SPRINGFIELD TECHNICAL COMMUNITY COLLEGE

ACADEMIC AFFAIRS

Course Number: PROG-350 Department: ______________________

Course Title: Internet/Network Security 1 Semester: Fall Year: 2003

Course Objective	Competencies
1. To teach student how to protect data 2. To have the student understand many types of computer security/Network threats 3. To teach students data encryption/decryption techniques 4. To get hands on skills with many popular security tools 5. To be able to secure data on a windows operating system platform 6. To setting up procedures and policies to protect the network and data 7. To have the student assess computer and network vulnerabilities	• Define and understand the following: • Identification, Authentication, non-repudiation • Account creation & termination (user access rights administration) • Biometric hardware/software used in conjunction with access control systems • Passwords (e.g. cracking/defensive cracking, guidelines for good passwords) • Access Control List/Access Control Matrix • File system permissions • Multilevel security (e.g. subject clearance levels) • Audit logs • Wireless technology • E-mail servers, routers, remote system access • Protocols: TCP/IP, Secure Sockets Layer, Secure Electronics Transaction • Telephony & Private Branch Exchange (PBX) security • Treats: (e.g. eavesdropping/wiretapping, traffic analysis, replay attacks, electromagnetic radiation interception, scanners, sniffers, Domain Name Server attacks. IP

Course Objective	Competencies
	spoofing, Denial of Service/Distributed Denial of Service attacks • Terminology (e.g. plaintext, ciphertext, cryptanalysis, key, algorithm, block cipher, stream cipher) • Symmetric cipher systems (e.g. Data Encryption Standard, Advanced Encryption Standard) • Asymmetric cipher systems (e.g. RSA algorithm, Diffie-Hellman) • E-mail encryption (e.g. Pretty Good Privacy) • Digital signatures • Digital certificates • Public Key Infrastructure (PKI) • Memory (e.g. random access memory, read only memory, cache, proxy cache) • Evaluation criteria (e.g. Trusted Computer System Evaluation Criteria, Common Criteria) • Availability • Object classification levels • Controls (prevent, detect, recover) • Separation of duties • Least privilege • Social engineering • Malicious code: Trojan Horses, Viruses, (e.g. boot sector, program (file), macro), Bombs (e.g. logic, time), Trapdoors, Worms, Controls (e.g. prevention/inoculation, anti-virus policy/software, backups)

Course Objective	Competencies
	• Security policies & procedures development (evaluate, develop, document, communicate, and implement) • Risk Analysis/Risk Assessment • Auditing (e.g. policies, guidelines, procedures) • Security monitoring, testing & evaluation • Security reviews & spot monitoring • Security maintenance • Security education and awareness • Physical Security (e.g. Fire suppression; guards; locks; alarms; disposal of sensitive media) • Understanding of security goals (confidentiality, integrity, availability, authentication, non repudiation) • Knowledge of system security tools & applications • NT Administration (e.g. setting registry keys, setting up a safe file system, secure account policies, backups, auditing monitoring and responding to incidents)