QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**
Course No.	**0133417**		**Course name**		**Internet of Things Security**
Credit Hours	**3**		**Prerequisite Co-requisite**		**Secure Communication Protocols**
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements** ☐ Elective requirements
Teaching style	☐ **Full online learning**		☐ ✓Blended learning		☐ Traditional learning
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 face to face : 1synchronous		☐ **3 Traditional**

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course introduces the fundamental concepts and principles of securing Internet of Things (IoT) devices and systems. Topics include IoT architectures, common vulnerabilities, secure design principles, cryptographic techniques, and mitigation strategies for IoT environments. The course emphasizes classroom lectures, real-world examples, and structured in-class activities.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Title: "IoT Security: Principles and Practices" Author: John Doe Date: 2023 Publisher: SecureTech Press			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	Journals: IEEE IoT Journal, Cybersecurity Review Periodicals: IoT Evolution World			
Supporting websites	NIST IoT Security Framework: https://www.nist.gov OWASP IoT Project: https://owasp.org			
The physical environment for teaching	☐ **Class room**	☐ labs	☐ **Virtual educational platform**	☐ Others

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Necessary equipment and software	
Supporting people with special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Identify IoT architectures and security challenges.	**MK1**
K2	Describe common IoT vulnerabilities and attack vectors	**MK2**
K3	Understand cryptographic methods for securing IoT data	**MK4**
K4	Recognize compliance requirements for IoT security standards.	**MK1**
K5		**MK5**
	Skills	
S1	Implement IoT security measures using tools like Nmap and Wireshark	**MK4**
S2	Analyze and mitigate real-world IoT security threats	**MK1**
	Competences	
C1	Collaborate on developing secure IoT frameworks in team projects.	

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	
1	Introduction to IoT Security
2	IoT Architectures and Protocols

3	Common IoT Vulnerabilities
4	Cryptographic Solutions for IoT
5	IoT Device Authentication Techniques
6	Secure Communication in IoT
7	IoT Security Tools Overview
8	Midterm Review and Exam
9	Risk Assessment in IoT
10	IoT Malware and Attack Patterns
11	IoT Privacy Concerns
12	Compliance and Frameworks
13	IoT Incident Response
14	Emerging Trends in IoT Security
15	Final Review
16	Final Exam

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

This activities was designed using the **Project-Based Learning (PBL)**

Project 1: End-to-End Secure IoT Communication & Authentication Framework

Task / Activity	Reference	Expected Results
Design and simulate a secure IoT ecosystem. Implement device authentication using digital certificates and DTLS handshake. Establish secure MQTT/TLS channels and test against eavesdropping & replay attacks.	NISTIR 8259 (IoT Cybersecurity), OWASP IoT Security Top 10, MQTT Security Specification	A functional simulation with authenticated devices, encrypted communication logs, and a test report demonstrating resilience to man-in-the-middle attacks.

Project 2: IoT Risk Assessment & Incident Response Playbook

Task / Activity	Reference	Expected Results
Conduct a risk assessment for a smart home scenario using the NIST Cybersecurity Framework. Identify threats (e.g., Mirai-like malware, data exfiltration) and create an IR playbook for a compromised device, including containment and evidence collection procedures.	NIST CSF for IoT, ENISA IoT Security Guidelines, Mirai Botnet Analysis Reports	A completed risk matrix with prioritized threats, a step-by-step incident response playbook, and a forensic data collection checklist for IoT devices.

Week	Task / activity	Reference	Expected results
1			
2			
3			
4			
5			
6			
7			
8			