

<b>Semester: 4</b>	<b>Course No.: 402</b>	<b>Course Code: FTM209-2C</b> <b>Course Title: Cyber Security and laws</b>
<b>Credits: 4</b>	<b>Course Category: MAJOR COURSE</b>	

**Course Outcomes: On successful completion of the course the learner will be able to**

<b>CO#</b>	<b>COGNITIVE ABILITIES</b>	<b>COURSE OUTCOMES</b>
<b>CO1</b>	<b>REMEMBERING</b>	Identify key terms and basic concepts of cyberspace, cyber threats, and cyber laws.
<b>CO2</b>	<b>UNDERSTANDING</b>	Explain the evolution of IT laws, types of cyber crimes, and challenges in cyber governance.
<b>CO3</b>	<b>APPLYING</b>	Apply cyber security principles to real-world scenarios like data protection, e-governance, and e-commerce.
<b>CO4</b>	<b>ANALYSING</b>	Analyze cybercrime cases and evaluate legal frameworks and regulatory loopholes.
<b>CO5</b>	<b>EVALUATING</b>	Critically assess national cyber policies, legal procedures, and digital evidence management.

<b>Unit No.</b>	<b>Unit Contents</b>	<b>Sessions Allotted</b>
<b>1</b>	<b>Introduction to Cyber Security and Cyber World</b> <ul style="list-style-type: none"> <li>• Defining Cyberspace and Overview of Computer and Web Technology</li> <li>• Architecture of Cyberspace</li> <li>• Communication and Web Technology</li> <li>• Internet and World Wide Web: An Introduction</li> <li>• Advent of the Internet</li> <li>• Internet Infrastructure for Data Transfer and Governance</li> <li>• Internet Society and the Global Connectivity Landscape</li> <li>• Regulation of Cyberspace: National and International Perspective</li> <li>• Concept of Cyber Security</li> <li>• Issues and Challenges of Cyber Security</li> <li>• Introduction to the Cyber World</li> <li>• Comparison: Cyber Security vs. Cyber Law</li> <li>• Types of Cyber Threats: Malware, Phishing, Ransomware, Social Engineering, etc.</li> </ul>	<b>12</b>
<b>2</b>	<b>Cyber Forensics, Cyber Crimes and Prevention Techniques</b> <ul style="list-style-type: none"> <li>• Definition, Classification of Cyber Crimes vs. Traditional Crimes</li> <li>• Common Cyber Crimes: <ul style="list-style-type: none"> <li>a) Data Theft, b) Hacking, c) Viruses/Worms, d) Phishing</li> <li>e) Cyber Stalking/Bullying, f) Identity Theft, g) Credit Card &amp; Banking Frauds</li> <li>h) Cyber Defamation, i) Illegal Selling/Gambling</li> <li>j) DoS Attacks, k) Cyber Terrorism, l) Software Piracy</li> </ul> </li> <li>• Reasons for Cyber Crimes; Methods of Execution</li> <li>• Prevention of Cyber Crimes &amp; Frauds</li> <li>• Critical Analysis &amp; Loopholes in IT Act, 2000</li> <li>• Freedom of Speech &amp; Human Rights in Cyberspace</li> </ul>	<b>14</b>
<b>3</b>	<b>Cyber Law</b> <ul style="list-style-type: none"> <li>• Evolution, Genesis &amp; Features of IT Act, 2000</li> <li>• Authorities, Powers, Penalties &amp; Offences under the Act</li> <li>• Business Issues in Cyberspace: IMs, Social Media, Mobile Apps, IoT</li> <li>• Domain Name Disputes &amp; Resolution</li> </ul>	<b>14</b>

	<ul style="list-style-type: none"> <li>• E-Forms, E-Money, RBI's PPI Regulations</li> <li>• E-Money Transfer, Data Privacy &amp; Secure Operations</li> <li>• E-Commerce &amp; Indian Laws: <ul style="list-style-type: none"> <li>a) Digital Signatures, b) E-Commerce Provisions, c) E-Governance</li> <li>d) E-Taxation, e) E-Contracts, f) Cyber Tribunal</li> </ul> </li> <li>• IPR in Cyberspace: <ul style="list-style-type: none"> <li>a) Trademarks, b) Cyber Squatting, c) Hijacking, d) Jurisdiction</li> <li>e) Copyright (Digital &amp; Software), f) WIPO Treaties, g) Patent Rights</li> </ul> </li> </ul>	
<b>4</b>	<b>Electronic Records</b> <ul style="list-style-type: none"> <li>• Authentication of Electronic Records</li> <li>• Legal Recognition of Electronic Records</li> <li>• Legal Recognition and Use of Digital Signatures</li> <li>• Applications of Electronic Records and Digital Signatures in Government and Agencies</li> <li>• Retention of Electronic Records</li> <li>• Intermediaries and Their Liabilities</li> <li>• Attribution, Acknowledgement, and Dispatch of Electronic Records</li> <li>• Secure Electronic Records and Digital Signatures</li> </ul>	10
<b>5</b>	<b>Cyber Security Management, Compliance and Governance</b> <ul style="list-style-type: none"> <li>• Cyber Security Planning and Policy Formulation</li> <li>• Cyber Crisis Management Plan (CCMP)</li> <li>• Business Continuity Planning (BCP)</li> <li>• Cyber Risk Assessment Techniques</li> <li>• Types of Security Controls and Their Objectives</li> <li>• Cyber Security Audit and Compliance Requirements</li> <li>• National Cyber Security Policy and Strategic Framework</li> <li>• Governance Mechanisms and Global Best Practices</li> </ul>	10

**Suggested Text Books:**

1. **Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives – Nina Godbole & Sunit Belpure**
2. **Cyber Law in India – Pavan Duggal**
3. **Information Technology Law and Practice – Vakul Sharma**
4. **Cyber Laws – Justice Yatindra Singh**

**Suggested Reference Books:**

- **Cyber Crime and Security – Alka Kalra**
- **Introduction to Information Security and Cyber Laws – Surya Prakash Tripathi, Ritendra Goyal, and Praveen Kumar Shukla**
- **Information Security: Principles and Practice – Mark Stamp**
- **Cyber Security Essentials – Charles J. Brooks et al.**