

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Data Security and Data Privacy
Course Code:	2ET2070103T
Pre-requisite Course:	Fundamentals, Data privacy attacks, Data linking and profiling, Access control models, Mathematical model for data sharing, Protection models, Medical privacy legislations, Privacy in World Wide web.

Course Objectives: After successful completion of the course, student will be able to

1. To understand the basic principles of Data Security & Privacy management.
2. To understand the basic concepts of the technical components involved in implementing of the security & privacy.
3. To understand that ensuring Data security & privacy in a modern organization is a problem for the management to solve and not one that the technology alone can address.
4. To analyze the important economic and commercial consequences of devising security and privacy solutions in an enterprise or the lack thereof.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Introduction of Data Security: Review of the essential terminologies, basic concepts of security and privacy. Relation or lack thereof between the Information Security, Network Security, Systems Security and the Cyber Security. Key principles of Information Security in terms of Security mechanisms, security attributes and the security attacks. Role of National Security Systems (CNSS) and CERTIN. The McCumber Cube for Security. Introduction to the Security Systems Development Life Cycle and the difference between the Software Security and the Security Software. Classical Security Models. Taxonomy of Security attacks. Illustrations of typical attacks. Cyber security threats. The basic terminologies viz. threats, defects, vulnerabilities, exploits, attacks, bugs.	11	20
2	Data privacy, Risk Analysis and Management: Information Asset, Information Classification, Secret, Confidential, Private and Public Information, Declassification or Reclassification, privacy invasion, privacy challenges in test environment. Privacy Technological Impact. Risk Analysis Process, Threat Identification, Probability of Threat Occurrence, Impact of the Threat and Controls, Risk Mitigation and Control Types, Cost Analysis, Risk Management, Approaches and Considerations, Security Models & Frameworks, Methodologies for Information System Security.	11	20

3	Firewalls & Intrusion Detection and Prevention Systems: Firewalls: Processing Modes, Categorized by Generations, by Structure, Architectures, Selecting the right firewall, Configuring and Managing Firewalls. Remote Access, the concept of Virtual Private Networks. Intrusion Detection and Prevention Systems: Why use IDPSs, Types, IDPSs Detection Methods, IDPS Response Behaviour, IDPS Approaches. Strengths and Limitations. Deployment and Implementation of IDPSs. Measuring the effectiveness of IDPSs. Honeypots, Honeynets and Padded Cell Systems. Network Reconnaissance: Network Scanning and Analysis.	12	30
4	Security Assessment and Techniques: Security Mechanisms: The Symmetric and Asymmetric Key Cryptography, Ciphers: Cryptographic Algorithms and the Cryptosystems, Mechanisms for Data Integrity and Entity Authentication, Access Control mechanisms. Cryptographic Tools: The Public-Key-Infrastructure (PKI), Digital Signatures, Digital Certificates, Hybrid Cryptographic Systems, Steganography. The Public Key Cryptography (PKC) limitations and looking beyond the PKC.	12	30

Text Books:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, Auerbach Pub, 2013.
2. Information Security Management Principles, by Andy Taylor, David Alexander, Amanda Finch, David Sutton, 3rd edition, BCS, The Chartered Institute for IT Publishers, 2020
3. S. Stalla-Bourdillon, J. Phillips, and M. D. Ryan, Privacy vs. Security. Springer London, 2014.
4. Houbing Song, Glenn A. Fink and Sabina Jeschke, "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications", Wiley-IEEE Press, 2017

Reference Books:

1. Principles of Information Security, By Michael E. Whitman, Herbert J. Mattord, Course Technology Press, 4th edition, 2011
2. Thomas J Shaw, "Information security and privacy: a practical guide for global executives, lawyers and technologists", American Bar Association, Chicago, 2011.

List of Open-Source Software/learning website:

- ☐ <https://freecoursesonline.co.uk/business/data-protection-and-data-security/>
- ☐ <https://www.coursera.org/courses?query=data%20security>
- ☐ <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content>

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Examine and apply the fundamental techniques of information security.	Understanding (2) Applying (3)
COL2	Examine and apply and identify potential security issues and the associated risks.	Applying (3)
COL3	Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society	Applying (3)
COL4	Plan for the future and design a solution based on user requirements. Explain business continuity, backup and disaster recovery. Understand troubleshooting and quality consumer support.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M	M												
CLO2	H	H		M					L							
CLO3	H	M	M	H												
CLO4	M	M	M	M					L							

H: High, M: Medium, L: Low