Department of Computer Applications
National Institute of Technology, Tiruchirappalli

1. Course Outline			
Course Title	Information Security		
Course Code	CA724		
Department	CA	**No. of Credits**	3
Programme	MCA	**Learning Hours**	3
Course Type	Programme Core	**Course Teacher**	Dr. P.J.A. Alphonse
Pre-requisites	CA 713, Basics on Networks, Operation Systems and Database		
E-mail	alphonse@nitt.edu	**Telephone No.**	0431-2503742
Course Type	Core Course	**Office**	Lyceum 107
Course Page	http://egov.nitt.edu/moodle/course/view.php?id=45		

2. Course Content

The Information Security course deals with the study and analysis of security in computers. It also explores Cryptography, Forensics, Network, Application and Data security.

3. Course Objectives

1. To understand the models of information security
2. To study and analyze cryptographic and forensic methods
3. Analyze and simulate the network security and application security
4. Explore the nature and logic behind security threats on the web as an ethical hacker

4. Course Learning Outcomes (CO)

1. Identify the information security models and their characteristics
2. Analyze the different types of cryptographic and forensic methods
3. Study the network security issues
4. Discover the layers of application security
5. Identify different threats and suggest fixes.

5. Course Outcome (CO)	Aligned Programme Outcome (PO)											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
Identify the information security models and their characteristics	H	H	A	A	A	H	H	A	L	H	A	H
Analyze the different types of cryptographic and forensic methods	H	H	A	A	H	A	H	A	L	L	A	H
Study the network security issues	H	H	H	A	H	A	H	L	L	H	H	H
Discover the working of application security	H	H	H	A	H	A	H	L	L	H	H	H
Identify different threats and suggest fixes	H	A	H	A	H	H	H	H	L	H	H	H

Lectures

Class lectures and class exercise with self-learning videos will form the primary teaching activity, the schedule for which is outlined below. Lecture material will address the intended learning objectives, and loosely follow the readings as specified in the Moodle course site. The lecture material will be made available before the class. The lectures are meant to be interactive, where learning takes place through interactive discussion in class. The Moodle site will be available for detailed content dissemination and discussion inside and outside the classroom, between students and with the teacher. Student engagement in class and in the Moodle online forum will count towards assessment of student participation that has assessment weightage.

Guest Lectures

Structured lectures will be supplemented by guest lectures by practitioners and researchers from industry and academia. These will serve to show the practical relevance of the course content and also expose the students to the open problems for research.

6. Course Teaching and Learning Activities

Week	Mode of Delivery	Topics
1.	Classroom activity	Critical characteristics of Information
		NSTISSC Security Model
		Components of information System
2.	Classroom activity	Review I
		Securing
3.	Classroom activity	Balancing
		SDLC
		Review II
4.	Classroom activity	Classical Cryptography
		Symmetric
		Asymetric
5.	Classroom activity	Modern
		Review III
		DRM
6.	Classroom activity	Stegnography
		Biometrics
		Review IV
7.	Classroom activity	Network security
		Wireless
		Intrusion
8.	Classroom activity	Application
		Database
		Email
9.	Classroom activity	VOIP
		Review V
		Threats
10.	Classroom activity	Tools
		Breaches
		Review VI

- All relevant material will be made available to the students in the moodle course site. Classroom activity includes lectures, tutorials, quiz, simulation exercise, laboratory exercise, mini-project, group task and seminar.

The assessment details for this course are given below. The assessment will be done for a total of 100 marks.

7. Course Assessment Methods – Theory

Sl. No.	Mode of Assessment	Nature	Tentative Schedule	Duration in Min.	Weightage (%)
1.	Test	Formative	4th week	60	20
2.	Test	Formative	8th week	60	20
3.	Class activity	Periodic	Course duration	NA	10
4.	End Semester Exam	Summative	November	120	50
				Total	100

8. Essential Learning material (Textbooks, Reference books, Websites, Journals, etc.)

1. William Stallings, "Cryptography and Network Security: Principles and Practices", 6th Edition, 2013, PHI.
2. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", 2003, Vikas Publishing House, New Delhi.
3. Niel Daswani, Christopher Kern, Anita Kesavan, " Foundations of Security: What every programme" APRESS, 2007

9. Course Exit Survey

- The students may give their feedback at any time to the course Teacher or through an email message in moodle, which will be duly addressed.
- The students may also give their feedback during Class Committee meeting and fill up the feedback form in moodle site at the end of each test.

10. Course Policy (including plagiarism, academic honesty, attendance, etc.)

Classroom Behavior

- Ensure that the course atmosphere, both in the class and discussions outside the class room with Teacher, is conducive for learning. Participate in discussions but do not dominate or be abusive. Be considerate of your fellow students and avoid disruptive behavior.

Exam policy

- Each student is required to take all exams at the scheduled times. All exceptions must be cleared with the professor prior to the exam time. Exams missed for insufficient reason and without being cleared with the professor prior to the exam time will be assigned a score of zero.

Assignments

- All assignments are due on or before the mentioned date and time and is to be uploaded on the course moodle site.

Late assignments

- Late submissions are not accepted.

Plagiarism

- The students are expected to come out with their original work on term activity, assignments and tests/examinations. If found to be plagiarized, it will be assigned a score of zero.

Attendance

- Attendance is expected. If a student misses a class, the student is still responsible for the material that is studied and for completing any assignments by the due date that may have been handed out by the instructor during class.

Academic Honesty

i) No type of academic dishonesty will be tolerated. If the student is caught cheating (on the assignments, exams, or project) the punishment will be the most severe penalty allowed by the Institute policy.
ii) Possession of any electronic device, if any, found during the test or exam, the student will be debarred for 3 years from appearing for the exam and this will be printed in the Grade statement/Transcript.
iii) Tampering of MIS records, if any, found, then the results of the student will be withheld and the student will not be allowed to appear for the Placement interviews conducted by the Office of Training & Placement, besides (i).

11. Additional Course Information

- The students can get their doubts clarified during class.
- Prior request for appointment through mail, stating the subject matter to be discussed, is required to fix a time for discussion of subject matter outside class. Appointment time will be communicated through reply mail.

For Senate's Consideration

(Dr. P.J.A. Alphonse)
Course Faculty

(Dr. Michael Arock)
PAC Chairperson

(Dr. S. R. Balasundaram)
Head