

PROGRAMME PROJECT REPORT (PPR)

Diploma in Cyber Security (DCS)

1. Introduction about the Programme

The evolution of Information Communication Technology (ICT) and growing security concerns demands flexible and generally comprehensive approach to the issue of cyber security. The rapid growth of ICT has raised various complex questions which need to be addressed. A need has been felt to address cyber security broadly, as also in sufficient depth so that even students from non-technical streams will develop a more complete picture of the cyber security issues. The syllabus has been prepared with an aim to create more aware, responsive and responsible digital citizens, thereby contributing effectively to an overall healthy cyber security posture and ecosystem.

2. Programme Mission & Objectives

2.1 Mission Statement


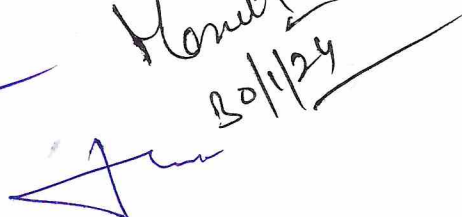
To equip students with the knowledge, skills, and ethical mindset required to thrive in the dynamic and evolving field of cybersecurity and also provide a comprehensive and hands-on educational experience that prepares individuals to safeguard digital assets, mitigate cyber threats, and contribute to the overall security of information systems.

2.2 Objectives

The Programme has been framed to achieve the following main objectives:

- To develop an understanding and knowledge of fundamental concepts in cybersecurity, including but not limited to cryptography, network security, computer forensics, and ethical hacking.
- To Provide students with practical, hands-on experience in cybersecurity tools and techniques.
- To encourage students to analyze problems, evaluate potential solutions, and make informed decisions in response to security incidents.



1  Monika
30/1/24


- To provide students with the knowledge and skills to assess and manage cybersecurity risks.
- To ensure students are familiar with the legal and ethical aspects of cybersecurity.

3. Relevance of the Programme

The relevance of a Diploma in Cybersecurity program is significant in today's digital age where the reliance on technology and interconnected systems has increased exponentially. With the increasing frequency and sophistication of cyber threats, there is a growing demand for skilled cybersecurity professionals who can protect organizations from cyber-attacks, data breaches, and other security incidents.

4. Prospective Target Group

- Having passed 10+2 in any Stream or the equivalence examination or the higher examination from the recognized Board/University.
- Having passed 2 Years ITI Programme in any trade after Matriculation from Punjab State Board of Technical Education & Industrial Training, Chandigarh or such examination from any other recognized State Board of Technical Education.
- Having passed 3 Years Diploma in any stream after Matriculation from Punjab State Board of Technical Education & Industrial Training, Chandigarh or such examination from any other recognized State Board of Technical Education.

Learners with above said eligibility may join this course to improve their knowledge, skills, employability, and entrepreneurship ability. The working persons and who cannot study through regular mode can continue their education through this open learning mode.

5. Appropriateness of the Programme

The Programme will provide academic continuity to the learning community and will facilitate continuous professional development for the employees and entrepreneurs across the country and Punjab state, in particular. The Programme aims to reach the learners who are distant and those lacking access. To reach the unreached, the courses' instructions and specially prepared study material in the form of printed notes and audio-video lessons to the learners will be delivered at their door steps through postal correspondence and digital media like e-mail, website etc. Limited face-to-face contact sessions will be held at Learner Support Centres (LSC) set up by the university as close as possible to the learner's home. Communication with the university and

2

Munshi
20/1/24

interaction between the teacher and the learners will be further facilitated using electronic media options like telephone, e-mails, chat sessions, video conferencing and tele conferencing, if and when required. All of these characteristics will help learners to engage in relevant, purposeful and interesting lessons.

Apart from this, the learners will have the advantage to study at their own pace and convenience as the Programme can be completed in the time span ranging from one year to two years.

The multiple exit and enter option for learners is facilitated. Learners are allowed to exit the Programme after the six months obtained at least 20 credits with a relevant certificate and re-enter the same programme at a later time.

6. Instructional Design

Annexure-A (Course Scheme of Diploma in Cyber Security)

Annexure-B (Syllabi of Diploma in Cyber Security)

7. Procedure for Admissions

Notifications regarding admission will be published in the leading national and regional newspapers. In addition to this, all the required information will be updated regularly on the university website

7.1 Programme Duration: 1 Year to 2 Years

7.2 The Medium of Examination: English

7.3 Eligibility:

- Having passed 10+2 in any Stream or the equivalence examination or the higher examination from the recognized Board/University.
- Having passed 2 Years ITI Programme in any trade after Matriculation from Punjab State Board of Technical Education & Industrial Training, Chandigarh or such examination from any other recognized State Board of Technical Education.
- Having passed 3 Years Diploma in any stream after Matriculation from Punjab State Board of Technical Education & Industrial Training, Chandigarh or such examination from any other recognized State Board of Technical Education.

7.4 Total Programme Fee:

3

Fee Head Details	Semester-1	Semester-2
Registration/ Continuation Fee	300	300
Tuition Fee	--	--
Examination Fee	1400	1400
I.T. and other Charges	1100	1100
Security Fee (Refundable)	--	--
Total Fee (Rs.)	2800	2800

7.5 Instructional Delivery Mechanisms:

The Programme has been designed with the aim to reach the distant and those lacking access to a regular mode of education. The courses' instructions and specially prepared study material will be made available through Learner Support Centres (LSCs) and digital media like e-mail, website etc. Limited face to face contact sessions will be held at the study centers set up by the university as close as possible to the learner's home. Communication with the university and interaction between the teacher and the learners will be further facilitated using electronic media options like telephone, e-mails, chat sessions, video conferencing and tele conferencing, if and when required.

Besides this, Counseling Sessions will be held at all the LSCs regularly during weekends. The university will also conduct live/virtual classes for learners using modern ICT methods. However, to ensure learner participation and interaction, online classes will be blended with face to face discussions and meetings with the learners.

8. Evaluation

The learners' progress is measured through the means of continuous evaluation and end semester examinations.

8.1 Continuous Internal assessment through assignments

Assignments help the learners to recapitulate the theory and go back to the text again in case they are unable to answer a particular question. Thus, assignments also help to reinforce learning in distance and open learning system of education. The assignments will consist of a

set of questions and activities that have to be answered by the programme participants by remaining at their own place.

Two assignments will be submitted for a 4 credits course and one assignment will be submitted by the learner for a 2 credits course. The assignments will cover all or any types of questions (long answer type, short answer type, objective type, multiple choice questions and case studies).

Learners will be required to obtain 40% marks as pass percentage in each assignment separately. In the final result, assignments will carry 30% weightage.

8.2 Semester End Examination

Semester end examination is the major component of the evaluation system and carries 70% weightage in the final result. The university will conduct end semester examination twice a year i.e., in June and in December. The learners can take the examination only after the completion of the course, failing which they can take the same in December or June of subsequent years but within the total span of the programme. In case any student fails to get a passing score in the semester end examination, they will be eligible to reappear in the next semester end examination for that course as and when it is held but within the total span of the programme only.

In order to claim Certificate/Diploma in Cyber Security, the learner is required to score at least 40% marks in both continuous evaluations (i.e.in assignments) as well as in semester end examinations separately.

8.3 Updated Notification for the Learners

The information regarding the university policies and procedures, academic activities like assignment submissions, question papers, results and other notices related to examination and evaluation will be uploaded on the official website of the university.

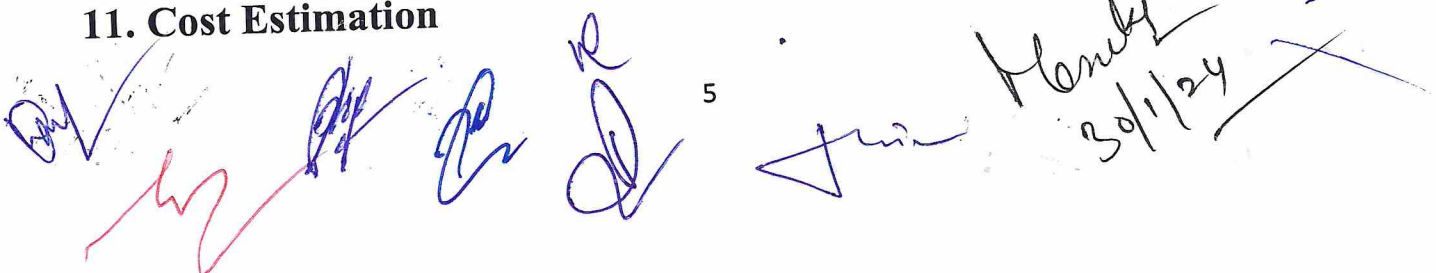
9. Laboratory Support

Modernize Computer Labs at the Learner Support Centres (LSCs) will be provided with all latest computers and software required for this Programme.

10. Library Resources

The students may avail the library facilities at their Learner Support Centres (LSCs).

11. Cost Estimation

 5

Handwritten signature: *Manish*
Date: *30/1/24*

The cost of the programme will be as per the fee decided upon.

12. Quality Assurance Mechanism

The university has constituted a “Centre of Internal Quality Assurance (CIQA) as per UGC (Open and Distance Learning) Regulations, 2020.

13. Programme Outcomes (POs)

Programme: Diploma in Cyber Security

Programme Outcomes (POs)	
On successful completion of this Programme, the students will be able to:	
PO1	Understand the fundamental principles of computer science, information technology, and cyber security and demonstrate knowledge of the legal and ethical issues related to cyber security.
PO2	Possess hands-on technical skills to analyse, design, and implement secure systems and networks.
PO3	Demonstrate the ability to analyse and solve complex cyber security problems through critical thinking, innovative approaches, and effective decision-making.
PO4	Demonstrate entrepreneurial skills and innovative thinking, potentially contributing to the development of new cyber security solutions and technologies.
PO5	Communicate effectively with technical and non-technical stakeholders, both in oral and written forms, to convey cyber security concepts and recommendations.
PO6	Understand and adhere to ethical standards and demonstrate social responsibility in their professional practice, considering the broader impact of cyber security decisions on individuals and society.
PO7	Assess and manage risks associated with information security and apply risk management principles to protect organizational assets.
PO8	Engage in lifelong learning to stay abreast of evolving cyber security threats, technologies, and best practices, adapting to the dynamic nature of the field.

14. Programme Specific Outcomes (PSOs)

Programme: Diploma in Cyber Security

Programme Specific Outcomes (PSOs)	
On successful completion of this Programme, the students will be able to:	
PSO1	Demonstrate a comprehensive understanding of core principles, concepts, and theories in cybersecurity, including cryptography, network security, and secure software development.
PSO2	Apply secure coding practices to develop software applications that are resilient to

6

Mouky
30/1/24

	common cybersecurity threats and vulnerabilities.
PSO3	Evaluate and manage cybersecurity risks, considering business impact and applying risk management frameworks.
PSO4	Conduct ethical hacking exercises and digital forensics investigations to identify and analyze security incidents.
PSO5	Understand and adhere to legal and regulatory requirements related to cybersecurity, and assess compliance within organizational contexts.

15. Course Outcomes (COs)

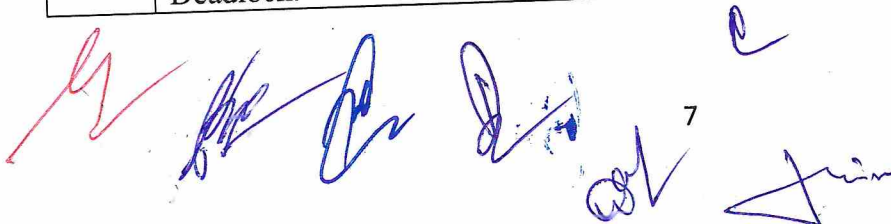
Course Outcomes (COs) of Courses of Semester-1

Course#1

Course: Data Communication and Networks	
Course Code: DCS-1-01T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand the fundamental concepts in data communication and networking
CO2	Explore real-world applications of principles of network design, topology, and the OSI/TCP/IP model
CO3	Develop the ability to identify and formulate problems related to computer network
CO4	Apply networking knowledge to design and configure basic computer networks, addressing schemes and Routing Protocols
CO5	Describe the basic concepts, principles, and techniques for the development of networks and trouble shooting

Course#2

Course: Operating Systems	
Course Code: DCS-1-02T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand the structure of computing systems, from the hardware level through the operating system level and onto the applications level.
CO2	Understand basics of operating system viz. system programs, system calls, user mode and kernel mode.
CO3	Learn the working with CPU scheduling algorithms for specific situation, and analyze the environment leading to deadlock and its rectification.
CO4	Explore the memory management techniques viz. caching, paging, segmentation, virtual memory, and thrashing.
CO5	Apply Methods for Handling Deadlocks, Deadlock Prevention, and Recovery from Deadlock.



 7

 Monday

 8/1/24

Course#3

Course: Operating Systems Lab	
Course Code: DCS-1-02P	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand Basics of UNIX/LINUX
CO2	Demonstrate the installation process of various operating systems.
CO3	Apply UNIX/LINUX operating system commands.
CO4	Understand different UNIX/LINUX shell scripts
CO5	Implement and execute various shell programs.

Course#4

Course: Introduction to Cyber Security	
Course Code: ICS-1-02T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand network security threats, security services, and countermeasures.
CO2	Understand principles of network security by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.
CO3	Develop cyber security strategies and policies
CO4	Measure the performance and troubleshoot cyber security systems.
CO5	Understand various Cryptographic Techniques

Course#5

Course Name: Introduction to Cyber Security Lab	
Course Code: ICS-1-02P	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Identify and analyze common cyber threats, including malware, phishing attacks, and network vulnerabilities.
CO 2	Apply techniques to detect, mitigate, and respond to various types of cyber threats.
CO 3	Implement security configurations for operating systems, network devices, and applications.
CO 4	Apply ethical hacking techniques to identify and exploit vulnerabilities in controlled environments, emphasizing responsible and legal practices.
CO5	Implement cryptographic techniques for security purpose

[Handwritten signatures and initials in red and blue ink]

8

Monika
30/1/24

Course Outcomes (COs) of Courses of Semester-2

Course#6

Course Name: Digital Forensics	
Course Code: DCS-2-01T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand the principles and concepts of digital forensics.
CO 2	Understand various types of cyber crimes
CO 3	Analyze computer architectures, file systems, and operating systems relevant to digital forensics investigations.
CO 4	Understand the legal and ethical considerations associated with digital forensics, including the admissibility of digital evidence in court.
CO 5	Utilize popular forensic tools and software for digital investigations.

Course#7

Course Name: Cyber Attacks and Counter Measures	
Course Code: DCS-2-02T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand the importance of a network basics and brief introduction on security of network protocols
CO 2	Demonstrate a solid understanding of foundational cybersecurity concepts, principles, and best practices.
CO 3	Apply risk assessment methodologies to evaluate and prioritize potential vulnerabilities within a given system or network.
CO 4	Design and develop security plans and strategies to ensure the integrity of information in compliance with best practices, relevant policies, standards, and regulations.
CO 5	Evaluate the impact of cybersecurity decisions on privacy, compliance, and organizational reputation, and adhere to ethical standards in the field.

Course#8

Course Name: Cyber Attacks and Counter Measures	
Course Code: DCS-2-02P	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Develop skills in configuring security settings for operating systems, networks,

Handwritten signatures and initials in red and blue ink, including a signature that reads "Hondas" and a date "30/1/24".

	and applications.
CO 2	Analyse network traffic using tools like Wireshark.
CO 3	Conduct vulnerability assessments to identify potential weaknesses and recommend appropriate countermeasures.
CO 4	Apply tools to analyze network traffic and system logs in real-time.
CO 5	Understand and apply secure coding practices to develop resilient software.

Course#9

Course Name: Cyber Laws	
Course Code: CL-2-03T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand various types of cyber crimes
CO 2	Understand Indian Laws to deal with Cyber Crimes and its critical analysis
CO 3	Understand Legal Recognition of Electronic Records and Electronic Evidence
CO 4	Examine and interpret laws related to cybercrimes, including hacking, identity theft, and online fraud.
CO 5	Explore the legal aspects of intellectual property rights, including copyright, patents, and trademarks, in the digital environment.



 Multiple handwritten signatures in blue and red ink are scattered across the page. On the right side, there is a signature that reads "Monika" with the date "30/1/24" written below it.