Level	Correlation
-	Nil
1	Slightly / Low
2	Moderate / Medium
3	Substantial / High

Assessment Rubrics:

- Quiz / Assignment/ Quiz/ Discussion / Seminar
- Midterm Exam
- Programming Assignments
- Final Exam

Mapping of COs to Assessment Rubrics :

	Internal Exam	Assignment	Quiz/ Seminar	End Semester Examinations
CO 1	✓		✓	✓
CO 2	✓		✓	✓
CO 3	✓			✓
CO 4		✓		✓

DSE

1. INTRODUCTION TO CYBER SECURITY (Stream: Cyber Security)

Discipline	COMPUTER SCIENCE				
Course Code	UK3DSECSC200				
Course Title	**INTRODUCTION TO CYBER SECURITY**				
Type of Course	DSE				
Semester	III				
Academic Level	2				
Course Details	Credit	Lecture per week	Tutorial per week	Practical per week	Total Hours/Week

	4	4 hours		0	4 hours
Pre-requisites	Basic understanding of computer systems and networking is desirable.				
Course Summary	This course is a disciplinary specific elective in the stream Cyber Security. The course introduction to Cybersecurity highlights the importance of Cybersecurity in modern society, exploring its evolution, and recognizing the various threats that digital systems face. Besides providing insights into the security policies, principles, procedures, and best practices for maintaining a secure environment, The Course provides a solid foundation for individuals seeking to pursue careers in cybersecurity. By mastering the fundamental concepts and techniques covered in this course, students will be better equipped to defend their digital assets, mitigate cyber threats, and contribute to the overall security of information systems in today's digital age.				

Detailed Syllabus:

Module	Unit	Content	Hrs
I	**Title of the Module: Introduction to Cyber Security**		**12**
	1	Information Security, Importance, Classification of information, Classification of Information Systems, LAN Classifications, threats-internal, external threats, threat agents, Malicious threat, non-malicious threats, threat intent	
	2	Threats to Security, Employees, Amateur hackers and Vandals, Criminal hackers and Saboteurs,	
	3	Cyber Security, - The C I A Triad, reasons for Cyber-crimes. Importance of Cyber security, Cyber-attacks- damages, history of cyber-crime, evolution of cyber-crime, cyber-crime classification, types of cyber-crimes- categories	
	4	Current scenario- Internet of Things, Challenges faced by Internet of things- Weak passwords, unsecured network access, inappropriate update protocols, unsecured interfaces, default settings, no device management, data storage and transfer challenges, inappropriate privacy protection, outdated components, Evolution of hacking equipments, tools and techniques, growing demand for data access.	

II	**Title of the Module**: **Application Security**		**12**
	5	Introduction, Database Security, Internet Security	
	6	Application Security- types, End Point Security- types, Identity and Access management, Identity management solutions and features	
	7	Mobile Security, Data Security, Drive by download, Infrastructure security, Disaster recovery	
	8	Email Security- S/MIME. PGP, MOSS, PEM, Net Security- SSL. SHTTP, browser scripts.	
III	**Title of the Module**: **Security Threats**		**12**
	9	Introduction to Security threats, Virus, Worms, Trojan Horse, Bombs, Trap Door, Email Spoofing,	
	10	Email Virus, Virus Life cycle, How virus works? Macro Viruses, Malicious Softwares, Network and Services Attack,	
	11	Denial of Service Attack (DOS), Types of DOS, Methods of attack,	
	12	SYN Flood attack, TCP Flooding, UDP Flooding, ICMP Flooding, Smurf, Ping of death, Tear Drop, LAND, Echo-CharGEN, Naptha Attacks	
IV	**Title of the Module: Cyber Security Components and Defense Mechanism**		**12**
	13	OSI Layer, Zero-day attacks- risks of Zero-day attacks	
	14	Network Security- types of attacks- common types of common attacks, port scanning techniques, Unauthorized access, man in the middle attacks, Types of attacks	
	15	Code and SQL injection attacks, types of SQL injections, inferential SQL	
	16	Identity and Access management, Mobile Security	
	17	Fighting Cyber-attacks- Defense in depth, Authentication, Cryptography, Security Technology -Firewall, Data loss Prevention, Antivirus Solutions, Intrusion Detection, Access Control, Access Control Models- discretionary, mandatory, role based, Virtual Private networks, web browsers, Data backup- differential, incremental, biometrics- physiological, behavioural characteristics, authentication factors- two factor, multi factor authentication, passwords- password managers.	
V	**Flexi Module- Not included for End Semester Exams**		**12**

	18	Electronic payment Systems. Credit cards, Debit Cards, Pros and Cons of using Debit vs Credit Cards, Types of Debit Cards, Types of Credit Cards, Credit card payment process, Smart Cards, Emoney, Electronic Fund Transfer. Ecommerce Business Model, Advantages, Disadvantages, Ecommerce Security systems, measures to ensure security Security Protocols in Internet, Electronic Cash, How is it used? Relevance, Cryptography in Information security Symmetric, Asymmetric, Digital Signature, Digital Signature Process, Role of Data Encryption and Challenges in implementing encryption protocols.	

References

Books:

1. Mayank Bhushan, Rajkumar Singh Rathore, Aatif Jamshed Fundamentals of Cyber Security Principles Theory and Practices, , BPB Publishers, 2017

2. Anand Shinde, Notion press, Introduction to Cyber Security- Guide to the world of Cyber Security, 2021

Course Outcomes

No.	Upon completion of the course the graduate will be able to	Cognitive Level	PSO addressed
CO-1	Summarise the fundamental principles and concepts of cybersecurity.	U	PSO-1
CO-2	Identify best practices for securing digital assets.	U	PSO-1,2
CO-3	Demonstrate awareness of common cyber threats and techniques used by attackers.	U	PSO-1
CO-4	Identify measures for implementing cybersecurity.	U	PSO-1

15R-Remember, U-Understand, Ap-Apply, An-Analyse, E-Evaluate, C-Create

Note: 1 or 2 COs/module

Name of the Course: INTRODUCTION TO CYBER SECURITY

Credits: 4:0:0 (Lecture: Tutorial: Practical)

CO No.	CO	PO/ PSO	Cognitive Level	Knowledge Category	Lecture (L)/ Tutorial (T)	Practical (P)

1	Summarise the fundamental principles and concepts of cybersecurity.	PO-1,2,3,6,7 PSO-1	U	F, C	L	-
2	Identify best practices for securing digital assets.	PO-1,2,3,4,6,7 PSO-1,2	U	F, C	L	-
3	Demonstrate awareness of common cyber threats and techniques used by attackers.	PO-1,2,3,4,6,7 PSO-1	U	F, C	L	-
4	Identify measures for implementing cybersecurity.	PO-1,2,3,6,7 PSO-1	U	F, C	L	-

F-Factual, C- Conceptual, P-Procedural, M-Metacognitive

Mapping of COs with PSOs and POs:

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PSO1**	**PSO2**	**PSO3**	**PSO4**
CO 1	2	1	1	-	-	2	2	1	1	-	-	-
CO 2	2	2	1	1	-	2	2	1	2	3	-	-
CO 3	2	2	1	1	-	2	2	1	2	-	-	-
CO 4	2	2	1	-	-	2	2	2	2	-	-	-

Correlation Levels:

Level	**Correlation**
-	Nil
1	Slightly / Low
2	Moderate / Medium

3	Substantial / High

Assessment Rubrics:

- Quiz / Assignment/ Quiz/ Discussion / Seminar
- Midterm Exam
- Final Exam

Mapping of COs to Assessment Rubrics:

	Internal Exam	Assignment	Discussion	End Semester Examinations
CO 1	✓			✓
CO 2	✓		✓	✓
CO 3	✓		✓	✓
CO 4		✓		✓

2. DATA SCIENCE FUNDAMENTALS (Stream: Data Science)

Discipline	COMPUTER SCIENCE				
Course Code	UK3DSECSC201				
Course Title	DATA SCIENCE FUNDAMENTALS				
Type of Course	**DSE**				
Semester	III				
Academic Level	2				
Course Details	Credit	Lecture per week	Tutorial per week	Practical per week	Total Hours/Week
	4	3 hours	-	2 hours	5 hours
Pre-requisites	NIL				
Course Summary	This course aims to introduce the student to the main concepts of data science, understand the essential principles and to implement spreadsheet-based data analysis. Through a blend of theoretical understanding and hands-on practice, learners will develop a solid foundation in data				