Ethics of information Age

Module Information			
Module Title	**Ethics of information Age**	**Module Delivery**	
Module Type	**Core**	☐ **Theory** ☒ **Lecture** ☐ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CYBT102**		
ECTS Credits	**2**		
SWL (hr/sem)	**50**		
Module Level	1	**Semester of Delivery**	1
Administering Department	Cyber Security Techniques Engineering	**College**	Technical Engineering College for computer and AI / KIRKUK
Module Leader		**e-mail**	E-mail
Module Leader's Acad. Title		**Module Leader's Qualification**	
Module Tutor	Name (if available)	**e-mail**	
Peer Reviewer Name	Name	**e-mail**	E-mail
Scientific Committee Approval Date	30/12/2025	**Version Number**	1.0

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. 7. Introduce students to new ways of thinking about race, ethnicity, and culture from the perspectives of sociology. 8. Use computational social science techniques to identify, counter, and measure the impact of communication in social cybersecurity.
Module Learning Outcomes	1. Understanding the impact of technology on society: Students will be able to analyze the effects of technology on social structures, institutions, and relationships, and identify potential cybersecurity risks associated with technological advancements. Students can explain the sociological significance of social identity groups and the processes that create them; determine the historical and contemporary factors that shape social inequality; and analyze the relationship between social structure and individual agency. 2. Students will be able to define and explain sociological concepts and explain social facts and society-related concepts. 3. Students will be able to effectively engage with and apply their “sociological imagination” to think critically about the social world and what separates sociology from other social science disciplines. 4. Students will be able to construct relevant arguments using data from credible sources and demonstrate familiarity with basic statistical concepts. 5. help students to develop critical thinking skills, understand sociological concepts and theories, and analyze social phenomena from a sociological perspective. 6. Help students to develop communication and research skills, as well as their ability to engage with diverse perspectives and apply sociological concepts to real-world issues.
Indicative Contents	Indicative content includes the following. Introduction to Sociology and Cybersecurity. (3hrs) Cybersecurity Fundamentals. (2hrs) Sociology Fundamentals. (10hrs) Cybersecurity and Society. (3hrs) Cybercrime and Deviance. (2hrs) Cybersecurity and Social Change. (2hrs) Cybersecurity and Globalization. (2hrs) Cybersecurity and Ethics. (1hrs)

	Introduction to Cyberbullying(2hrs) Effects of Cyberbullying (1hrs) Human-factors, Cyber security, and sociology. (3hrs) Risks and cybersecurity incidents and how society should deal with them. (3hrs)

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 learning and by considering types of simple case study discussions involving some sampling activities that are interesting to the students.

Student Workload (SWL)

Structured SWL (h/sem)	33	**Structured SWL (h/w)**	2
Unstructured SWL (h/sem)	17	**Unstructured SWL (h/w)**	4
Total SWL (h/sem)	**50**		

Module Evaluation

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	LO #1, #2 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)

Week	Material Covered
1	• Introduction to Sociology and Cybersecurity: • Overview of the course • Introduction to sociology and cybersecurity • The importance of cybersecurity in modern society
2	**Cybersecurity Fundamentals.** • Cybersecurity basics • Cyber threats and vulnerabilities • Cybersecurity best practices
3	**Sociology Fundamentals**. • Introduction to sociology. • Social structures and institutions. • Social norms and values.
4	**Cybersecurity and Society** • The impact of cybersecurity on society. • Social and cultural factors that influence cybersecurity practices. • Privacy and security policy. • social, political, legal, criminological, and economic dimensions of cybersecurity through a social science framework
5	**Cybercrime and Deviance** • Types of cybercrime. • Theories of deviance and cybercrime. • The impact of cybercrime on society.
6	**Cybersecurity and Social Change** • Cybersecurity and social change • The role of technology in social change • Cybersecurity and activism
7	Cybersecurity and Globalization. • Cybersecurity and globalization • The impact of globalization on cybersecurity • Cybersecurity and international relations
8	**Cybersecurity and Ethics** • Ethical issues in cybersecurity • Cybersecurity and social responsibility • Cybersecurity and the future of society
9	**Introduction to Cyberbullying** • Definition of cyberbullying • Types of cyberbullying • How cyberbullying differs from traditional bullying
10	**Effects of Cyberbullying.** • Emotional and psychological impact on victims • Impact on academic performance • Legal and social consequences
11	**Responding to Cyberbullying.** • How to identify cyberbullying. • Legal and ethical considerations • Reporting cyberbullying incidents**.** **Supporting victims of cyberbullying.**

12	**Human-factors and Cyber security** • Human-factors approach to understanding cybersecurity threats, social factors that contribute to cyber incidents
13	**Risks and cybersecurity incidents** • The political and legal mechanisms that are developed to control the behaviors of those who create risks and cybersecurity incidents.
14	**Review and Student Presentation**
15	**Final Exam**

Learning and Teaching Resources

	Text	Available in the Library?
Required Texts	Introduction to Sociology" by George Ritzer.	Yes
Recommended Texts	1. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman 3. "The Cybersecurity Canon: Must-Read Books" by Palo Alto Networks	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.