MODULE DESCRIPTION FORM

Module Information					
Module Title	**Introduction to Cybersecurity**			**Module Delivery**	
Module Type	**Core**			☐ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☒ **Seminar**	
Module Code	**CYBT 107**				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level	1		**Semester of Delivery**	1	
Administering Department	CYBT		**College**	TECCAIK	
Module Leader	Name		**e-mail**	E-mail	
Module Leader's Acad. Title	Professor		**Module Leader's Qualification**		
Module Tutor	Name (if available)		**e-mail**	E-mail	
Peer Reviewer Name	Name		**e-mail**	E-mail	
Scientific Committee Approval Date	21/10/2025		**Version Number**	1.0	

79 96

Relation with other Modules			
Prerequisite module	None	**Semester**	
Co-requisites module	None	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	1. Examining legal and regulatory requirements, ethical issues, and the development of cybersecurity policy for commercial and government organizations. 2. Introduce students to the field of sociology and its central theoretical perspectives from Cybersecurity perspective. Provide students with basic ideas and knowledge in the science of sociology. 3. Help students understand the similarities and differences between different sociological paradigms. 4. provide students with basic ideas and knowledge in the science of sociology and how cybersecurity issues effects society. 5. Introduce student to terminology related to cybersecurity such as Cybercrime and deviance, Globalization. 6. Explore the development of organizational cybersecurity policy that meets an organization's compliance requirements and business goals.
Module Learning Outcomes	1. Describe the fundamental concepts and principles of cybersecurity. Students should be able to explain the basic terminology, models, and frameworks used in cybersecurity, such as confidentiality, integrity, availability, risk management, and threat modeling. 2. Identify common cybersecurity threats and attacks. Students should be able to recognize the most common types of cyber threats and attacks, such as malware, phishing, social engineering, and denial-of-service, and understand their impact on individuals, organizations, and society. 3. Apply cybersecurity best practices and tools. Students should be able to apply basic cybersecurity best practices and tools to protect their own devices and data, such as strong passwords, encryption, firewalls, and antivirus software. 4. Analyze cybersecurity incidents and breaches. Students should be able to analyze real-world cybersecurity incidents and breaches, such as data breaches, ransomware attacks, and cyber espionage, and understand their causes, consequences, and mitigation strategies. 5. Evaluate ethical and legal issues in cybersecurity. Students should be able to evaluate ethical and legal issues related to cybersecurity, such as privacy, surveillance, intellectual property, and cybercrime, and understand their implications for individuals, organizations, and society. 6.
Indicative Contents	**Indicative content includes the following.** **Introduction to Cybersecurity (4 HOURS)** **Cybersecurity Fundamentals (6HOURS)** **Cybersecurity Operations (4 HOURS)**

	Cybersecurity Ethics and Law (4 HOURS) **Incident Response and Recovery. (4 HOURS)** **Threat Analysis Mode . (4 HOURS)** **Introduction to Security Policy (4 HOURS)** **Disaster Recovery and Business Continuity (4 HOURS)** **Security policy management and maintenance (4 HOURS)**

Learning and Teaching Strategies

Strategies	Type something like: The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	79	**Structured SWL (h/w)**	5
Unstructured SWL (h/sem)	96	**Unstructured SWL (h/w)**	6
Total SWL (h/sem)	**150**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	3	10% (10)	5, 8, and 10	LO #1, #2, #5 and #10, #11
	Assignments	2	10% (10)	2 and 12	LO #3, #4 and #6, #7
	Projects / Lab.	1	10% (10)	Continuous	All
	Report	1	10% (10)	13	LO #5, #8 and #10
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #7
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

KEY LEARNING OUTCOMES OF THE COURSE UNIT

	Material Covered
Week 1	1. **Introduction to Cybersecurity** • Definition of cybersecurity • Importance of cybersecurity • Cybersecurity threats and attacks • Cybersecurity best practices
Week 2	**Introduction to Cybersecurity** • Cybersecurity threats and attacks • Cybersecurity best practices
Week 3	**Cybersecurity Fundamentals** • Security models and frameworks • Risk management
Week 4	**Cybersecurity Fundamentals** • Security policies and procedures • Security controls and countermeasures
Week 5	**Cybersecurity Operations** • Incident response and management • Security monitoring and analysis • Vulnerability assessment and management • Penetration testing and ethical hacking
Week 6	**Cybersecurity Ethics and Law** • Ethical and legal issues in cybersecurity • Cybercrime and cyber law
Week 7	**Cybersecurity Ethics and Law** • Cybersecurity regulations and standards • Cybersecurity career paths and opportunities
Week 8	**Incident Response and Recovery.** • Incident Response and Recovery • Incident response planning
Week 9	**Incident Response and Recovery** • Incident detection and analysis • Incident containment and eradication
Week 10	**Incident Response and Recovery** • Business continuity and disaster recovery
Week 11	**Threat Analysis Mode** • , Categorization of threats. • Analysis of threats.
Week 12	**Introduction to Security Policy** • Overview of security policy development and implementation

	• Why security policy is important. • Risk assessment and analysis • Hands-on exercises in developing security policies
Week 13	**Disaster Recovery and Business Continuity**
	Security Policy Implementation • Best practices for implementing security policies. • Developing and implementing security protocols. • Incident response planning. • Hands-on exercises in implementing security policies.
Week 14	**Security policy management and maintenance** • Security policy auditing and compliance • Security policy training and awareness
Week 15	**Review and Presentation**
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus)	
	Material Covered
Week 1	Lab 1: Network Security Monitoring Software
Week 2	Lab 2: Vulnerability Assessment Software
Week 3	Lab 3: Packet Sniffer Software
Week 4	Lab 4: Encryption Tools
Week 5	Lab 5: Web Vulnerability Scanning Tools
Week 6	Lab 6: Penetration Testing Tools
Week 7	Lab 7: Antivirus Software
Week 8	Lab 8: Network Intrusion Detection Tools
Week 9	Lab 9: Keylogger Software
Week 10	Lab 10: Threat Intelligence Enrichment Tools
Week 11	Lab 11: Threat Identification in the Network
Week 12	Lab 12: Packet Sniffing Tools
Week 13	Lab 13: Network Security Monitoring Software
Week 14	Lab 14: Vulnerability Assessment Software
Week 15	Review and Students presentation
Week 16	Final Exam

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Introduction to Computer Networks and Cybersecurity by Chwan-Hwa (John) Wu and J. David Irwin, 2013	Yes
Recommended Texts	1. Guide to Cyber Security for Beginners 2. Cybersecurity Essentials by Charles J. Brooks and Christopher Grow	No
Websites		

Grading Scheme

Group	Grade	Marks %	Definition
Success Group (50 - 100)	**A -** Excellent	90 - 100	Outstanding Performance
	B - Very Good	80 - 89	Above average with some errors
	C - Good	70 - 79	Sound work with notable errors
	D - Satisfactory	60 - 69	Fair but with major shortcomings
	E - Sufficient	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX –** Fail	(45-49)	More work required but credit awarded
	F – Fail	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.