CBEL Code-ELO-102
Course Name- Data Protection in the Digital Business
Total Duration- 40 hours

Credits: 4		
Lecture Hours	**Practical/Activity Hours**	**Mode**
16	**24**	**Blended**

Overview

Data Security and privacy will encourage professionals and learners to think critically about the trade-offs and challenges presented by the ever-changing role of the technology and privacy policy used in the digital business. Besides, to explore technological, legal and ethical implications of one's personal data. The risk and rewards of data collection and surveillance, and the needs for security policy, advocacy and privacy monitoring. Data Protection is centred around how data should be collected, stored, managed, and shared with third parties, and compliance with the applicable privacy laws. Along with data security, data privacy creates a data protection area with protected usable data in the digital world.

The students will be able to understand what is data security and privacy, examine data security and privacy, evaluate data security policies and enforcements, choose what data is important and why, and how to implement data security and privacy to ensure protected usable data.

Module:

Interactive sessions=16 Hours (including activities)

Assignment/ assessment/ Project/ MOOC = 24 Hours

Interactive sessions:

1. Concept of classical cryptography
2. Approaches of cryptography
3. Network security threats
4. Access control methods and systems
5. Activity monitoring systems
6. Data discovery and classification
7. Data subject access request(DSAR) under GDPR
8. Third party management
9. Privacy policies

Assignment/ assessment/ activity/ MOOC [A1-A4]

Data Security / Encryption and decryption methods / DLP – CASB / Activity monitoring Software / Data privacy consent form / Data discovery and classification tools / Data removal policy and software etc.

A1 Data Security Concept and approaches (Assignment based)

A2 Data Privacy and risk management policies

A3   Data Protection techniques and policy management, model design and practices.

A4 Data Security / Privacy project / MOOC *(shall be notified after batch commencement)*

Suggested Readings

1. The Art of Invisibility (Kevin Mitnick).

2. No Place to Hide (Edward Snowden).

3. Principles of Information Security (Michael E. Whitman and Herbert J. Mattord)

4. Elementary Information Security (Richard E. Smith).

ASSESSMENT SCHEME

☐ Interim Formative Assessment [A1-A2-A3: 3 Hours in Class]
☐ Course-end Summative Assessment [A4: 24 Hours outside Class]

Formative Assessment- X

Sl No.	Slot	Hours	Content / Topic	Assessment Type	Marks
A1	L2	1	Content / Topics covered in L1 - L2	Theory	20
A2	L4	1	Content / Topics covered in L1 - L4	Practical	40
A3	L7	1	Content / Topics covered in L5 – L7	Practical	40
				Total [A1 + A2 + A3]	**100**

Summative Assessment - Y

A4	Post L8	24	Content / Topics covered in L1 – L8	Practical: Live Project	**100**

Computation of Final Score: [X + Y]

- **X :** 20% of total marks obtained out of total marks 100 in Interim Formative Assessment
  cumulatively (A1+A2+A3)

- **Y :** 80% of marks obtained out of total marks 100 in Course-end Summative
  Assessment (A4)

Gradation Scheme:

- 90 – 100 : O - Outstanding
- 80 – 89   : A - Excellent
- 70 – 79   : B - Very Good
- 60 – 69   : C - Good
- 50- 59   : D – Pass

Eligibility for Certification:

- Attendance & active participation class lectures/interactions.
- Completion/submission of all the three activities/assignments as part of Formative Assessment [A1, A2 & A3].
- Obtaining minimum Grade D as per the formula for computation of Final Score stated above.

NB: A candidate must satisfy all the criteria mentioned in order to receive the course completion certificate.