NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE PLAN – PART I			
Name of the Programme and specialization	**B-Tech (Minor)**		
Course Title	**Information Security**		
Course Code	**CAMI19**	**No. of Credits**	**3**
Course Code of Pre-requisite subject(s)	**CAMI10**		
Session	**~~July~~ / January 2023**	**Section (if, applicable)**	**2nd,3rd and 4th year students**
Name of Faculty	**NILIN PRABHAKER**	**Department**	**Computer Applications**
Official Email	**405320002@nitt.edu**	**Telephone No.**	**8969605780**
Name of PAC Chairperson	**Dr. Michael Arock**		
Official E-mail	**michael@nitt.edu**	**Telephone No.**	**91-431-2503736**
Course Type	☑ **~~Core~~ course** Minor	□ **Elective course**	

Syllabus (approved in BoS)

Information Security - Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, SDLC, Security SDLC

Cryptography: Classical Cryptography, Symmetric Cryptography, Public Key (Asymmetric cryptography), Modern Cryptography. Forensics: DRM technology (including watermarking and fingerprinting of images, video and audio), Steganography, Biometrics

Network Security: Network Protocols, Wireless Security (WiFi, WiMAX, Bluetooth, and cell phone), IDS and Network Intrusion Management

Application Security: Email Security, Web Security, and Database Security, Secure Software Development, VoIP Security

Information Security Threats: Viruses, Worms and other malware, Email Threats, Web Threats, RFID, Identity Theft, Data Security Breaches, Hacking Tools and Techniques

References:

1. W. Stallings, Cryptography and Network Security: Principles and Practice, 6th Edition, Prentice Hall, 2013
2. Neil Daswani, Christoph Kern, Anita Kesavan, " Foundations of Security: What Every Programme", APRESS, 2007.
3. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, 2003.

COURSE OBJECTIVES

To study the concepts and requirements of Information Security.

MAPPING OF COs with POs

Course Outcomes	Programme Outcomes (PO) (Enter Numbers only)
1. Explain the models of information security	1,3,5,6,7,8,11,12
2. Apply cryptography techniques to data	1,2,5,11,12
3. Simulate the various network security issues	1,5,6,7,11,12,8
4. Experiment with application security	1,5,6,7,11,12,10
5. Explore the nature and logic behind the various security threats on the web	1,5,6,7,8,11,12

COURSE PLAN – PART II

COURSE OVERVIEW

The Information Security course deals with the study and analysis of asepcts of security in computers used in various organizations. It also covers Cryptography , Network Security, Application Security and Information Security Threats along with study of Hacking tools and Forensics.

COURSE TEACHING AND LEARNING ACTIVITIES

S.No.	Week/Contact Hours	Topic	Mode of Delivery
1	Week1 / 3 Hours	Information Security Introduction, Characteristics, Need of Information security	Offline Class Presentation and B/W Board
2	Week 2 / 3 Hours	NSTISSC Security Model, Components of an Information System, Securing the Components	Offline Class Presentation and B/W Board
3	Week 3 / 3 Hours	Balancing Security and Access, SDLC, Security SDLC	Offline Class Presentation and B/W Board
4	Week 4 / 3 Hours	Cryptography Introduction and Classical Cryptography	Offline Class Presentation and B/W Board
5	Week 5 / 3 Hours	Symmetric Cryptography	Offline Class Presentation and B/W Board
6	Week 6 / 3 Hours	Public Key (Asymmetric cryptography)	Offline Class Presentation and B/W Board
7	Week 7 / 3 Hours	Forensics: DRM technologies, Steganography and Biometrics	Offline Class Presentation and B/W Board
8	Week 8 / 3 Hours	Network Protocols and Wireless Security	Offline Class Presentation and B/W Board
9	Week 9 / 3 Hours	IDS and Network Intrusion Management	Offline Class Presentation and B/W Board

10	Week 10 / 3 Hours	Application Security: Email Security, Web Security,	Offline Class Presentation and B/W Board
11	Week 11 / 3 Hours	Database Security, Secure Software Development, VoIP Security	Offline Class Presentation and B/W Board
12	Week 12 / 3 Hours	Information Security Threats	Offline Class Presentation and B/W Board
13	Week 13 / 3 Hours	Hacking Tools and Techniques	Offline Class Presentation, Demo and B/W Board

COURSE ASSESSMENT METHODS (shall range from 4 to 6)

Sr.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Cycle Test 1	Week 5	1 Hour	20
2	Cycle Test 2	Week 10	1 Hour	20
3	Assignment	-----	-----	10
4	Compensation Assessment*	Week 11	1 Hour	20
5	Final Assessment *	3rd Week of May	3 Hours	50

***mandatory; refer to guidelines on page 4**

COURSE EXIT SURVEY (mention the ways in which the feedback about the course shall be assessed)

- Students through the class representative may give their feedback at any time to the course faculty which will be duly addressed.
- Students may also give their feedback during class committee meeting.

COURSE POLICY (including compensation assessment to be specified)

MODE OF CORRESPONDENCE (email/phone)

Students can get the availability of faculty member over phone and email. They can get their doubts clarification at any point of time with their faculty member with prior appointment.

COMPENSATION ASSESSMENT

One compensation assessment for absentees in assessment(Other than final assessment) is mandatory. Only genuine cases of absence shall be considered.

ATTENDANCE POLICY (A uniform attendance policy as specified below shall be followed)

- At least 75% attendance in each course is mandatory.
- A maximum of 10% shall be allowed under On Duty (OD) category.
- Students with less than 65% of attendance shall be prevented from writing the final assessment and shall be awarded 'V' grade.

ACADEMIC DISHONESTY & PLAGIARISM

- Possessing a mobile phone, carrying bits of paper, talking to other students, copying from others during an assessment will be treated as punishable dishonesty.
- Zero mark to be awarded for the offenders. For copying from another student, both students get the same penalty of zero mark.
- The departmental disciplinary committee including the course faculty member, PAC chairperson and the HoD, as members shall verify the facts of the malpractice and award the punishment if the student is found guilty. The report shall be submitted to the Academic office.
- The above policy against academic dishonesty shall be applicable for all the programmes.

ADDITIONAL INFORMATION

FOR APPROVAL

Course Faculty __________ CC- Chairperson ______________ HOD ______________

NILIN
PRABHAKER