop a functional prototype or system. The course culminates with a comprehensive project report and a formal presentation to faculty and/or industry stakeholders, demonstrating the ability to tackle complex, real-world problems with data-driven strategies. Emphasis is placed on teamwork, project management, and effective communication of findings.
Prerequisite(s): CSE 495

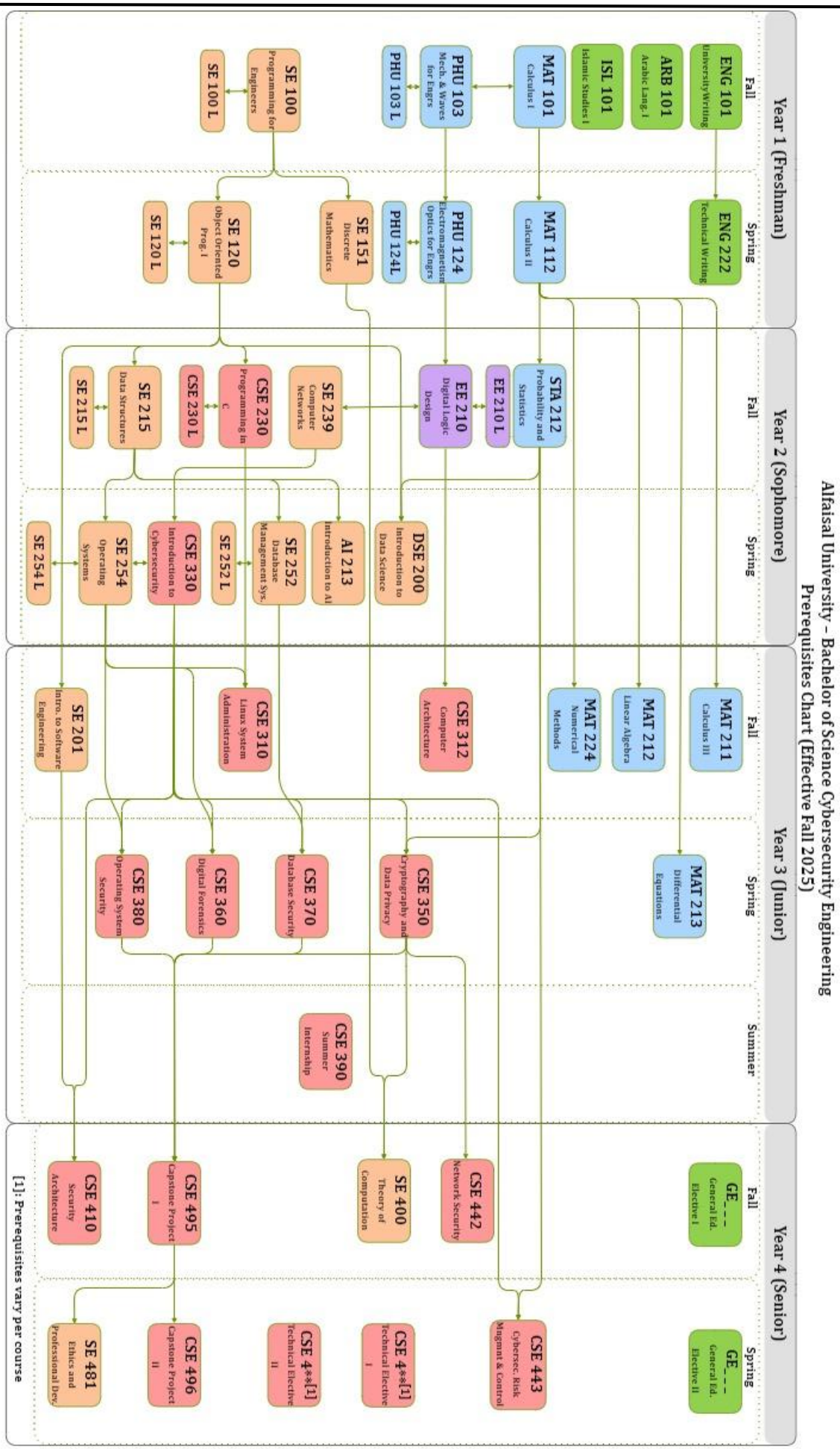
Technical Elective Courses

CSE 444: Technical Elective 1 (Web and mobile security) **3 (3-0-0)**
This course focuses on the unique security challenges associated with web applications and mobile platforms. Students examine common vulnerabilities such as cross-site scripting, broken authentication, insecure data storage, and malicious code injection. Topics extend beyond basic weaknesses to include API security, single-page application (SPA) safeguards, mobile application sandboxes, secure session management, and hardened containerized deployments. By mastering these concepts, students will be equipped to build and maintain secure web and mobile applications that protect user data and privacy across multiple platforms.
Prerequisite(s): SE 252, CSE 330

CSE 451: Technical Elective 4 (Secure Software Engineering) 3 (3-0-0)
This course focuses on building security into every phase of software development through a proactive approach. Students explore secure development lifecycles (SDLCs) and engage with industry standards such as OWASP to integrate security considerations at each stage of design and implementation. Through hands-on exercises, they learn to identify and prevent common vulnerabilities, apply threat modeling techniques, and incorporate automated security testing tools— including static and dynamic analysis— into modern CI/CD pipelines. Topics include code reviewing best practices, secure coding frameworks, application security architecture, and the practical integration of cryptographic services. By applying these practices, students gain the skills to produce resilient software that can withstand attacks while protecting user data and system integrity.
Prerequisite(s): CSE 410

CSE 454: Technical Elective 3 (Ethical hacking) 3 (3-0-0)
This course focuses on identifying, assessing, and managing security risks within organizational settings. Students will explore frameworks such as NIST and ISO, perform both quantitative and qualitative risk analyses, prioritize mitigation measures, and ensure alignment with compliance requirements and regulatory guidelines. Topics include vendor risk management, third-party audits, continuous monitoring, cyber insurance considerations, and integrating risk metrics into strategic decision-making. By the end of the course, students will be equipped to shape security governance, effectively communicate risk to stakeholders, and foster a responsive risk management culture within organizations.
Prerequisite(s): CSE 442

CSE 472: Technical Elective 2 (Penetration Testing) 3 (3-0-0)
In this hands-on course, students learn to think like attackers to identify vulnerabilities before malicious actors can exploit them. They practice reconnaissance, vulnerability scanning, exploitation techniques, and the safe use of testing tools. Ethical guidelines, scoping agreements, and reporting findings are integral parts of the curriculum. Students emerge with a structured methodology for uncovering system flaws and providing recommendations to strengthen defensive measures.
Prerequisite(s): CSE 442


Alfaisal University – Bachelor of Science Cybersecurity Engineering
Prerequisites Chart (Effective Fall 2025)
Year 1 (Freshman)
Year 2 (Sophomore)
Year 3 (Junior)
Year 4 (Senior)
Fall
Spring
Summer
ENG 101 University Writing
ARB 101 Arabic Lang. I
ISL 101 Islamic Studies I
MAT 101 Calculus I
PHU 103 Mech. & Waves for Engrs
PHU 103 L
SE 100 Programming for Engineers
SE 100 L
ENG 222 Technical Writing
MAT 112 Calculus II
PHU 124 Electromagnetism Optics for Engrs
PHU 124L
SE 151 Discrete Mathematics
SE 120 Object Oriented Prog. I
SE 120 L
STA 212 Probability and Statistics
EE 210 Digital Logic Design
EE 210 L
SE 239 Computer Networks
CSE 230 Programming in C
CSE 230 L
SE 215 Data Structures
SE 215 L
DSE 200 Introduction to Data Science
AI 213 Introduction to AI
SE 252 Database Management Sys.
SE 252 L
CSE 330 Introduction to Cybersecurity
SE 254 Operating Systems
SE 254 L
MAT 211 Calculus III
MAT 212 Linear Algebra
MAT 224 Numerical Methods
CSE 312 Computer Architecture
CSE 310 Linux System Administration
SE 201 Intro. to Software Engineering
MAT 213 Differential Equations
CSE 350 Cryptography and Data Privacy
CSE 370 Database Security
CSE 360 Digital Forensics
CSE 380 Operating System Security
CSE 390 Summer Internship
GE_ _ _ General Ed. Elective I
CSE 442 Network Security
SE 400 Theory of Computation
CSE 443 Cybersec. Risk Mngmnt & Control
CSE 4**[1] Technical Elective I
CSE 4**[1] Technical Elective II
CSE 495 Capstone Project I
CSE 410 Security Architecture
GE_ _ _ General Ed. Elective II
CSE 496 Capstone Project II
SE 481 Ethics and Professional Dev.
[1]: Prerequisites vary per course