III YEAR SEM-1IB.Tech CSE	ELECTIVE	L	T	P	C
CODE: CS3607	CYBER SECURITY	2	2	0	4

COURSE OBJECTIVES	
1.	To understand basics of Cyber Security and its legal aspects.
2.	To be able to do Risk Assessment.
3.	To understand the Policies, Standards and Procedures to provide Information Security.
4.	To learn the concepts of UNIX and Windows Security.

SYLLABUS:

UNITI(Basics of Cyber Security and Legal Aspects)
History of Information Security, Understanding security, CNSS security model, Security in SDLC, Types of threats and attacks, Principles of Information Security, Laws and Ethics for Information Security, Introduction to IT ACT, International Laws and Legal bodies.

Unit II (Assets, Security Policies, Standards and Disaster Recovery)
Asset, Asset classification, Understanding the basics of Information Security Policy, Standards and Practices, Types of Policies, Policy development process, ISO 27001, NIST Security Model, Business Continuity Planning, Disaster Recovery, Maintaining Backups.
.

Unit III (Risk Assessment and Access Controls)
Identification, Assessment, Analysis, Control of Risk, Quantitative vs Qualitative Risk Management, FAIR approach to risk assessment, NIST Risk management framework, Authentication vs Authorization, Types of authentication, Understanding different types of Access Controls(ACLs, RBAC, RUBAC etc.).

Unit IV (System and Web Application Security)
UNIX security, Windows security, Active VS Passive attacks, Information Gathering -Analysis of HTTP Get and Post method, Crawling, Robot.txt file, Server fingerprinting, OWASP Top 10,

UNIT V
Causes and prevention of Overflow attacks, SQL injection, Cross Site Scripting, Whitelisting vs Blacklisting, Mobile Devices risks, Blue jacking,

Unit VI (Physical Security and Information Security Maintenance)
Physical Vulnerability Assessment, Securing Assets, Physical Intrusion Detection, Procedures and Methods to maintain the implemented information Security.

RESOURCES:

Video Lectures
http://nptel.ac.in/courses/106106129/lecture by Prof. V. Kamakoti IIT Madras
https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/ lecture by various professors of MIT.

Text Books
1. Principles of Information Security, Whitman, Thomson
2. Information Security: The complete reference, Mark Rhodes-Ousley, TMH
3. Hack proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn IdoDubrawsky, Steve W.Manzuik and Ryan Permeh, wileyDreamtech

Reference Books
1. Ethical Hacking and Penetration Testing Guide by RafayBaloch
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
3. Hacking Exposed 7: Network Security Secrets and Solutions by Stuart McClure , Joel Scambray, George Kurtz.

OUTCOMES:

After successful completion of the course, the learners would be able to

1. Analyze any organization for Information Security loopholes.
2. Implement Information Security framework for an organization.
3. Learn and understand the legal aspects of Information Security.
4. Identify the Information Security risk and their solutions.