AMITY UNIVERSITY

UTTAR PRADESH

Course Title: **Cyber and Information Security**

Credit Units:

L	T	P/S	SW/FW	TOTAL CREDIT UNITS
3	0	0	0	3

Course Level: UG
Course Code: IT415

Course Objectives:

- To provide a broad understanding of Cyber and Information Security.
- To provide the student with basic knowledge of cybercrime dynamics, cyber law & Intellectual property issues; explore legal & policy developments for dealing fraud using Cyber space.

Pre-requisites: NIL

Course Contents/Syllabus:

	Weightage (%)
Module I	**20%**
Descriptors/Topics • Introduction to Information, Computer and Network Security, • Security Concepts, kinds of security breaches, • Threats and Risks, Point of vulnerability, • Attacks- Passive and Active, Security Services, Confidentiality, Authentication, Non-Repudiation, Integrity, Access Control, Availability, • Model for Internetwork Security, Internet Standards and RFCs	
Module II	**20%**
Descriptors/Topics • Sources of security threats, Motives, Target Assets, • Consequence of threats, E-mail threats, Web threats, Hacking, Intruders, Insider threats • Cyber Squatting, Cyber Stalking, Crime of deception, Content Oriented Online Crime, Malicious Software use and detection, • Cyber Terrorism, Information warfare and surveillance, Virtual Crime, Online Frauds • Identity Theft and Intellectual property theft, Network threats-Worms, Virus, Spam's, Ad-ware, Spy ware, • Trojans and convert Channels, Backdoors, Bots, IP spoofing, ARP spoofing, • Session hijacking, Sabotage, phishing, Zombie/Zombie Drone.	

Module III	
Descriptors/Topics • Security Engineering: Security Threat Management, Risk Assessment, • Introduction to Cyber Forensics, Evaluation of crime scene & evidence collection, • Security Policies, Risk Management, Procedure and Guidelines. • Cyber Laws: Advantages, cyber lawyers, Jurisdiction and Sovereignty. • The IT Act of India 2000 • Intellectual property rights, Ownership & Enforcement of IPR • Defenses for Infringement • Copy right objective , Transfer of copy right, practical aspect of licensing • Benefits, jurisdictional Issues, copy right in digital media, patents in cyber world	**20%**
Module IV	
Descriptors/Topics • Introduction to Cryptography • E-Commerce Security • Message Authentication, Hash functions, Hashes and Message Digests • Number Theory for Information Security • Public Key Algorithms , Public-key Infrastructure, PKI Applications • Cryptographic Protocols, Digital Signature • Digital Watermarking and Steganography • Biometric Security • Encryption, Symmetric Key Encryption, Data Encryption Standard (DES), Kerberos	**20%**
Module V	
Descriptors/Topics • Introduction to Security Risk Management, risk assessment, • Security Assurance Approaches: OCTAVE and COBIT approaches. • Security Management of IT Systems: Network security management, Firewalls, IDS and IPS configuration management. • Web and wireless security management. • Security Models, Access control models, role-based and lattice models. • Computer security log management, malware handling and vulnerability management programs. • Specifying and enforcing security policies, • Information security audit and principles of audit. • Information Security Standards and Compliance: Overview of security standards ISO 17799 Standard, Legal and Ethical issues, PCI DSS	**20%**

Student Learning Outcomes:

- Recognize Cyber Crimes and Information Security Issues.
- Explain existing Cyber Laws.
- Interprets Intellectual Property Rights.
- Identify standards related to information security

Pedagogy for Course Delivery:

The course would be covered under theory. It incorporates designing of problems, analysis of solutions submitted by the students groups and how learning objectives were achieved. Continuous evaluation of the students would be covered under quiz, viva etc.

Assessment/ Examination Scheme:

Theory L/T (%)	Lab/Practical/Studio (%)	Total
100%	NA	100%

Theory Assessment (L&T):

Continuous Assessment/Internal Assessment					End Term Examination
Components (Drop down)	Mid-Term	Home Assignment	Presentation/Viva	Attendance	
Weightage (%)	10%	8%	7%	5%	70%

Text Reading:

- Cryptography and Information Security: V.K. Pachghare, PHI
- Cyber Laws and IT Protection: Harish Chander, PHI
- Slay, J. and Koronios, A., IT Security and Risk Management, Wiley, 2006.
- Hossein Bidgoli, Information Security, Volume 3, Threats, Vulnerabilities, Prevention, Detection, and Management, Wiley, 2006
- Mark Merkow, Information Security : Principles and Practices, 1/e, Pearson Education
- Marjie T. Britz, Computer Forensics and Cyber Crime : An Introduction, 2/e, Pearson Education

References:

- William Stallings, Network Security Essentials (Applications and Standards) Pearson Education.
- Ortmeier, P. J. Security Management: An Introduction, 2nd edition, Prentice Hall., 2005
- Skoudis, Ed & Zeltser, and Lenny Malware: Fighting Malicious Code. Second Ed. Prentice Hall PTR., 2004

- Skoudis, Ed & Liston, Tom, Counter Hack Reloaded, Second Edition. Prentice Hall PTR. Plano, TX , 2006
- Wall, David, Cybercrime: The Transformation of Crime in the Information Age. Polity Publishing , 2007
- Ross J Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2008