C-S/455 Fundamentals of Information Security
Student Learning Outcomes

Security Concepts
1.1 Students are able to define the concepts of confidentiality, availability and integrity as they relate to information security.
1.2 Students are aware of the relationships and tradeoffs among confidentiality, availability and integrity.
1.3 Students are able to define the concepts of authentication, non-repudiation, access control and privacy.
1.4 Students are aware that security applies to hardware, software and data.
1.5 Students can define the following basic information security terms: threats and vulnerabilities, risk analysis, cost benefit analysis, attacks, exploits, controls.
1.6 Students can categorize different strategies in the following methods of defense detection, recovery, deflection, deterrence, prevention.
1.7 Students can define and apply the Principle of Weakest Link.
1.8 Students are aware of the essential role of trust in any security policy or practice.
1.9 Students can explain the relationship between trust and information assurance.
1.10 Students can explain the concepts of sophisticated attackers and script kiddies and their differences.

Security Management
2.1 Students can explain the difference between security policy and practice.
2.2 Students can construct a comprehensive information security policy based on environmental characteristics.
2.3 Students can select appropriate practices for typical security policies.
2.4 Students can explain the role of risk analysis and risk mitigation and their importance in risk management.
2.5 Students can perform a basic risk analysis.
2.6 Students can perform basic security planning, including physical security and technological security.
2.7 Students are aware of common social engineering attacks and can prescribe associated mitigation techniques.

Encryption
3.1 Students can explain the different cryptographic techniques required to preserve integrity, confidentiality and authenticity.
3.2 Students can define encryption, decryption, plain text, cipher text, and can explain their role in cryptography.
3.3 Students can explain and identify keys, when used in cryptographic ciphers.
3.4 Students can explain and identify the difference between a stream cipher and a block cipher.
3.5 Students can define cryptanalysis, apply simple cryptanalysis and explain its implication for the success of failure of cryptographic algorithms.
3.6 Students can define, identify and offer simple examples of substitution ciphers.
3.7 Students can define, identify and offer simple examples of transposition ciphers.
3.8 Students can define, identify and offer simple examples of product ciphers.
3.9 Students can design a one-time pad cipher and explain its usefulness and limitations.
3.10 Students can explain the Shanon characteristics of good ciphers.
3.11 Students can analyze the quality of cryptographic algorithms using confusion, diffusion and unicity distance as metrics.
3.12 Students are aware of the basics, especially the concept of rounds, in Fiestel ciphers.
3.13 Students are able to explain the advantages, disadvantages, and applications of symmetric encryption.
3.14 Students are aware of the applications and limitations of the DES algorithm.
3.15 Students are aware of the applications and advantages of the AES algorithm.
3.16 Students can explain the difference between symmetric and asymmetric (PKI) encryption, can identify proper uses for each, and identify well-known algorithms of each type.
3.17 Students can design the basic mechanisms required to form a public key encryption, as described in the Diffie-Hellman PKI concept.
3.18 Students can explain the basics of the RSA algorithm.
3.19 Students can construct a cryptographic hashing algorithm.
3.20 Students can explain the proper situations for applying cryptographic hashing.
3.21 Students can explain the need for key exchange protocols.
3.22 Students can design security symmetric authentication protocols.
3.23 Students can design security asymmetric authentication protocols.
3.24 Students can explain the purpose and fundamental protocols for network certificates.
3.25 Students can design an algorithm for constructing and using digital signatures.
3.26 Students are aware of steganography.
3.27 Students can write software that utilizes encryption, hashing and digital signatures.

Software Security
4.1 Students can explain how boot sectors, buffer overflows and memory leaks can be vulnerable to security attacks.
4.2 Students can offer examples of common computer viruses and their impact.
4.3 Students can utilize software to scan for the presence of and vulnerabilities to malicious code.
4.4 Students explain the use of virus signatures in scanning.
4.5 Students can define the concepts of honey pots and secure sandboxes and their relationship to computer security.
4.6 Students can explain fundamental software engineering practices including peer evaluations, tiger teams, modularity, encapsulation configuration management and verification; and can explain the importance of such practices to software security.

**Host-level Security**

5.1 Students can explain how access control lists can be used to implement security policies.
5.2 Students can configure a host computer using access control list mechanisms.
5.3 Students can define the Principle of least privilege and explain why this is relevant to host-level security.
5.4 Students can define the challenge-response concept and how it is applied in security practices.
5.5 Students can explain the utility of password protection, be aware of common password cracking utilities and the associated password vulnerabilities.
5.6 Students can provide a collection of best use policies for password protection.
5.7 Students can explain the concepts of smartcards and tokens and can identify their strengths and weaknesses in user authentication.
5.8 Students are aware of biometric devices for user authentication.
5.9 Students can identify the primary operating system objects that require protection.
5.10 Students can explain how physical, temporal, logical, and cryptographic separation all play a role in operating system security.
5.11 Students are aware of the importance of proper memory management for security.
5.12 Students can implement file protections in the Windows operating environment.
5.13 Students can implement file protections in the Unix operating environment.
5.14 Students can configure a commonly available host firewall.
5.15 Students can define the concept of a trusted system.
5.16 Students can explain the Bell-LaPadula and related models of security.
5.17 Students can explain the Chinese wall policy and its applications in security.

**Network Security**

6.1 Students know the names and roles of the seven layers of the OSI model for network transmission.
6.2 Students understand the role of network ports in providing network services.
6.3 Students can explain the fundamental rules of IPv6.
6.4 Students can explain the difference for UDP and TCP, the associated network services and their different security vulnerabilities.
6.5 Students are aware of the threats and vulnerabilities of such services as telnet, rlogin, bind and SNMP.
6.6 Students can explain the role of routers in network packet transmission.
6.7 Students can perform simple router configuration.
6.8 Students can configure routers for packet filtering via access control lists.
6.9 Students can explain the differences and relative advantages of static, dynamic and stateful firewalls.
6.10 Students can configure a network firewall using access control lists.
6.11 Students can explain the need for both network and host firewalls.
6.12 Students can explain the differences between router filters, firewalls and intrusion detection systems.
6.13 Students can explain the capabilities and limitations of intrusion detection systems.
6.14 Students can explain the difference between intrusion detection and intrusion prevention.
6.15 Students can explain the concept of virtual private networks and can identify their benefits and limitations.
6.16 Students can design the proper placement of network devices for proper security.
6.17 Students can explain the utility of the DMZ in network security layout.
6.18 Students can explain the concept of secure tunneling and be aware of its use in providing hardened services such as SSL and HTTPS.
6.19 Students can explain packet sniffing and the information it provides.
6.20 Students can perform port scanning for the purpose of security audits.
6.21 Students are aware of Web browser vulnerabilities.
6.22 Students can explain the use, and potential for misuse, of Web application cookies.
6.23 Students can explain the basics of SQL injection attacks.
6.24 Students can utilize CERT and other trusted Internet services to access the latest information on vulnerabilities and fixes.

**Legal & Ethical Issues**

7.1 Students can define the concepts of intellectual property, copyrights, and patents.
7.2 Students can explain the fundamental issues of employer/employee rights and responsibilities.
7.3 Students can construct common acceptable use policies.
7.4 Students can identify typical computer crimes.
7.5 Students can broadly explain the impact of the most significant laws and court opinions applicable to information security.