ONE YEAR ADVANCED DIPLOMA IN CYBER SECURITY & DATA PROTECTION LAWS

Course Structure

Subject Code	Subject	Marks	Credits
	SEMESTER – I		
1.1.1.	**Law of Cyber Security**	100	5
1.1.2.	**Data Protection Laws in foreign Jurisdictions (US, UK, Canada, Singapore and European Union)**	100	5
1.1.3.	**Cyber security Concepts and Cryptography**	100	5
	SEMESTER - II		
1.2.4.	**Data Protection Law In India**	100	5
1.2.5.	**Cyber Security and Forensics LAB Sessions: - Digital Evidence Retrievals and Analysis Systems (DERAS)**	100	5
1.2.6.	**Open Source Intelligence (OSINT)**	100	5

1.1.1 LAW OF CYBER SECURITY

I. INTRODUCTION TO Cyber Jurisprudence

- Meaning of Law
- Sources of Law
- Hierarchy & Composition of the Indian Judiciary
- Civil Courts Structure and Procedures
- Criminal Court Structure and Procedures
- Understanding Cyber Space
- Defining Cyber Laws
- Internet Governance, ICANN, UDRP, INDRP
- Jurisdiction in Cyber Space

II. Understanding Law relating to Information and Technology

- Information Technology Act – An Overview
- The Indian Law of Contract - Construction of Electronic Contracts
- Issues of Security and Privacy
- Technical Issues in Cyber Contracts
- Security and Evidence in E-Commerce
  - Dual Key Encryption, Digital Signatures
  - Security issues in E-Commerce

III. E-Banking and Legal Issues

- Electronic Money
- Regulating e-transactions
- Role of RBI and Legal issues
- Transnational Transactions of E-Cash
- Credit Card and Internet
- Laws relating to Internet credit cards
- Secure Electronic Transactions
- RBI Security Framework Guidelines for Banks
- Guidelines for payment gateway providers
- SEBIs framework for stock market

IV. Law of Cyber Crimes

- Defining Crime, Classification of Cyber Crimes
- General Principles of Criminal Law applicable to Cyber Crimes
- Law relating to punishments in IPC and IT Act –
- Cyber Crimes:
    - Hacking, Phishing
    - Obscenity & Pornography, Child Pornography
    - Cyber Stalking
    - Theft of Identity
    - Cyber Defamation
    - Cyber Terrorism
    - Cyber warfare
    - Cyber Cheating
    - Data Diddling
    - Steganography
- Breach of Confidentiality and Privacy
- Offences of/by Companies
- Liability of Intermediaries including 2011 guidelines
- Deep web, Dark net
    - Cyber Investigation
    - Compoundable Offences
    - Powers of Police Officers
    - Law of Evidence in Cyber Crimes (Electronic Evidence)
    - Admissibility and relevancy of Electronic Evidence
    - Sec 65A, 65 B

V. Emerging and Contemporary Issues in cyber space

- Quantum Computing
- Artificial Intelligence
- IOT (Internet of things)
- BIGDATA
- Block chain technology

1.1.2. DATA PROTECTION LAWS IN FOREIGN JURISDICTIONS (US, UK, CANADA, SINGAPORE AND EUROPEAN UNION)

I. Historical Perspective of emergence of Data Protection laws in different countries General Data Protection regulation (GDPR)

- Application of GDPR guidelines to Indian Companies
- GDPR- Applicability, Data Protection Principles and Data Subject Rights, Exemptions and Derogations
- GDPR-Cross Border Transfer of Data, SCC, BCR
  GDPR-Compliance Obligations, DPIA, Privacy By Design,
  DPO, Remedies, Liabilities and Sanctions

TK v Asociatia de Proprietari bloc M5A-ScaraA: (Some CJE U Guidance on the Use of Video Surveillance in Apartment Buildings under EU Data Protection Law)

II. DIFC-Overview

Singapore PDPA-Applicability, Principles, Data Subject's Rights, Exemptions,
Singapore PDPA-Compliance Obligations
Challenges in Compliance of Multiple Data Protection Laws

III. Data Protection Law in UK:

- The Data Protection Act 2018
  - Meaning of certain terms used in the GDPR,Meaning of "controller", Meaning of "public authority" and "public body".
  - Lawfulness of processing, Lawfulness of processing: public interest etc,
  - Child's consent in relation to information society services
  - Special categories of personal data, and criminal convictions etc
  - Rights of the data subject
  - Restrictions on data subject's rights
  - Power to make further exemptions etc by regulations, Accreditation of certification providers,
  - Transfers of personal data to third countries etc
  - Specific processing situations
  - Principles, The first data protection principle, The second data protection principle, The third data protection principle, The fourth data protection principle, The fifth data protection principle, The sixth data protection principle
  - Representation of data subjects
  - Framework for Data Processing by Government
  - Offences and penalties

IV. Data protection laws in US

- HIPAA (Health Insurance Portability and Accountability Act
- **National Provider Identifier Standard.**
- **Transactions and Code Sets Standard.**
- **HIPAA Privacy Rule.**
- **HIPAA Security Rule.**

- **HIPAA Enforcement Rule.**
- CCPA- Applicability, Principles and Data Subject's Rights, Legitimate Interests, CCPA-Compliance Obligations, Notice, Consent, Legitimate Interest etc
- NDHM Regulatory requirement – August 28, 202

V. Data Protection laws in Canada

- Federal: Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA');
- British Columbia: Personal Information Protection Act, SBC 2003 c 63('BC PIPA');
- Alberta: Personal Information Protection Act, SA 2003 c P-6.5 ('AB PIPA'); and
- Quebec:Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 ('Quebec Private Sector Act').

1.1.3. CYBER SECURITY CONCEPTS AND CRYPTOGRAPHY

Protecting privacy and ensuring the security of data are more than only following government regulations. Organizations must develop sound data security policies to assist in preventing the unauthorized or unintentional disclosure of data. Data security breaches involving the financial information of customers are well publicized and, unfortunately, all too common. A robust privacy and data protection technologies – including an emphasis on cyber security and end-user best practices – can help avoid the costly consequences of data loss while protecting the company's reputation.

This paper helps to understand the technical aspects of Cyber Security and Data Protection concepts and frameworks in practice

I. Cyber Security Concepts

- Cyber Security Concepts: Cyber security issues, goals, architecture, attacks, Security Services and Mechanisms.
- Introduction to Cryptography: Network security model, Cryptographic systems,
- Crypt analysis, Steganography.
- Types of Cryptography: Symmetric key and Asymmetric Key Cryptography,
- Encryption and Decryption Techniques.
- Cryptographic Algorithms: Cryptographic hash, Message Digest, Data Encryption
- Standard, Advanced Encryption Standard, RSA, ECC (Introductory concepts only)

II. Cyber Security Threats and Vulnerabilities

- Overview of Security Threats and Vulnerability: Types of attacks on
- Confidentiality, Integrity and Availability.

- Vulnerability and Threats.
- Malware: Viruses, Worms, Trojan horses
- Security Counter Measures; Intrusion Detection Systems, Antivirus Software
- Ransoware, extortion

III. Ethical Issues in Information Security & Privacy

- Information Security, Privacy and Ethics
- Cyber Crime
- Hacking: Ethical issues
- Responsible vulnerability disclosure
- Privacy respecting security technologies and AI

IV. APPLICATION OF CYBER SECURITY

- System Security
- Desktop Security
- Dynamic and static source code testing
- Database Security
- Operating System Security: Designing Secure Operating Systems, OS Security

V. Cyber Security Audits, Vulnerability Assessment and Penetration Tests

- ISO 27001 Audits
- PCIDSS (Payment Card Providers)

VI. Security Management

- Disaster Recovery
- Digital Signature
- Ethical Hacking, Penetration Testing
- Computer Forensic

VII. Introduction to Cyber Forensic Tools – Virtual Lab

- EaseUS Data Recovery Wizard
- Wondershare Recoverit
- ICare Data Recovery

ONE YEAR ADVANCED DIPLOMA IN CYBER SECURITY & DATA PROTECTION LAWS

Semester – II

1.2.4. DATA PROTECTION LAW IN INDIA

I. Introduction to Data and Data Protection Laws:

- Definition of Data
- Kinds of Data
  - Public Data
  - Personal Data
  - Sensitive Personal Data
  - Health Data
  - Biometric Data
  - Meta Data
  - Big Data
- Data Principal and Data Fiduciaries

II. Data Protection Law in India:

- IT Act, 2000 and Data Protection
  - Sec 43A
  - Sec 72A
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("the IT Rules").

III. Non-Personal Data Governance Framework ('the NPD Framework'),

- Digital Information Security in Healthcare Act ('DISHA') – Health Data
  - central-level and a state-level digital health authority
  - privacy and security measures for digital health data
  - storage and exchange of electronic health data.
  - National Electronic Health Authority 'NeHA' at the central level
  - State Electronic Health Authority ('SeHA') at the State level

- Indian Constitution – Art -21
  - Judicial Decisions of Right to privacy and other related rights.
  - **Right to Privacy, Supreme Court Judgment, K.S. Puttaswamy v. Union of India,** 2017 (10) SCALE 1.
  - *R Rajagopal and Ors v. State of Tamil Nadu* [Writ Petition (Civil) No. 422 of 1994],
  - *Mr X v. Hospital Z* [Civil Appeal No. 4641 of 1998].
  - *Subhranshu Rout @ Gugul v. State of Odisha* [BLAPL No. 4592 of 2020],
  - *Sri Vasunathan v. the Registrar General, High Court of Karnataka and Ors* [General Writ Petition No. 62038 of 2016],
  - *Dharamraj Bhanushankar Dave v. State of Gujarat and Ors* [SCA No. 1854 of 2015]
  - Aadhar judgment

IV.Emergence of Data Protection Laws in India

A. Personal Data Protection Bill 2019

- Competition Commission of India and Ant trust regulation vis-a vis data protection,
- Sri Krishna Committee report, Existing Approaches to Data Protection, Understanding the Contours of the Indian Approach, Data Principals and
- Data Fiduciaries, Jurisdiction.

- Conceptual Understanding of Jurisdiction
- Prescriptive Jurisdiction .
- The Case for Data Non-Exceptionalism...
- Putative Bases for Jurisdiction .
- Retrospective and Transitional Application of the Data Protection Law
- Consent .
  - A revised operational framework for consent Consequences of such a Framework .
  - Enforcement of the Revised Framework.
  - Standard of Consent .
  - Different Standards for Different Types of Personal Data Processing .
  - Consent Dashboard and Avoiding Consent Fatigue.
  - Consent and Contractual Necessity
  - Protection of Children's Personal Data
  - processing of child's personal data in the GDPR.
  - The consent to the processing of child's personal data.
  - The methods to verify the legitimacy of the consent in the GDPR.
  - The different juridical regimes of the consent to the processing of personal data and of the consent concerning contracts in relation to a child.
  - The profiling of child's personal data. –
  - Identification of guardian data fiduciaries
  - Who is a child
  - Barred Practices.
  - Regulatory Approach .
  - Community Data.
  - Entities to which the Law Applies.
- Obligations of Data Fiduciaries
  - Amendments to the Aadhaar Act.
  - Amendments to the RTI Act.
  - SDPI (Sensitive personal Data or Information Rules 2011
  - NON-CONSENSUAL PROCESSING , Non-Consensual Grounds for Processing, Functions of the State, Compliance with Law or Order of Court or Tribunal
  - Exemptions... Security of the State. Prevention, Detection, Investigation and Prosecution of Contraventions of Law....
    : Enforcement

A. Structure and Functions of the (Data Protection Authorities)
B. The Regulated Entities: Classification and Obligations..
C. Data protection authority of India DPI
D. Government Data and risks to personal data
   a. Special categories of personal data
   b. Individual rights in processing personal data
   c. Restrictions on International Data transfers,

E. Data **Security and Data Breach**
F. **Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003**
G. Objective and broad scope (email, phone, SMS, automated calls, robocalls)

- Provisions relating to electronic marketing communications
- ICO Guidance on direct Marketing and Direct Marketing Commission Code
- DMA telephone preference services
- ICO services to the public- Reporting complaints and concerns Penalties for Data breach,
- Privacy notices, Subject access , Employment practices, CCTV, Data protection impact assessment.

1.2.5. CYBER SECURITY AND FORENSICS

This paper emphasises on Advance concepts of Cyber Security and Data Protection with practical orientation with help of Digital Evidence Retrievals and Analysis Systems (DERAS)– A Virtual Lab.

The primary purpose of the DERAS LAB is to equip enrolled student's with the knowledge, skills, and abilities to properly identify and seize digital evidence. Through a combination of lecture, demonstration, hands-on exercises, labs, and a practical exercise investigators learn how to seize digital evidence from a personal computer (PC) and notebook computer hard drives, floppy diskettes, compact disks (CDs), DVDs, thumb drives, various flash media, Cloud databases, Dedicated Servers, Virtual Data Storage Platforms etc. acquiring forensically valid images for digital evidence and retrieval processing.

Scientifically Authenticated Evidence determines legal proceedings immensely, In recent time's evidence emerge from IT and ICT utilization's as well, hence students of the course should understand the following

1. Digital formats of data storage media
2. The internal architecture of the existing Storage Medias
3. Data storage mechanisms on Digital Domain's (DD)
4. Data retrieval process both deleted and prevalent memory structure's
5. Analyzing the process of retrieved data etc.

I. Network and Cyber Security

- Network Security Model, Network Security Threats
- Firewalls: Overview, Types, Features, User Management
- Intrusion Detection System, Intrusion Prevention System
- Public Key Infrastructure, Digital Signature Schemes

II. Internet and Web Application Security

- Email security: PGP and SMIME
- Web Security: Web authentication, Injection Flaws, SQL Injection
- Web Browser Security
- E-Commerce Security
- Wireless Network Security

- Wireless Network Components
- Security issues in Wireless Networks
- Securing a Wireless Network
- Mobile Security

III. Understanding World of Deep and Dark Web

- Understand the complete working, terminology and be able to have a complete understanding about the Deep/Dark web.
- To access the Deep web as well as the Dark web with Complete Ease and total security.
- To visit some advanced and famous websites located on the Hidden Web(Deep and Dark Web).
- Understanding Working, Trading, Buying, Selling as well as Mining CRYPTOCURRENCIES.
- About the Dangers as well as precautions to be taken care of while surfing the Web.
- Use Darknet Email services.
- Anonymously access the dark net and TOR hidden services (onion services)

LAB SESSIONS: - DIGITAL EVIDENCE RETRIEVALS AND ANALYSIS SYSTEMS (DERAS)

DERAS Lab tools:

1. Linux Based VAPT tools

DEFT: Digital Evidence Forensic Tools Kit (Kali Linux)

Disk Identification/spacing/structuring tools

- fdisk -lu
- fls/dev/sdb1

Mounting tools

- mount /dev /sdb1 /home/urmika/moun
- unmount moun

Imaging tools

- dd if = /dev/sdb1 -of = /sdb1.iso
- ddrescue /dev/sdb1 /home/urmika/rescue.iso

Hashing tools :

- md5sum /dev/sdb1 -> md5.txt
- sha1sum /dev/sdb -> sha1.txt

Carving tools

- foremost -t jpg -o /home/urmika/foremost rescue.iso (by using the -t jpg command, only the jpg files were retrieved from the iso file)
- bulk_extractor -o /be dev/sdb1 (the extracted histograms were saved in the "be" drive)

Analysis tools

Various Autopsy tool of DEFT 8.2 to analyses the retrieved data.

2. Network Forensics tools

- Wireshark
- MITMPROXY
- Burpsuite

1.2.6. Open source intelligence (OSINT)

I. Foundations of OSINT

- Overview of OSINT
  - What is OSINT?
  - Who uses OSINT and why?
- The Intelligence Process
  - What is it and how does it apply to OSINT?
- Creating and Understanding the OSINT Process Stages
- Goals of OSINT Collection
- Setting Up an OSINT Platform
  - Using virtual OSINT systems and mobile emulators
  - Understanding issues that could decrease investigator anonymity
  - Using VPNs for OSINT work
  - Leveraging different web browsers and browser add-ons and extensions
- Documentation
  - How to record data within OSINT investigations
  - Examination of link analysis tools, Mind Map applications, and activity-recording programs
- Sock Puppets
  - What is an OSINT sock puppet or false identity?
  - When and how to use sock puppets effectively in investigations
  - How to create a sock puppet

    - Issues that could get your sock puppet account disabled
- Data Analysis
    - How to analyze data obtained from the Internet
    - Types of logic and reasoning
    - Identification of and methods to reduce logical fallacies and bias
    - Network theory and link analysis techniques

II. Core OSINT Skills

- Leveraging Search Engines
    - Preparation for using search engines
    - Using advanced search operators
- Harvesting Web Data
    - Techniques and tools to download files from Internet sources
- File Metadata Analysis
    - Extracting and validating metadata from files
- Reverse Image Searching
    - What reverse image searching is and how to use it in OSINT investigations
- Image Analysis
    - How to analyze images to geolocate and extract meaningful data points
- Imagery and Maps
    - Exploration of how to use maps and imagery in OSINT work
    - Comparison of different imagery data sources
- Language Translation
    - Multiple methods of extracting and translating foreign text

III. Business and Dark Web OSINT

- Business OSINT
    - Analyzing online business registrations and documents
    - Examining the resources companies use in their work
- Surface, Deep, and Dark Webs
    - What are they and why does it matter in OSINT work?
- Overview of Several Dark Webs
    - Comparison of a few major dark web networks, why people use them, and how to perform OSINT in those networks
- Tor

- What is Tor?
- How can it be used by investigators and by their targets?
- Techniques for investigating data found in Tor

- OSINT Automation
  - Using applications to work more efficiently
- Breach Data
  - Ethical analysis of breach data use
  - Investigation into how breach data can augment OSINT work

IV. Open Source Intelligence Tools demonstrated on DEFT 8.2 Forensic tool kits are

- **Maltego**
- **Recon-ng**
- **theHarvester**
- **Shodan**
- **Google dorks**