Program	ADP Data Science	
Course Code	CC-308	
Course Title	Information Security	
Credit Hours	**Theory**	**Lab**
	3	0
Lecture Duration	90 minutes (1.5 Hours), 2 lectures per week	
Semester	8	
Pre-requisites	**Courses**	**Knowledge**
	None	Nil
Follow Up Courses	Nil	

Course Learning Outcomes (CLOs)

CLO No	Course Learning Outcome	Bloom Taxonomy
CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management, and ethics	C2 (Explain)
CLO-2	Discuss legal, ethical, and professional issues in information security	A2 (Discuss)
CLO-3	Apply various security and risk management tools for achieving information security and privacy	C3 (Apply)
CLO-4	Identify appropriate techniques to tackle and solve problems in the discipline of information security	C4 (Identify)

Aims and Objectives	1. In this course students learn basics of information security, in both management aspect and technical aspect. 2. Students understand of various types of security incidents and attacks, and learn methods to prevent, detect and react incidents and attacks. Students will also learn basics of application of cryptography which are one of the key technologies to implement security functions.
Learning Outcomes	• CLO-1: Explain key concepts of information security such as design principles, cryptography, risk management, and ethics • CLO-2: Discuss legal, ethical, and professional issues in information security • CLO-3: Apply various security and risk management tools for achieving information security and privacy • CLO-4: Identify appropriate techniques to tackle and solve problems in the discipline of information security

Syllabus	I. Information security foundations, security design principles; security mechanisms, symmetric and asymmetric cryptography, encryption, hash functions, digital signatures, key management, authentication and access control; software security, vulnerabilities and protections, malware, database security; network security, firewalls, intrusion detection; security policies, policy formation and enforcement, risk assessment, cybercrime, law and ethics in information security, privacy and anonymity of data.
Contents	II. **Computer Security Concepts** i. Threats, Attacks, and Assets ii. Security Functional Requirements iii. Fundamental Security Design Principles iv. Attack Surfaces and Attack Trees v. Computer Security Strategy vi. Standards III. **Cryptographic Tools** i. Confidentiality with Symmetric Encryption ii. Message Authentication and Hash Functions iii. Public-Key Encryption iv. Digital Signatures and Key Management v. Random and Pseudorandom Numbers vi. Practical Application: Encryption of Stored Data IV. **User Authentication** i. Digital User Authentication Principles ii. Password-Based Authentication iii. Token-Based Authentication iv. Biometric Authentication v. Remote User Authentication vi. Security Issues for User Authentication vii. Practical Application: An Iris Biometric System V. **Access Control** i. Access Control Principles ii. Subjects, Objects, and Access Rights iii. Discretionary Access Control iv. Example: UNIX File Access Control v. Role-Based Access Control vi. Attribute-Based Access Control vii. Identity, Credential, and Access Management viii. Trust Frameworks

VI. **Database and Data Centre Security**

i. The Need for Database Security
ii. Database Management Systems
iii. Relational Databases iv. SQL Injection Attacks
v. Database Access Control
vi. Inference vii. Database Encryption
viii. Data Center Security

VII. **Malicious Software**

i. Types of Malicious Software ii. Advanced Persistent Threat iii. Propagation — Infected Content - Viruses iv. Propagation — Vulnerability Exploit - Worms
v. Propagation — Social Engineering — SPAM E-Mail, Trojans
vi. Payload — System Corruption vii. Payload — Attack Agent — Zombie, Bots
viii. Payload — Information Theft — Keyloggers, Phishing, Spyware ix. Payload — Stealthing — Backdoors, Rootkits x. Countermeasures

VIII. **Denial-of-Service Attacks**

i. Denial-of-Service Attacks ii. Flooding Attacks
iii. Distributed Denial-of-Service Attacks iv. Application-Based Bandwidth Attacks v. Reflector and Amplifier Attacks
vi. Defenses Against Denial-of-Service Attacks vii. Responding to a Denial-of-Service Attack

IX. **Intrusion Detection**

i. Intruders
ii. Intrusion Detection iii. Analysis Approaches iv. Host-Based Intrusion Detection
v. Network-Based Intrusion Detection vi. Distributed or Hybrid Intrusion Detection vii. Intrusion Detection Exchange Format viii. Honeypots

X. **Firewalls and Intrusion Prevention Systems**

i. The Need for Firewalls ii. Firewall Characteristics and Access Policy iii. Types of Firewalls iv. Firewall Basing
v. Firewall Location and Configurations
vi. Intrusion Prevention Systems

	XI. **IT Security Management and Risk Assessment** i. IT Security Management ii. Organizational Context and Security Policy iii. Security Risk Assessment iv. Detailed Security Risk Analysis XII. **Legal and Ethical Aspects** i. Cybercrime and Computer Crime ii. Intellectual Property iii. Privacy iv. Ethical Issues
Teaching-learning Strategies	The course will be based on the following teaching and learning activities: • Lectures covering the theoretical part using PowerPoint presentations • Case studies • Review questions
Assignments	Total 4 Assignment
Textbooks	• Computer Security: Principles and Practice, 3rd edition by William Stallings
Reference Material/Suggested Readings	• Whitman, M. E., & Mattord, H. J. (2019). Principles of information • security. • Gollmann, D. (2011. Computer security. Chichester: Wiley. Easttom, W., & Safari, an O'Reilly Media Company. (2011). Computer Security Fundamentals, Second Edition. • Gordon, A. (2015). Official (ISC)2 Guide to the CISSP CBK, Fourth Edition. Hoboken: CRC Press.
Notes	• Power Point slides with reading material from book.

Detailed Lecture wise plan

Week	Lecture	Topic	Source Book (Ch#)	Recommendation for Learning Activities
1	1	Computer Security Concepts Threats, Attacks, and Assets Security Functional Requirements	Ch-01	
	2	Fundamental Security Design Principles Attack Surfaces and Attack Trees Computer Security Strategy	Ch-01	

Week	Lecture	Topic	Source Book (Ch#)	Recommendation for Learning Activities
2	3	Cryptographic Tools Confidentiality with Symmetric Encryption Message Authentication and Hash Functions	Ch-02	
	4	Public-Key Encryption Digital Signatures and Key Management	Ch-02	
3	5	Random and Pseudorandom Numbers Practical Application: Encryption of Stored Data	Ch-02	
	6	User Authentication Electronic User Authentication Principles Password-Based Authentication	Ch-03	**Assignment-1**
4	7	Token-Based Authentication Biometric Authentication Remote User Authentication	Ch-03	**Quiz-1**
	8	Security Issues for User Authentication Practical Application: An Iris Biometric System	Ch-03	
5	9	Case Study: Security Problems for ATM Systems	Ch-03	
	10	Access Control Access Control Principles Subjects, Objects, and Access Rights Discretionary Access Control Example: UNIX File Access Control	Ch-04	
6	11	Role-Based Access Control Attribute-Based Access Control Identity, Credential, and Access Management Trust Frameworks	Ch-04	
	12	Case Study: RBAC System for a Bank	Ch-04	
7	13	Database and Cloud Security The Need for Database Security Database Management Systems	Ch-05	**Assignment-2**

Week	Lecture	Topic	Source Book (Ch#)	Recommendation for Learning Activities
	14	Relational Databases SQL Injection Attacks	Ch-05	**Quiz-2**
8	15	Database Access Control Inference Database Encryption	Ch-05	
	16	Cloud Computing Cloud Security Risks and Countermeasures	Ch-05	
9	17	Data Protection in the Cloud Cloud Security as a Service	Ch-05	
	18	Malicious Software Types of Malicious Software (Malware) Advanced Persistent Threat	Ch-06	
10	19	Propagation—Infected Content—Viruses Propagation—Vulnerability Exploit—Worms Propagation—Social Engineering—Spam EMail, Trojans	Ch-06	
	20	Payload—System Corruption Payload—Attack Agent—Zombie, Bots	Ch-06	
11	21	Payload—Information Theft—Keyloggers, Phishing, Spyware Payload—Stealthing—Backdoors, Rootkits Countermeasures	Ch-06	
	22	Denial-of-Service Attacks Flooding Attacks	Ch-07	
12	23	Distributed Denial-of-Service Attacks Application-Based Bandwidth Attacks Reflector and Amplifier Attacks	Ch-07	
	24	Defenses Against Denial-of-Service Attacks Responding to a Denial-of-Service Attack	Ch-07	
13	25	Intrusion Detection Intruders Intrusion Detection Analysis Approaches	Ch-08	**Assignment-3**

Week	Lecture	Topic	Source Book (Ch#)	Recommendation for Learning Activities
	26	Host-Based Intrusion Detection Network-Based Intrusion Detection Distributed or Hybrid Intrusion Detection	Ch-08	**Quiz-3**
14	27	Intrusion Detection Exchange Format Honeypots Intrusion Detection, Example System: Snort	Ch-08	
	28	Firewalls and Intrusion Prevention Systems The Need for Firewalls Firewall Characteristics and Access Policy	Ch-09	
15	29	Types of Firewalls Firewall Basing Firewall Location and Configurations Intrusion Prevention Systems Example: Unified Threat Management Products	Ch-09	**Assignment-4**
	30	IT Security Management and Risk Assessment IT Security Management Organizational Context and Security Policy Security Risk Assessment Detailed Security Risk Analysis	Ch-14	**Quiz-4**
16	31	Legal and Ethical Aspects Cybercrime and Computer Crime Security policies, Policy formation and enforcement	Ch-19	
	32	Cybercrime, law and ethics in information security, Privacy and anonymity of data. Intellectual Property Privacy Ethical Issues	Ch-19	