



**NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY, ASSAM**

**PROGRAMME: B.A., LL.B. (HONS.)FYIC**

**DETAILS OF COURSE OFFERED**

**EVAN SEMESTER (VIII) – ACADEMIC YEAR:.....**

| <b>SL. NO</b> | <b>COURSE CODE</b>   | <b>COURSE TITLE</b>       | <b>L</b>                  | <b>T/P</b>                | <b>CR</b> | <b>CH</b> |
|---------------|--|---------------------------|---------------------------|---------------------------|-----------|-----------|
| <b>1</b>      | <b>BL806.7<br/>(CRIMINAL LAW,<br/>SPECIALIZATION<br/>GROUP PAPER –<br/>IV)</b> | <b>IT<br/>OFFENCES-II</b> | <b>4<br/>PER<br/>WEEK</b> | <b>1<br/>PER<br/>WEEK</b> | <b>4</b>  |           |

- A. CODE AND TITLE OF THE COURSE: BL806.7, CRIMINAL LAW, SPECIALIZATION GROUP PAPER- IV ), IT OFFENCES-II**
- B. COURSE CREDIT: 4 (TOTAL MARKS : 200 MARKS)**
- C. MEDIUM OF INSTRUCTION: ENGLISH**
- D. COURSE COMPILED BY: THANGZAKHUP TOMBING**
- E. COURSE INSTRUCTOR: THANGZAKHUP TOMBING**

## 1. COURSE OBJECTIVES

In an inter-connected world through the World Wide Web the possibility of trade and commerce has become almost limitless, homogenous and at the same time highly complex and exploitative. Soft powers and IT knowledge is the mainstay in the 21<sup>st</sup> century. Social media platforms like facebook, whatsapp, Instagram, twitter, podcast etc are the most effective for connecting people but they are also the most pervasive platform for generating big data, spreading, tainted, manipulated, communalised and fake news. It is imperative that there is robust international cooperation and regulations to combat, caution, address and redress upcoming global cyber-crime menace.

## 2. TEACHING METHODOLOGY

The course will be taught on theory based, class discussion, handing out of assignments and seminars for holistic learning.

## 3. COURSE LEARNING OUTCOMES

By the end of the course students will have sound knowledge of the complex yet intricate aspects of Global cyber-crime from perspective of soft power, issues of sovereignty and interconnected and overlapping of cyber offence for research as well for practice as sound legal practitioner in the ever widening field of cyber- crime.

## 4. COURSE EVALUATION METHOD

The course shall be assessed for 200 marks. The Evaluation scheme would be as follows:

Internal assessment: 70% (140 marks)

Semester End Examination: 30% (60 marks)

| Sl. No. | Marks Distribution       |          |
|---------|--------------------------|----------|
| 1       | Project Work             | 40 marks |
| 2       | Seminar/Group Discussion | 20 marks |
| 3       | Assignment/Assessment    | 30 marks |
| 4       | Mid-Semester Test        | 40 marks |
| 5       | Attendance in class      | 10 marks |
| 6       | Semester End Examination | 60 arks  |

## 5. DETAILED STRUCTURE OF THE COURSE (SPECIFYING COURSE MODULES AND SUB-MODULES)

### MODULE I

- Cyber Jurisprudence at International and Indian Level
- Cyber Law - International Perspectives

- UN & International Telecommunication Union (ITU) Initiatives
- Council of Europe - Budapest Convention on Cybercrime
- Asia-Pacific Economic Cooperation (APEC)
- Organization for Economic Co-operation and Development (OECD)
- World Bank

## **MODULE II**

- Commonwealth of Nations
- Different offences under IT Act, 2000 v. Global IT offences
- Dispute Resolution in Cyberspace
- Concept of Jurisdiction

## **MODULE III**

- Indian Context of Jurisdiction and IT Act, 2000.
- International Law and Jurisdictional Issues in Cyberspace.
- Dispute Resolutions

## **MODULE IV**

- Freedom of Speech and Expression in Cyberspace- social media v. mainstream media
- Challenges of Mob lynching, fake news and the Global world
- Right to Access Cyberspace – Access to Internet
- Right to Privacy • Right to Data Protection

## **6. PRESCRIBED READINGS**

W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves* (Reprint edition ed. 2011).

John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation* (2008).

Jaishankar, K. (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour* (New York: CRC Press/Taylor Francis, 2014).

Jonathan Rosenoer, *Cyber Law*, Springer, New York, (1997).  
Yar, M. *Cybercrime and Society* (London: Sage, 2013, 2nd ed.)

Dan Pyle Millar & Robert L. Heath, *Responding to Crisis: A Rhetorical Approach to Crisis Communication* (2003).

Justice Yatindra Singh, *Cyber Laws*, Universal Law Publishing Co, New Delhi, (2012).

S. R. Bhansali, *Information Technology Act, 2000*, University Book House Pvt. Ltd., Jaipur (2003).

Chris Reed & John Angel, *Computer Law*, OUP, New York, (2007).

Taylor, R. W., E. J. Fritsch and J. Liederbach, *Digital Crime and Digital Terrorism* (New Jersey: Prentice Hall Press, 2014, 3rd ed.)

Vasu Deva, *Cyber Crimes and Law Enforcement*, Commonwealth Publishers, New Delhi, (2003).

Jewkes, Y. and M. Yar (eds.) *Handbook of Internet Crime* (Cullompton: Willan Publishing, 2010)

Lloyd, I, *Information Technology Law*, Oxford University Press Blackstone's Statutes on IT and E-Commerce, Oxford University Press.

Verma S, K, Mittal Raman, *Legal Dimensions of Cyber Space*, Indian Law Institute, New Delhi, (2004)

Sudhir Naib, *The Information Technology Act, 2005: A Handbook*, OUP, New York,(2011)