Title of Course: Data Security Officer

Class: MSc II DS

DURATION: Three Months

Name of Co-ordinator: Mr.Khandagale S.B.

Department of Data Science

Title: Data Security

Sector: - Information Technology (I.T.)

Year of implementation: 2023

Structure of Skill Development Course

Duration	Theory Hours	Practical Hours	Total Hours	Credits	No. of students in batch
3 Month	20	30	50	03	30

Syllabus

Course Objectives: Students should be able to…

1. Understanding the fundamentals of data security and the threats and attacks that can compromise the confidentiality, integrity, and availability of data.
2. Learning best practices for securing data at rest and in transit, including encryption, access control, and authorization.
3. Gaining an understanding of advanced data security techniques such as secure coding practices, cloud security, data anonymization, and compliance with regulations and industry standards.
4. Evaluating the effectiveness of data security measures in protecting against real-world threats and attacks.

5. Applying data security principles to a real-world data science scenario and demonstrating the ability to secure sensitive data effectively

Theory Syllabus (20 Hrs)

- **Unit 1: Introduction to Data Security(10)**

Overview of data security in the context of data science, Types of data security threats and attacks, Fundamentals of cryptography and encryption, Best practices for securing data at rest and in transit, Introduction to access control and authorization

- **Unit 2: Advanced Data Security Techniques**

Secure coding practices for data science projects, Security considerations for cloud-based data storage and processing, Data anonymization and de-identification techniques, Protecting against insider threats and data breaches, Compliance with regulations and industry standards (e.g. GDPR, HIPAA, PCI DSS)

Practical Syllabus (30 Hrs)

List of Experiments:----------24 hr

1.Overview of data security in the context of data science

2.Types of data security threats and attacks

3.Introduction to cryptography and encryption

4. Introduction to access control and authorization

5.Protecting against insider threats and data breaches

6.Compliance with regulations and industry standards GDPR,

7.Compliance with regulations and industry standards HIPAA,

8. Compliance with regulations and industry standards PCI DSS

9. Case Study on cloud-based data storage

10. Case Study on cloud Security

Course Outcomes: Students will be able to…

1. Understand the importance of data security in the context of data science and recognize the various types of data security threats and attacks.

2.Explain the fundamentals of cryptography and encryption, and apply them to protect sensitive data at rest and in transit.

3.Implement access control and authorization mechanisms to control who can access and modify data in a database or other storage medium.

4.Apply secure coding practices and implement security measures for cloud-based data storage and processing.

5.Implement data anonymization and de-identification techniques to protect against privacy breaches and evaluate their effectiveness against real-world threats.

6.Identify and protect against insider threats and data breaches.

7.Understand the compliance requirements for data security regulations and industry standards, such as GDPR, HIPAA, and PCI DSS.

8.Apply data security principles to a real-world data science scenario and demonstrate the ability to secure sensitive data effectively

Reference Books:

1."Data Protection: A Practical Guide to UK and EU Law" by Peter Carey

2."Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson

3."Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier

4."Network Security Essentials: Applications and Standards" by William Stallings

5."Data Privacy and Security" by Darius Dziuda

6."Python Cryptography" by Samuel Bowne

7."Practical Cloud Security: A Guide for Secure Design and Deployment" by Chris Dotson

8."Anonymizing Health Data: Case Studies and Methods to Get You Started" by Khaled El Emam and Luk Arbuckle

9."The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson

10."CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide" by Mike Chapple, James Michael Stewart, and Darril Gibson

BOS Sub Committee:

1. Prin. Dr. B. T. Jadhav
2. Mr. R.P. Waghamare
3. Mr. S. B. Khandagale
4. Ms. Jadhav S.P.

Academic Expert:

1. Mr. Mehul Jadhav

Industrial Expert:

1. Mr. Vijayendra Shinde