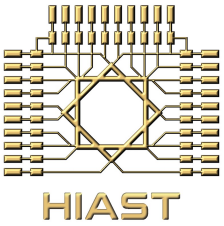
Syrian Arab Republic

Higher Institute for Applied Sciences and Technology



Course Specification Document

Title	Data Security

Credits	3.5 ECTS

Aims	This course aims to provide the student with knowledge related to information security, relevant security policies, risk analysis and assessment methods, and their management. Additionally, it introduces him to the tools, protocols, and systems used in information system security, such as authentication systems, access control management, and standard protocols used. This enables the student to analyze potential risks to the network, utilize appropriate security tools to protect applications and information systems.

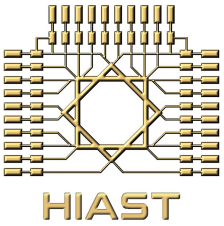
Intended learning outcomes

On successful completion of this course, the student will be able to:

- Understand the fundamental principles of information security, including risks, threats, and information protection models.
- Understand the principles and methodology of developing a security policy and methods for analyzing and assessing risks in an information system.
- Understand the principles and the different types of encryption and their applications in information security.
- Recognize the basic principles and models of authentication, access control systems, and standard protocols used in information security.
- Recognize the methods of protecting network services and the guidelines followed to enhance software security when designing them.

Syllabus

- **General introduction:** Concepts and definitions of information and network security, CIA model, threats and risks to information systems.
- **Security management and risk assessment:** Information security policy, risk analysis and assessment, security measures and procedures, risk management.
- **Threats to information systems:** Network attacks, malware.
- **Intrusion prevention and detection tools:** Firewall, intrusion prevention and detection system.
- **Encryption Algorithms and Applications:** Symmetric key encryption, asymmetric key encryption, hashing functions, digital signatures.
- **Authentication systems and access management:** Authentication systems, access control, authentication system models and applications - digital certificates, SMIME, Kerberos.



- **Network security applications and protocols:** TLS, SSL, SSH, IPSec, VPN.
- **Web services security and data management:** Web service security, domain name service security, data management and information centers security.
- **Operating system security:** Windows, Linux.
- **Software security:** Fundamentals of security in software design, software input handling, memory management, software permissions and system environment variables, interaction with the operating system, software output handling.