جامعة الحسين التقنية
Al Hussein Technical University

School of Computing and Informatics
BSc in Cybersecurity

➢ **Table 1** University Requirements

Course Number	Course Name	Course Type	CH	Prerequisite(S)
0030301121	English Pre-Intermediate Intensive + Lab	HTU	4	Pre-Foundation English Elementary Intensive + Lab (0030301120)
0030301122	English Intermediate	HTU	3	English Pre-Intermediate Intensive + Lab (0030301121)
0030301123	English Upper - Intermediate	HTU	3	English Intermediate (0030301122)
0030301124	English Advanced	HTU	3	English Upper – Intermediate (0030301123)
0040302111	Professional Skills	HTU	1	
0040302211	Professional Practice	HNC	3	[Professional Skills (0040302111) or Soft Skills I (30302111)] and English Intermediate (0030301122)
0040302231	Entrepreneurship Bootcamp	HTU	4	English Upper – Intermediate (0030301123) + [Professional Practice (0040302211) or Soft Skills II (30302112)]
0030301111	Arabic Language & Communication Skills	HTU	1	Remedial Arabic Language (30301110)
0030302129	Military Science	HTU	1	
0030302232	Leadership Camp	HTU	1	Entrepreneurship Bootcamp (0030302231) or Entrepreneurship Bootcamp (0040302231)
	University Elective I	HTU	1	
	University Elective II	HTU	1	
	University Elective II	HTU	1	
	Total		**27**	

➢ **Table 2** College Requirements

Course Number	Course Name	Course Type	CH	Prerequisite(S)
0030303111	Functional Math	HTU	3	Remedial Math (0030303110)
0040303121	Maths for Computing	HNC	3	Functional Math (0030303111)
0040303130	Fundamentals of Computing	HTU	4	
0040201100	Programming	HNC	3	Fundamentals of Computing (0040303130)
0040303221	Discrete Maths	HND	3	Maths for computing (0040303121) Corequisite Data Structures & Algorithms (0040201201)
0040201290	Planning a Computing Project	HNC	4	Professional Practice (0040302211)

0030303121	STEM Lab I	HTU	1	
	Total		**21**	

- **Table 3** Department Requirements

Course Number	Course Name	Course Type	CH	Prerequisite(S)
0010203180	Networking	HNC	3	Fundamentals of Computing (0040303130)
0040201260	Website Design & Development	HNC	3	Programming (0040201100)
0040201201	Data Structures & Algorithms	HND	3	Programming (0040201100)
0000203280	Security	HNC	3	Fundamentals of Computing (0040303130)
0010203340	Cryptography	HTU	3	Discrete Maths (0040303221)
0010203210	Network Security	HND	3	Security (0000203280)
0010203361	Forensics	HND	3	Computer Organization and Design (0010203380) Security (0000203280)
0010203300	Information Security Management	HTU	3	Network Security (0010203210)
0000201391	Computing Research Project	HND	6	Planning a Computing Project (0040201290)
0010204282	Database Design & Development	HNC	3	Programming (0040201100)
0010204312	Business Intelligence	HND	3	Database Design & Development (0010204282)
0040201220	Software Development Lifecycle	HNC	3	Programming (0040201100)
0010203380	Computer Organization and Design	HTU	3	Programming (0040201100) Corequisite Discrete Maths (0040303221)
0040201341	Operating Systems	HND	3	Data Structures & Algorithms (0040201201)
0000203360	Penetration Testing	HTU	3	Network Security (0010203210)
0010203362	Ethical Hacking	HTU	3	Penetration Testing (0000203360)
0000203400	Risk Analysis & Systems Testing	HTU	3	Security (0000203280)
0000203420	Secure Coding	HTU	3	Database Design & Development (0010204282)
	Elective I	HTU	3	
	Elective II	HTU	3	
	Elective III	HTU	3	
0010203491	Capstone project I	HTU	1	>=90 hrs including core courses
0010203492	Capstone project II	HTU	2	Capstone project I (0010203491)
0010203390	HNC Training	HTU	12	Minimum number of completed hours >= 85
0010203490	HND Training	HTU	6	Pre or corequisite HNC Training (0010203390)
	Total		**87 CH**	

- **Table 4:** List of Elective Courses (9 CH):

Course Number	Course Name	Course Type	CH	Prerequisite(S)
0010203421	Web Security	HTU	3	Network Security (0010203210) Website Design & Development (0040201260)
0010203411	Internet of Things Security	HTU	3	Network Security (0010203210)
0010203410	Mobile and Wireless Security	HTU	3	Network Security (0010203210)
0010203401	Incident response management	HTU	3	Secure System Design and Development (0010203420) Risk Analysis & Systems Testing (0000203400)
0010203402	Ethical Issues in Cyber Security	HTU	3	Ethical Hacking (0010203362)
0040201450	Cloud Computing	HTU	3	Networking (0010203180) Operating Systems (0040201341)
0000204414	Data Analytics for IT Professionals	HTU	3	Business Intelligence (0010204312)
0000204456	Artificial Intelligencefor IT Professionals	HTU	3	Business Intelligence (0010204312)
0010203420	Secure System Design and Developments	HTU	3	Secure Coding (0000203420)
0010203470	Special Topics	HTU	3	Department Approval

➢ **Table 5** Course Brief Description

Course Name	Course Brief Description
Functional Math	This course reviews the fundamental concepts in numerical analysis, linear algebra, functions and graphs, differentiation, integration, and metrics. It strengthens the problem formulation skills (i.e., the ability to translate real application problems into a series of mathematical processes). It also focuses on developing the mathematical reasoning skills, such as mathematical deductions and proofs.
Maths for Computing	This course introduces students to the mathematical principles and theory that underpin the computing curriculum. Through a series of case studies, scenarios and task-based assessments students will explore number theory within a variety of scenarios; use applicable probability theory; apply geometrical and vector methodology; and finally evaluate problems concerning differential and integral calculus. Among the topics included in this course are prime number theory, sequences and series, probability theory, geometry, differential calculus and integral calculus.
Fundamentals of Computing	This course provides a comprehensive route to developing an in-depth exposure to personal computers, hardware, and a range of operating systems. Students learn the functionality of various hardware and software components and best practices in maintenance and safety issues. In addition to, basic computer skills, programming concepts, algorithms, variables and data types; arithmetic, logical, relational, Boolean, and assignment operators; simple input and output statements, selection structures, loop structures, single and multidimensional arrays, character strings, functions, data structures, input/output file operations.
Programming	Define basic algorithms to carry out an operation and outline the process of programming an application; Comparative programming language paradigms, procedural, object-orientated and event-driven programming languages. Design and tradeoffs of programming language features and implementation, including syntax, control structures, types, and security. Explain the characteristics of procedural, object-orientated and event-

	driven programming. Analyze Integrated Development Environments (IDEs); Implement basic algorithms in code using an IDE; Determine the debugging process and explain the importance of a coding standard.
Discrete Maths	This course introduces students to the discrete mathematical principles and theory that underpin software engineering. Through a series of case studies, scenarios and tasked-based assessments students will explore set theory and functions within a variety of scenarios; perform analysis using graph theory; apply Boolean algebra to applicable scenarios; and finally explore additional concepts within abstract algebra. Among the topics included in this course are: set theory and functions, Eulerian and Hamiltonian graphs, binary problems, Boolean equations, Algebraic structures and group theory.
Professional Practice	This course provides a foundation for good practice in a variety of contexts. The ability to communicate effectively using different tools and mediums will ensure that practical, research, design, reporting and presentation tasks are undertaken professionally and in accordance with various communication conventions. Continuing professional development, self-improvement and working towards various goals is an area that is encouraged in the workplace through the appraisal's framework. Among the topics included in this course are: the development of communication skills and communication literacy; the use of qualitative and quantitative data to demonstrate analysis, reasoning and critical thinking; and tasks that require the integration of others within a team-based scenario and planning and problem-solving.
Planning a Computing Project	The course provides examination of project management principles and modern software project management practices. The fundamental knowledge and skills to enable them to undertake independent research and investigation for carrying out and executing a computing project which meets appropriate aims and objectives. Methods for managing and optimizing the software development process are discussed along with techniques for performing each phase of the systems development lifecycle. Present the project and communicate appropriate recommendations based on meaningful conclusions drawn from the evidence findings and/or analysis. Reflect on the value gained from conducting the project and its usefulness to support sustainable organizational performance.
STEM Lab I	This course develops the basic skills in the fields of science, technology, engineering, and mathematics through a set of practical experiments, covering mechanical, electrical, electronics, automation, mechanics of materials, robotics, computer applications, and process control.
Networking	The aim of this course is to provide students with wider background knowledge of computer networking essentials, how they operate, protocols, standards, security considerations and the prototypes associated with a range of networking technologies. This course will provide students with skills to successfully install operate and troubleshoot a small network; and the operation of IP data networks, router, switching technologies, IP routing technologies, IP services and basic troubleshooting.
Website Design & Development	This course introduces students to the underpinning services required to host, manage and access a secure website before introducing and exploring the methods used by designers and developers to blend back-end technologies (server-side) with front-end technologies (client-side).

	This course also discusses the reasons, requirements, relationships, capabilities and features of the systems they will be using and gives them an opportunity to explore various tools, techniques and technologies with 'good design' principles to plan, design and review a multipage website. The topics included in this course are: domain structure, domain name systems, web protocols, database servers, development frameworks, website publishing, content management, search engine optimization, web browsers, HTML standards, CSS and CSS pre-processing (LESS, SASS), presentation models, responsive design, integrated development environments, user requirements, interface design, user experience, branding, navigation, optimization and validation.
Data Structures & Algorithms	This course introduces students to data structures and how they are used in algorithms, enabling them to design and implement data structures. The course introduces the specification of abstract data types and explores their use in concrete data structures. Based on this knowledge, students should be able to develop solutions by specifying, designing and implementing data structures and algorithms in a variety of programming paradigms for an identified need. Topics included in this course are abstract data types specification, formal data notations, data encapsulation, complex data structures, programming language implementations using handles, pointers, classes and methods, algorithm types, data structure libraries, algorithm complexity, asymptotic testing and benchmarking.
Security	The aim of this course is to provide students with knowledge of security, associated risks and how security breaches impact on business continuity. Students will examine security measures involving access authorization, regulation of use, implementing contingency plans and devising security policies and procedures. Among the topics included in this course are detection of threats and vulnerabilities in physical and IT security, and how to manage and assess risks relating to organizational security. Network Security design and operational topics, including address translation, DMZ, VPN, firewalls, AV and intrusion detection systems. Remote access will be covered, as will the need for frequent vulnerability testing as part of organizational and security audit compliance. Assess risks to IT security; Describe IT security solutions; Review mechanisms to control organizational IT security; Manage organizational security.
Cryptography	This course introduces students to the theoretical principles of cryptography and looks at some practical applications, many of which we use on a daily basis. Students are expected to investigate the inner workings of cryptographic systems and how to correctly use them in real-world applications. Students are expected to explore the mathematical algorithms in relation to cryptography and their applications. Students are also expected to analyse the symmetric and asymmetric encryption methods and ciphers, public key cryptography and the security issues related to their implementation. In addition, students are expected to investigate advanced encryption protocols and their applications.
Network Security	This course introduces students to the fundamental principles of Network Security. Topics included in this course are: historical Network Security (NS) principles and associated aspects such as Firewalls, Routers, Switches, MD5, SSL, VPN, AES, SHA-1/2, RSA, DES, 3DES; different types of public and private key cryptography such as Caesar Cipher, IPSec; types of attacks that can be done on a network and methods of preventing such

	attacks such as Man-In-the-Middle (eavesdropping), Denial of Service (DoS), Distributed Denial of Service (DDoS) (ping); Certificate Authority (CA); 'The Cloud' Security aspects and associated counter-measures such Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), phishing, spoofing, DNS attack, SQL Injection, MAC Address spoofing/control.
Forensics	This course introduces students to digital forensics involving the use of specialized techniques to investigate the recovery, authentication and analysis of data on electronic data storage devices as well as Network Security breaches and cyberattacks using different tools and techniques. Topics included in this course are: describing the process of carrying out digital forensics; Forensic Investigation legal guidelines and procedures; understanding low level file structures of several Operating Systems (OS); creating a book disk to enable forensic examination of devices; and undertaking a forensic examination of a device(s) and/or Network Security breaches and cyberattacks.
Information Security Management	This course introduces students to the basic principles of an ISMS and how businesses use them to effectively manage the ongoing protection of sensitive information they hold. There are many reasons for establishing an ISMS for an organisation, but one of the main goals is to enable the organisation to manage information security as a single entity which can be monitored and continually improved upon. This course considers information security management in a business context and will allow students to understand how modern organisations manage the ongoing threats to their sensitive assets.
Computing Research Project	The course offers the opportunity to engage in sustained research in a specific field of study. They conduct an individual research project under a close supervision. Expose to theoretical or experimental research techniques. In Conduct and present a survey of the literature relevant to the research topic. Prepare a thesis reporting on the research project and its outcomes. They will also be expected to present a poster and a short seminar describing their work.
Database Design & Development	The aim of this course is to give students opportunities to develop an understanding of the concepts and issues relating to database design and development, as well as to provide the practical skills to translate that understanding into the design and creation of complex databases. Topics included in this course are: examination of different design tools and techniques; examination of different development software options; considering the development features of a fully functional robust solution covering data integrity, data validation, data consistency, data security and advanced database querying facilities across multiple tables; appropriate user interfaces for databases and for other externally linked systems; creating complex reports/dashboards, testing the system against the user and system requirements; and elements of complete system documentation.
Business Intelligence	Discuss business processes and the mechanisms used to support business decision-making; Compare the tools and technologies associated with business intelligence functionality; Demonstrate the use of business intelligence tools and technologies; Discuss the impact of business intelligence tools and technologies for effective decision-making purposes and the legal/regulatory context in which they are used.

Secure Coding	The aim of the course is to learn about secure software, including its design, implementation and maintenance. During the course students will be exposed to a selection of topics from the following: performing threat modelling, issues in authentication and authorization, auditing for security, input sanitizing, TOCTOU vulnerabilities, memory management issues, fixing vulnerabilities and patch distribution.
Computer Organization & Design	This course introduces students to the principles of digital logic design, computer systems organization and low-level language program development using CPU registers to manipulate data. Students will explore how program instructions and data types can be represented, stored in a computer system, and used to carry out a computing task.
Operating Systems	This course introduces students to different operating systems such as DOS, Windows, UNIX and Linux. The topics covered are the tasks of operating systems such as controlling and allocating memory, prioritizing system requests, controlling input and output devices, facilitating data networking and managing files, including security and protection. Among the topics included in this course are: the history and evolution of Operating Systems; the definition of an Operating System; why Operating Systems are needed; how Operating Systems started and developed; Operating Systems management roles; management of memory, processes, processors, devices and files; security and protection: user security, device, application and process protection; inter-process communication; comparison of Operating Systems; distributed and networked systems; concurrent systems; multi-user systems; graphical interface systems; and practical application of Operating Systems: user interface commands of major Operating Systems; installations and extensions of Operating Systems.
Penetration Testing	Introduction to the principles and techniques associated with the cybersecurity practice known as penetration testing. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The student discovers how system vulnerabilities can be exploited and learns to avoid such problems.
Ethical Hacking	This course covers the most common methods used in computer and network hacking with the intention of learning how to better protect systems from such intrusions. These methods include reconnaissance techniques, system scanning, accessing systems by network and application-level attacks, and denial of service attacks. Finally, Basic Malware Analysis methods and tools under Linux will be studied at the end of this course
Risk Analysis & Systems Testing	The aim of this course is to provide students with knowledge and skills to use risk-based testing (RBT) using a medium-sized application, developing a full and detailed RBT procedure and documenting the results. They will then be able to evaluate the effectiveness of the application and the testing procedures employed. RBT is used widely in industry to organise software testing and use test resources more efficiently. This course introduces students to prioritising testing software features according to risk of failure, evaluated as a function of criticality or importance and impact of failure. Risk of software failure determines the priority of tests within a Test Plan, strategically carrying out testing over multiple test cycles.
Secure System Design & Development	The aim of this course is to learn about design, implementation as well as verification/validation of secure software systems and architectures. It

	covers the principles and practices of secure and high assurance software development process, including security development lifecycle models, and design/verification/validation using languages and tools such as UML. Tools and techniques for code analysis and testing, and evaluation and certification of software will also be emphasized. The course defines and identifies vulnerability detection and avoidance.
Elective I Elective II Elective III	The student can choose two courses from a list of advanced topic courses in Cybersecurity field that will be offered by the department.
Capstone project I Capstone project II	A project-based course intends to reflect different skills and competencies acquired by the student in different courses. The students will learn how to handle a project, starting with the specifications, requirements, design, and implementation then preparing a comprehensive report.
HNC Training HND Training	On-the-job training is a hands-on method of teaching the skills, knowledge, and competencies needed for students to perform a specific job within the workplace. Students learn in an environment where they will need to practice the knowledge and skills obtained during their training.
Web Security	The course covers the issues and techniques in developing secure web-based applications; related topics such as network security, web server security, application-level security and web database security. The course also introduces the vulnerability of web based applications and how to protect those applications from attacks. In addition, advanced topics related to Web, such as E-commerce security, Web 2.0, collaborative Web-based applications, etc., will also be studied.
Internet of Things Security	With the increasing deployment of Internet of Things (IoT) in different domains, IoT security and privacy have become a serious concern. This course covers topics related to IoT security, including: devices, operating systems, sensors, storage, and IoT networking protocols. Students will also learn about IoT devices and systems security and the possible privacy threats and vulnerabilities with a focus on how to mitigate any possible attacks.
Mobile and Wireless Security	This course introduces advanced topics on security and privacy for wireless communication systems, including cellular and wireless networks such wireless body area networks, personal area networks and area local networks. It will discuss current security threats in wireless and mobile networks. It will cover recent technologies used to protect network security and discuss the design and operation of security protocols designated for wireless networks.
Incident Response Management	This course presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. Topics covered include incident response planning (preparation, organization, building and managing a Computer Emergency Response Team (CERT)). Other topics include Incident Response (prevention, detection, notification, reaction, recovery, maintenance), Vulnerability Assessment, Incident Analysis, Malcode Analysis, Forensics and Investigations. The course also covers computer network defence: intelligence and situational awareness, tools and processes.
Ethical Issues in Cyber Security	This course examines the ethical issues in cybersecurity. It discusses the impact of technical decisions to support network security on the values of individuals, organizations, and society. Topics include intellectual

	property, plagiarism, privacy and work, methods of avoiding, detecting, and analyzing intrusions. Students will study tradeoffs intrinsic in security policies, behaviors, and protocols.
Cloud Computing	This course is designed to develop an understanding of the fundamental concept of Cloud Computing, cloud segments, and cloud deployment models, the need for Cloud Computing, an appreciation of issues associated with managing cloud service architecture and to develop a critical awareness of Cloud Computing based projects. Topics included in the course are the paradigms of networking, fundamentals of Cloud Computing, Cloud Computing architecture, deployment models, service models, security, technological drivers, and cloud service providers.
Special Topics	Selected state-of-the-art topics in Cyber Security.