

## Cyber Security

1.1 Course Number: CS431

1.2 Contact Hours 3-0-0 Credits: 9

1.3 Semester-offered: 4<sup>th</sup> Year-Even

1.4 Prerequisite: None

1.5 Syllabus Committee Member: Dr. Sushum Biswas, Dr. Daya Sagar Gupta & Dr. Gargi Srivastava

2. **Objective:** This subject focuses on cyberthreats and cybersecurity, provides the much needed awareness in the times of growing cybercrime episode. The course provides adequate orientation on laws in reference to cybercrime and cybersecurity taking into account the Indian as well as global scenario.

3. **Course Content:**

Unit-wise distribution of content and number of lectures

Unit	Topics	Sub-topic	Lectures
1	Introduction	Introduction. Phenomenon of cybercrime: Definitions, topology of cybercrime, development of computer crime and cybercrime	6
2	Cyber Offence	Extent and impact of cybercrime offences, Offences against the confidentiality, integrity and availability of computer data and systems, Content-related offences, Copyright and trademark related offences, Computer-related offences, Combination offences.	9
3	The challenges of fighting cybercrime	Opportunities, general challenges, and legal challenges. Capacity building: Cybersecurity and cybercrime, Capacity building methodology	10
4	Policies	Strategy as a starting point, the relevance of policy, the role of regulators in fighting cybercrime, high standards in developing countries, Overview of activities of regional and international organizations	9
5	Legal response	Definitions, substantive criminal law, digital evidence, jurisdiction, procedural law, international cooperation, Liability of Internet providers	6
		<b>Total</b>	<b>40</b>

#### **4. Readings**

4.1 Textbook: Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, By Nina Godbole and Sunit Belapure , Wiley India.

4.2 Reference books: Cybersecurity: Understanding cybercrime, phenomenon, challenges, and legal response ITU Report, November' 2014

#### **5 Outcome of the Course:**

- Understand, appreciate, employ, design and implement appropriate security technologies and policies to protect computers and digital information.
- Identify & Evaluate Information Security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios
- Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection