<table>
<tr><td>Course Title</td><td>Computer and Network Security</td><td>Course No</td><td colspan="4">old COM505</td></tr>
<tr><td rowspan="2">Department/ Specialization</td><td rowspan="2">Computer Science and Engineering</td><td rowspan="2">Credits</td><td>L</td><td>T</td><td>P</td><td>C</td></tr>
<tr><td>3</td><td>1</td><td>0</td><td>4</td></tr>
<tr><td>Faculty proposing the course</td><td>Noor Mahammad Sk</td><td>Status</td><td colspan="2">Core □</td><td>Elective</td><td>■</td></tr>
<tr><td>Offered for</td><td>M.Tech, PhD - CSE, ECE, Mechanical</td><td>Type</td><td colspan="2">New □</td><td>Revision</td><td>■</td></tr>
<tr><td>To take effect from</td><td></td><td rowspan="2">Submitted for approval</td><td colspan="4" rowspan="2">____ Senate</td></tr>
<tr><td>Prerequisite</td><td>Computer Networks, Operating System</td></tr>
<tr><td>Learning Objectives</td><td colspan="6">The course covers principles of computer systems and network security. Discussion about various attack techniques and how to defend against them. Topics include network attacks and defenses, intrusion detection and prevention, computer and network forensics, firewall and content filtering, security issues in the wireless and sensor networks.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="6">Students can understand the need for security. Can able to understand the vulnerability, threat and attack. Functions of the security appliances.</td></tr>
<tr><td>Course Contents (with approximate breakup of hours for lecture/ tutorial/practice)</td><td colspan="6">Introduction to Computer Network Security: Introduction, securing the computer networks- hardware/software, forms of protection, security standards; Sources of vulnerabilities and its assessment (4 hrs)

Security challenges, Assessment, Analysis and Assurance: sources of security threats, threat motives, management and correlation and security threat awareness; System security policy, Building a security policy, security requirement specification, Threat Identification and analysis, Vulnerability identification and assessment and security monitoring and auditing; Disaster Management, Resources for disaster planning and recovery (6hrs+4T).

Access Control, Authorization and Authentication: Access - Rights, Control systems; authorization- mechanisms, types, principles, and granularity; Authentication - factors and effectiveness, elements, types, methods and policy (4 hrs+2T).

Cryptography: Symmetric Encryption, public key encryption, enhancing security and Key management; Public key Infrastructure, hash function and digital signatures (4 hrs).

System Intrusion Detection and Prevention: Intrusion detection mechanism, systems, types; Response to system intrusion, challenges to intrusion detection systems and implementations; Intrusion prevention systems (4 hrs).

Computer and Network Forensics: Computer forensics, network forensic and forensics tools (2 hrs + 2T).

Firewall, Virus and Content Filtering: firewall- types, configuration, implementations and limitations; Scanning, Filtering and blocking; Virus filtering and content filtering (4 hrs+2T).

Computer Network Security Protocols: Application Level Security, Security in the Transport Layer, Network layer, Link layer and over LANs (6 hrs).

Security in Wireless Network and Devices: WLAN security concerns and best practices</td></tr>
</table>

	for WI-FI security (4 hrs). **Security in sensor networks**: Challenges, vulnerabilities and attacks, security mechanisms and best practices for sensors (4 hrs).
Essential Reading	1.Joseph Migga Kizza, A Guide to Computer Network Security, Springer Publisher, Second Edition, December 2008.
Supplementary Reading	1. Nong Ye, Secure Computer and Network Systems Modeling, Analysis and Design, Wiley Publishers, First Edition, February 2008. 2. Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, October 2004. 3. Cheswick, Bellovin, and Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition*, Addison-Wesley Professional, 2003.