**SIT403: SYSTEM SECURITY AND AUDIT**

**Credit hours:** 3 hours

**Pre-requisites**: SIT200 *Database Management System, SIT202 Network Design and Management*

**Purpose of the Course**

This course provides students with a background, foundation, and insight into computer security.

**Learning Outcomes**

At the end of the course the students should be able to:

1. Describe the security pitfalls in many important computing tasks today;
2. Asses the controls that can check these weaknesses;
3. Identify the existing controls that are inadequate in computing systems:
4. Appraise the different kinds of computing applications their weakness and controls.
5. Identify vulnerabilities associated with computer security

**Course Description**

|  |  |
| --- | --- |
|  | Topic / Sub topics |
| WEEK 1 | Information Security Fundamentals and principles |
| WEEK 2 | Threats, Attacks, Vulnerabilities, and hazards. Computer Intrusion |
| WEEK 3 | Security Breaches; Threats and Vulnerability |
| WEEK 4 | Security Goals |
| WEEK 4 | Security Controls: Intrusion, Detection, Identification, and Prevention |
| WEEK 5 | Program Security: Viruses and Other Malicious Code: Characteristics; types; Trojan Transmission |
| WEEK 6 | Preventing Infection  Controls Against Threats, Administering security |
| WEEK 7 | CAT 1 |
| WEEK 8 | Personal computer security Risks and management, Risk analysis |
| WEEK 9 | Security planning; Organizational security policies; Trusted operating Systems |
| WEEK 10 | Protected Objects and Methods of Protection; Protecting memory and Addressing; protecting Access to general objects; File protection mechanism; User Authentication Security Features |
| WEEK 11 | CAT |
| WEEK 12 | Database Security: Security Requirements; Reliability and Integrity; Sensitive data; Inference problems; Multilevel Databases Security |
| WEEK 13 | Firewalls and Gateways; Encrypting Gateways; Multilevel Security on Networks; trusted network Interface; Secure Communication |
| WEEK 14 | System audit – Process; Guidelines; Activities; document such as operating procedure, work instruction, training manual, etc. |

**Teaching Methodologies**

Lectures, practical and tutorial sessions in Computer Laboratory, individual and group assignments, exercises and project work

**Instructional Materials/Equipment**

Overhead projector and computer, handouts, white boards, Textbooks, appropriate software.

**Course Assessment**

30% Continuous Assessment (Tests 10%, Assignment 10%, Practical 10%)

70% End of Semester Examination.

**Course Textbooks**

1. Kevin D. Mitnick,  [William L. Simon,](http://goodreadz.com/author/show/10952.William_L_Simon) The Art of Deception: Controlling the Human Element of Security ISBN371-563945

|  |  |  |
| --- | --- | --- |
| 1. Dieter Gollmann, Computer Security, Wiley, ISBN-10: 0470741155 | ISBN-13: | |
| 9780470741153 |  |  |

1. Jones and Ashenden, Risk Management for Computer Security, Butterworth-Heinemann, Print Book ISBN : 9780750677950, eBook ISBN : 9780080491554

**Reference Textbooks**

1. John E. Canavan, Fundamentals of Network Security, 2008 Adison Weisly
2. Edward Amoroso, (2004), Fundamentals of computer security technology, AT&T Bell Labs, Whippany, NJ,
3. Edward Amoroso, Fundamentals of computer security technology, 2011prentice hall, ISBN 371-563980

**Course Journals**

1. Acta Informatica ISSN 0001-5903
2. Advances in Computational Mathematics ISSN 1019-7168
3. Advances in data Analysis and Classification ISSN1 1862-5347
4. Annals Of software Engineering ISSN 1022-7091

**Reference Journals**

1. Journal of computer science and Technology ISSN 1000-9000
2. Journal of Science and Technology ISSN 1860-4749
3. Central European Journal Of Computer Science ISSN 1896-1533
4. Cluster computing ISSN 1386-7857