

Himachal Pradesh University

(NAAC Accredited “A” Grade University)

Summerhill, Shimla-171005,

Himachal Pradesh, India

Plan, Scheme, and Syllabus

to start a programme

Certificate Course

in

Cyber Security

(Effective from Session 2026-2027)



Center for AI on Cyber Physical Systems

Himachal Pradesh University

(NAAC Accredited A" Grade University)

Summerhill, Shimla-171005

Content

	Page
1. Introduction	3
2. Program Details:	3
(a) Program	
(b) Duration	
(c) Eligibility	
(d) Mode of Admission	
(e) Fee Structure	
3. Examinations	4
4. Minimum Criteria to Award Certificate Course	4
5. Scheme of Syllabus	6
6. Detailed Syllabus	7

1. Introduction: The history of Cyber Security began in the 1970s, when the first computer networks emerged and researchers discovered vulnerabilities that could be exploited. One of the earliest notable events was the creation of the “Creeper” virus in 1971, which led to the first antivirus program, “Reaper.” As computers became more interconnected in the 1980s and 1990s, cyber threats grew rapidly, prompting the development of firewalls, intrusion detection systems, and encryption technologies. The rise of the internet age brought new forms of attacks—worms, viruses, phishing, and large-scale data breaches—highlighting the need for stronger security practices. In the 2000s and beyond, cyber security evolved into a critical discipline focusing not only on technical defenses but also on risk management, digital forensics, and global cyber regulations. Today, with the expansion of cloud computing, IoT, and AI, cyber security continues to advance, playing a vital role in protecting individuals, organizations, and nations from ever-growing digital threats.

2. Program Details:

- a) Program: Certificate course in Cyber Security
- b) Duration & Seats: Six-month Program with 30 seats. (*Course will be start, if minimum 10 students will be admitted to the course)
- c) Eligibility: 10+2 in any stream with 50% aggregate marks in qualifying exam (45% for SC/ST/PWD)
- d) Mode of Admission: Direct Admission on merit bases
- e) Fee Structure: Rs. 10,000/-

3. Examinations:

As the certificate course is spanned over six months, the learning outcomes shall be assessed on the following components:

Sr. No.	Assessment Component
1.	Course End External Examinations (Theory)
2.	Internal Assessment (Theory)
3.	Fundamentals of Cyber Security Lab

4. Minimum Criteria to Award Certificate course:

The candidate will be awarded with the Certificate Course after securing 40% marks in all the Courses prescribed in the Scheme of Syllabus of Cyber Security. The total credit for the certificate course in Artificial Intelligence is seven (07).

Certificate Course

In

Cyber Security

Scheme

&

Syllabus

Credit Based System

Effective from

Academic Session 2026-2027

Scheme of Syllabus

Total credit of the certificate course: 07

Sr. No.	Broad Category	Category	Course Code	Course Title	L	P	H	C	Semester End Marks	
									ESE	IA
1.	PCC	Major	PCC-CST-1	Fundamentals of the Computer Networks & Cyber Security	3	0	3	3	50	25
2.	PCC	Major	PCC-CST-2	Foundation Course on Cyber Security laws and Cyber Forensic	3	0	3	3	50	25
3.	PCC	Major	PCC-CSL	Fundamentals of Cyber Security Lab	0	1	2	1	30	20
Total							8	7	130	70
									Total = 200	

Centre for AI on Cyber Physical Systems

Course Code	PCC-CST-1	Credit 3	L-3, T-0, P-0
Name Of the Course	Fundamentals of the Computer Networks & Cyber Security		
Lectures to be delivered	45 (1 Hr. Each) (L=45, T=0 for each semester)		
Course End Examination	Max Marks: 50	Min Pass Marks: 40%	Max Time: 2 Hrs.
Internal Assessment: Class test/Assignments/Presentations/etc-20 Marks, Attendance- 5 Marks			Max Marks: 25
Instructions: For Paper Setters: There will be 3 parts (A, B, C) and examiner shall set a total of six (6) questions from all the sections (A, B, C) in total. Part A will have 2 questions from section A of the syllabus of 10 marks each and the student shall have to attempt anyone. Part B will have 2 questions from section B of 10 marks shall have to attempt anyone. Part C will have 2 questions from section C of 10 marks shall have to attempt anyone Part D will have 7 questions from all the sections of the syllabus of 4 marks each and students have to attempt any 5 questions. For Candidates: Students will attempt eight (8) questions in total by selecting one questions from each section A, section B and section C and five questions from section D. Use of non-programmable calculators is allowed.			
Course Objective: To provide students with foundational knowledge and skills to identify, understand, and respond to basic computer and cyber security threats.			
SECTIONS	COURSE CONTENT		
Section A	Introduction to Computer and Computer Networks: Fundamental of Computer network, Do's and Don'ts about Computer, Computer Peripherals, Various types of search engines and web browsers, Internet, Safe use of internet in online shopping, online banking, safe downloading, social engineering, email uses, phishing, VoIP Phishing, Safe and secure use of the web browsers. Fundamental of Computer Security: Data Security and Management, Encryption and Decryption, Digital Signature, Firewalls, Antiviruses, File Security, User Security, Mobile Device Security.		
Section B	Introduction to Cyber Security and Threats: Cyber Security concerns, Cyber Crimes, Importance of Cyber Security, Basics Computer Ethics, Cyber Threats (Virus, Worms, Trojan Horse, malware, Ransom ware, Identity Theft etc.), Cyber Bullying, Cyber Grooming, Online Gaming, Email Frauds, Online Transaction Frauds, Safeguard of our social networking profiles, Torrent and infected websites.		
Section C	Wireless Security: Unsecured and Secured Wi-Fi Uses, Risk of using unsecured Wi-Fi, how to use secure Wi-Fi. Cyber Crime awareness government websites and Cyber Crime examples: National Cyber Crime reporting portal, Indian Cybercrime Coordination Centre, Indian Computer Emergency Response Team.		
Course Outcome: At the end of the course, the student will be able to - To understand the Cyber Threats and resolve & recover from the cyber incident through timely information sharing. - Understand General Internet Safety and Computer Security Concepts. - To know about how to maintain data privacy and wireless security. - Relate the models to real-world networking scenarios.			
Reference Books - Anand Shinde, "Introduction to Cyber Security: Guide to the World of Cyber Security" Notion Press (28 February 2021). - Mayank Bhushan, Raj Kumar Singh Rathore and Aatif Jamshed, "Fundamental of Cyber Security (Principles, Theory & Practices)" BPB, First Edition (1 January 2017). - Nilakshi Jain & Ramesh Menon: "Cyber Security and Cyber Laws", Wiley (1 October 2020); Wiley India Pvt Ltd.			

Centre for AI on Cyber Physical Systems

Course Code	PCC-CST-2	Credit 3	L-3, T-0, P-0
Name Of the Course	Foundation Course on Cyber Security laws and Cyber Forensic		
Lectures to be delivered	45 (1 Hr. Each) (L=45, T=0 for each semester)		
Course End Examination	Max Marks: 50	Min Pass Marks: 40%	Max Time: 2 Hrs.
Internal Assessment: Class test/Assignments/quiz/seminar-20Marks, Attendance- 5 Marks.			Max Marks: 25
Instructions: For Paper Setters: There will be 3 parts (A, B, C) and examiner shall set a total of six (6) questions from all the sections (A, B, C) in total. Part A will have 2 questions from section A of the syllabus of 10 marks each and the student shall have to attempt anyone. Part B will have 2 questions from section B of 10 marks shall have to attempt anyone. Part C will have 2 questions from section C of 10 marks shall have to attempt anyone Part D will have 7 questions from all the sections of the syllabus of 4 marks each and students have to attempt any 5 questions. For Candidates: Students will attempt eight (8) questions in total by selecting one questions from each section A, section B and section C and five questions from section D. Use of non-programmable calculators is allowed.			
Course Objective: To provide students with foundational knowledge of cyber security laws, regulations, and digital forensic techniques, enabling them to understand legal frameworks governing cybercrime and apply basic forensic methods for investigating cyber incidents.			
SECTIONS	COURSE CONTENT		
Section A	Cyber Security: Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.		
Section B	Cyberspace Law & Cyber Forensic: Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Cyber Forensics: Introduction, Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics.		
Section C	Cybercrime: Malware Attacks, Phishing and Social Engineering, Cyberstalking and Cyberbullying, Cyber Terrorism and Cyber Espionage. Examples and Mini-Cases Examples: Official Website of Maharashtra Government Hacked, Indian Banks Lose Millions of Rupees, Parliament Attack, Pune City Police Bust Nigerian Racket, e-mail spoofing instances. Mini-Cases: The Indian Case of online Gambling, An Indian Case of Intellectual Property Crime, Financial Frauds in Cyber Domain.		
Course Outcome: At the end of the course, the student will be able to - To understand the Cyber Threats and resolve & recover from the cyber incident through timely information sharing. - Understand General Internet Safety and Computer Security Concepts - To know about how to maintain data privacy and wireless security.			
Reference Books: - Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Perspectives,Wiley . - B.B. Gupta,D.P. Agrawal, HaoxiangWang, Computer and Cybersecurity: Principal s, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,2018. - Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress. - Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.			

Centre for AI on Cyber Physical Systems

Course Code	PCC-CSL	Credit 1	L-0, T-0, P-2
Name Of the Course	Fundamentals of Cyber Security Lab		
Total Practical Sessions	30 (2 Hrs. Each)		
Course End Examination	Max Marks: 30	Min Pass Marks: 40%	Max Time: 2 Hrs.
Internal Assessment: Lab Work Assessment/Experiment Performance /Viva-15 Marks, Attendance- 5 Marks			Max Marks: 20
List of Experiments			
Course Objective: To provide a basic understanding regarding computer Security, physical security, email management and threat detection, and mobile app security.			
Sr.No.	Name of the Experiment		
1.	Fundamentals of Computers • IP address • MAC Address • Static IP • Dynamic IP		
2.	Installation of Windows on VirtualBox. • Virtual Box • Win 8 -ISO		
3.	Physical Security, Windows Backdoor. • Syskey.		
4.	Introduction to password management practices.		
5.	Demonstration of network vulnerabilities and threats		
6.	Email Security • Header Analysis. • Email Tracker pro. • Read notify.		
7.	Mobile Security Apps. • Smart phone encryption.		
8.	Open-Source Software Tools		
Course Outcome:			
At the end of the course, the students will be able to:			
• Perform the functions related to the installation of the window. • Able to identify the network vulnerabilities and threats. • Able to identify the email and mobile threats			
Reference Books:			
1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRCPress.			
2. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T&F Group.			