| | | | | | |
|---|---|---|---|---|---|
| Course Title | Information Security | | | | |
| Course Code | CSE405 | | | | |
| Course Type | Compulsory | | | | |
| Level | Bachelor (1st Cycle) | | | | |
| Year / Semester | 4th Year / 7th Semester | | | | |
| Teacher's Name | TBA | | | | |
| ECTS | 6 | Lectures / week | 3 hours / 14 weeks | Laboratories / week | N/A |
| Course Purpose and Objectives | This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. The purpose of the course is to provide the student with an overview of the field of information security and assurance. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses, and an overview of the information security planning and staffing functions.<br>Specific topic coverage includes:<br>Introduction to Information Security<br>• The Need for Security<br>• Legal, Ethical, and Professional Issues in Information Security<br>• Planning for Security<br>• Risk Management<br>• Security Technology: Access Controls, Firewalls, and VPNs<br>• Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools<br>• Cryptography<br>• Physical Security<br>• Implementing Information Security<br>• Security and Personnel<br>• Information Security Maintenance | | | | |
| Learning Outcomes | Upon successful completion of the course, students will be able to:<br>• define information security, risk management, risk identification, risk mitigation strategy options and risk control, basic principles of cryptography, physical security considerations, digital forensics and other critical concepts of information security | | | | |

| | | | |
|---|---|---|---|
| | - enumerate the phases of the security systems development life cycle<br>- describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure<br>- assess risk based on probability of occurrence and likely impact<br>- analyze a security incidents and design countermeasures.<br>- explain the mechanism to protect confidentiality and completeness of data.<br>- list and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories | | |
| Prerequisites | CSE300 OR MAT205 | Co-requisites | None |
| Course Content | Introduction to Information Security: the history of information security; what is security; CNSS security model; components of an information system; balancing information security and access; approaches to information security implementation; the systems development life cycle; the security systems development life cycle; security professionals and the organization; communities of interest; information security: is it an art of a science?<br>The Need for Security: business needs first, threats, attacks, secure software development.<br>Legal, Ethical, and Professional Issues in Information Security: law and ethics in information security, relevant US laws, international laws and legal bodies, ethics and information security, codes of ethics and professional organisations.<br>Planning for Security: an overview of risk management, risk identification, risk assessment, risk control strategies, selecting a risk control strategy, quantitative versus qualitative risk control practices, risk management discussion points, recommended risk control practices.<br>Risk Management: information security planning and governance, information security policy, standards and practices, the information security blueprint, security education, training and awareness program, continuity strategies.<br>Security Technology: Access Controls, Firewalls, and VPNs: access controls, firewalls, protecting remote connections.<br>Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools: intrusion detection and prevention systems, honeypots, honeynets, and padded cell systems, scanning and analysis tools, biometric access controls. | | |

| | |
|---|---|
| | Cryptography: foundations of cryptology, cipher methods, cryptographic algorithms, cryptographic tools, protocols for secure communications, attacks on cryptosystems.<br>Physical Security: physical access controls, fire security and safety, failure of supporting utilities and structural collapse, interception of data, mobile and portable systems, special considerations for physical security.<br>Implementing Information Security: information security project management, technical aspects of implementation, nontechnical aspects of implementation, information systems security certification and accreditation.<br>Security and Personnel: positioning and staffing the security function, credentials of information security professionals, employment policies and practices, secure considerations for nonemployees, internal control strategies, privacy and the security of personnel data.<br>Information Security Maintenance: security management maintenance models, digital forensics. |
| Teaching Methodology | Face- to- face |
| Bibliography | Michael E. Whitman, Mattord, Principles of Information Security, Cengage<br>Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, Pearson<br>Mark S. Merkow, Jim Breithaupt, Information Security: Principles and Practices, Pearson<br>William (Chuck) Easttom, II, Computer Security Fundamentals, Pearson<br>Umesh Hodeghatta Rao, Umesha Nayak, The InfoSec handbook – an introduction to information security. |
| Assessment | Examinations 70%<br>Assignments/Lab 20%<br>Class Participation and Attendance 10%<br>100% |
| Language | English |