Savitribai Phule Pune University

(Formerly University of Pune)

DEPARTMENT OF TECHNOLOGY

Foundation Course in Cyber Security

1. **About the course:**

Brief Job Description: This job role is responsible for assisting in preparation of cyber security related documents and initiate cyber security awareness campaigns within the organization and with associates. The main duties consist of assisting superiors in the preparation of security policy documents, preparing training material for security awareness campaigns, coordinating with departments in matters of security issues and assisting superiors in the conduct of security testing.

Personal Attributes: This job may require the individual to work independently in the collection of data and make decisions for his/her own area of work. The individual should have a high level of documentation drafting capability, passion for information security and attention for detail, should be ethical, compliance and result- oriented, should also be able to demonstrate interpersonal skills, along with willingness to undertake desk-based job with long working hours.

2. **Aim & Objectives of the Course:**

- Demonstrate an understanding of cyber defense and attack methods.
- Demonstrate an understanding of how traditional intelligence methods and procedures are applied to the cyber security domain.
- Comprehend and appreciate the legal and ethical environment impacting individuals as well as business organizations and have an understanding of the ethical implications of IT legal decisions.
- Improve cyber security skills and expand citizen sensitization and awareness.
- Reinforce prevention, detection, reaction, analysis, recovery and response skills to cope with cyber intrusion, cyber delinquency and cyber terrorism.
- Provide an avenue for the learner to obtain assistance for and to resolve issues related to cyber security, cyber safety and data privacy at least of a basic level

3. **Title of the course:**

Foundation course in Cyber Security

4. **Abbreviation of the Course:**

CCS

5. **Academic year in which course is to be initiated**

Academic year	Open to	Examination
2024-25	All Students	End of academic year

6. Eligibility criteria for admission to the course:

12th Standard OR Equivalent.

7. Structure of the course (course duration):

(45 hours)

Modules	Mandatory / Optional	Estimated size (learning hours)
CSF – Module 1 Fundamentals of Cyber Security	Mandatory	1
CSF – Module 2 Fundamentals of Networking	Mandatory	9
CSF – Module 3 Basic of Security Testing	Mandatory	9
CSF – Module 4 Fundamentals of Access Management	Mandatory	10
CSF – Module 5 Fundamentals of Incident Management & Response	Mandatory	9
CSF – Module 6 Fundamentals of Security Operations	Mandatory	7
Total		45

8. **Fee Structure:** The tuition fees and laboratory fees and other fees must be paid at the time of admission to the course. Students can opt for any one of the three learning modes. The course fees are as follows.

Blended Online Learning: Rs. 9,500=00 +GST

9. Teaching scheme of the course (mode of teaching and learning):

Blended Online Learning- Self Paced

10. Examination system:

On successful completion of examination, students will be awarded Certificate in Cyber Security by the University and Skills Factory Learning Private Limited jointly. The examination pattern for this Course is as follows:

Code	Title	Type	Distribution of marks			Credits
			Internal	Univ.	Total	
CCS	Certificate in Cyber Security	Theory, Practical cum Assignments	30	70	100	2

Mandatory Internal and External Evaluation: The course evaluation has two components: Internal assessment for 30 marks that may contain assignment/oral/viva/internal test, etc and the External examination will online mode for 70 marks.

11. Procedure for conducting External and Internal assessment:

Online assignment submission and online examination as per University Rules and schedule.

12. Grade System

- The examination outcome will not affect the regular academic examinations.
- Students will be awarded grades on the basis of marks achieved.
- The examination will be conducted for all modules at the end of the course.
- Criteria for assessment will be created by Skills Factory Learning Pvt Ltd (SFLPL). Each performance criterion@ (PC) will be assigned Theory and Skill Based Practical marks proportional to its importance in the module.
- The assessment will be conducted online through Skills Factory Learning Pvt Ltd (SFLPL)
- Format of questions will include a variety of styles suitable to the Performance Criteria (PC) being tested such as multiple choice questions, fill in the blanks, situational judgment, etc.

@Performance Criteria are statements that together specify the standard of performance required when carrying out an exam task.

13. Rules for Performance Improvement examination

- A Performance Improvement examination will be held by SFLPL after one month from the date of declaration of result.

- This Re-examination fees will be charged at Rs. 1000+ GST

14. Award of grades and credit allocation:

Marks	Grade
80 and above	A+
70 to 79	A
60 to 69	B
41 to 59	C
40 and less	D

External (Online) evaluation comprises of the aforesaid modules on the basis of following components:

Module	Examination Pattern	Type of questions	Marks
Module 1 Fundamentals of Cyber Security	Online Examination	Objective questions, MCQs	15
Module 2 Fundamentals of Networking	Online Examination	Objective questions, MCQs	15
Module 3 Basic of Security Testing	Online Examination	Objective questions, MCQs	15
Module 4 Fundamentals of Access Management	Online Examination	Objective questions, MCQs	15
Module 5 Fundamentals of Incident Management & Response	Online Examination	Objective questions	20
Module 6 Fundamentals of Security Operations	Online Examination	Objective questions	20
		Total	**100**

15. Basis for allocation of marks:

Course-related practical work will be entirely based on the skills to be developed in the students.It would include the topics as has been prescribed in the syllabi of every module

Internal Assessment: 30 marks

Practical components may be based on laboratory work, project, presentation etc. unless otherwise clearly specified in the syllabi of the modules

University Examination (External Evaluation): 70 marks

The marks would be clubbed with the internal assessment for the award of grades.

The Certificate in Cyber Security course is divided into 2 credits:

Sr. No.	Module No.	Module Name	No. of Credits	No of Hours	Marks
1	Module 1, 2	Fundamentals of Cyber Security Fundamentals of Networking	One credit for theory part and one credit for practical part totalling two credits as per syllabus	10	20
2	Module 3	Basics of Security Testing		9	20
3	Module 4	Fundamentals of Access Management		10	20
5	Module 5	Fundamentals of Incident Management and Response		9	20
6	Module 6	Fundamentals of Security Operations		7	20

Savitribai Phule Pune University

(Formerly University of Pune)

DEPARTMENT OF TECHNOLOGY

Syllabus

16. Model Syllabus for Certificate in Cyber Security:

Sl. No.	Module Name	Topics	Objective	Theory	Practical cum Assignment
				15	30
1	Fundamentals of Cyber Security	a) Definition of Cyber Security and its important in present scenario	a. Explain the fundamentals of Cyber Security and the relevance of Cyber Security	1 Hrs	
		b) Popular security events in the history of Cyber Security	b. Discuss different disciplines covered under Cyber Security.		
		c) Different disciplines of Cyber Security (such as application security, network security, data security, end-point security etc.)	c. Discuss differences between Information Security and Cyber Security.		
		d) Difference between Information Security and Cyber Security	d. Explain the CIA (Confidentiality, Integrity and Availability) guiding principles for information security.		
		e) Definition of CIA (Confidentiality, Integrity and Availability) Triad in Information Security	e. Discuss what cyber security is and different types of cyber security threats.		
		f) Definition of cyber security threats and their types	f. Discuss different types of malwares used to trigger cyber security incidents.		
		g) Types of malwares (such as Worms, Virus, Trojan Horse, Rootkit, Ransomware, Spyware, Adware, Logic Bomb etc.) and their characteristics	g. Explain different types of Cyber Security Attacks and their applications.		
		h) Types of Cyber Security Attacks and their applications (such DDoS/DoS attack, SQL injection attack, Phishing, Eavesdropping attack etc.)	h. Explain enterprise architecture and different components of enterprise architecture.		
		i) Basics of enterprise architecture and components (Networks, Security Controls, Servers, etc.)	i. Explain the basic concepts of Networking, Network Ports and Network Protocols		

2	Fundamentals of Networking	a) Basic concepts of Networking, Network Ports and Network Protocols	a. Different types of devices that constitute a network (such as Modem, Hub, NIC, Switch, Router etc.)	2 Hrs	7 Hrs
		b) Understanding of different types of network devices (such as Modem, Hub, NIC, Switch, Router, Repeater, Bridge etc.)	b. Explain common terminologies related to networking (such as MAC Address, IP Address, Domain Name System etc.)		
		c) Basics definitions of key networking terminologies (such as MAC Address, IP Address, DNS (Domain Name System) etc.)	c. Explain the uses of Ping and Traceroute to troubleshoot network issues		
		d) Basics of Ping and Traceroute	d. Explain different types of networks (such as Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN) etc.)		
		e) Types of network categories (such as Local Area Network (LAN), Wide Area Network (WAN), Virtual Private Network (VPN) etc.) and their components	e. Explain fundamentals of network models like OSI (Open System Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol)		
		f) Fundamental concept of OSI (Open System Interconnection) model and TCP/IP (Transmission Control Protocol/Internet Protocol) model	f. Explain different types of internet protocols (such as IPv4, IPv6 etc.)		
		g) Types of internet protocols (such as IPv4, IPv6 etc.)	g. Discuss how network sharing and subnetting is implemented		
		h) Basics of network sharing and subnetting	h. Discuss different components of network infrastructure		
		i) Fundamental concepts of network infrastructure and firewall	i. Explain the basic fundamentals of network firewall		
		Demonstrate how to set up a LAN (Local Area Network) network using a standard router and 3-4 personal computers installed with Windows/ Linux based operating system. Demonstrate how to look for IP Address and MAC addresses of devices connected in the network. Explain how to change the IPv4/IPv6 addresses of devices and systems connected to the network.			

3	Basics of Security Testing	a) Definition of security testing	a. Explain that security testing is	3 Hrs	6 Hrs
		b) Importance of security testing and its reals world implications	b. Describe the importance of security testing and its real-world applications		
		c) Basics concepts of Vulnerability Scanning test and its applications	c. Discuss the different types of security tests		
		d) Basics concepts of Security Scanning test and its applications	d. Explain the basic concept of Vulnerability Scanning test and its applications		
		e) Basics concepts of Penetration test and its applications	e. Explain the basic concept of Security Scanning test and its applications		
		f) Basics concepts of Risk Assessment test and its applications	f. Explain the basic concept of Penetration test and its applications		
		g) Basics concepts of Security Auditing test and its applications	g. Explain the basic concept of Risk Assessment test and its applications		
		h) Basics concepts of Posture Assessment test and its applications	h. Explain the basic concept of Security Audit test and its applications		
		i) Definition of Ethical Hacking and its application and its applications	i. Explain the basic concept of Posture Assessment test and its applications		
		j) Fundamentals of network monitoring for threats	j. Define Ethical Hacking and explain its applications		
		k) Types of popular security testing tools and their applications	k. Discuss the fundamental concept of network monitoring		
		Demonstrate how to penetrate a dummy website using standard web penetration tool. One can use Vega tool found in Kali Linux for this. Similarly demonstrate how to scan for vulnerabilities in the website using a standard vulnerability assessment tool. One can also use OWASP tool found in Kali Linux for this purpose.	l. Discuss the popular security test tools available and their applications		

4	Fundamentals of Access Management	a) Definition of Identity and Access Management	a. Explain the fundamentals of Identity and Access Management (IAM)	3 Hrs	7 Hrs
		b) Importance of Identity and Access Management in Information Security and Cyber Security	b. Discuss the importance of (IAM) in Information Security and Cyber Security		
		c) Basic concepts of User Identification, Authentication and Authorization	c. Explain the fundamental concepts of User Identification, Authentication and Authorization		
		d) Basic understanding of user Identification and Access Management policies	d. Discuss common user Identification and Access Management policies		
		e) Basic access control models	e. Discuss different types of security controls		
		f) Types of security authorizations and encryptions	f. Explain different types of user authorization and encryptions		
		g) Basics of Single Sign On (SSO) authentication	g. Explain the basics of Single Sign On (SSO) authentication		
		h) Best practices followed under access management	h. Discuss the best practices followed under IAM		
		Demonstrate Identity and Access Management in practise using standards tools provided by a public cloud platform provider (such as AWS, Azure, Google Cloud etc.). Demonstrate how to create access policies and enable or disable access for specific users.	i. Define what security controls are		
	Fundamentals of Incident Management and Response	a) Basic understanding of different types of security controls and their applications (such as deterrence, detection, prevention, correction etc.)	a) Discuss different types of security controls and their applications (such as deterrence, detection, prevention, correction etc.)	3 Hrs	6 Hrs
		b) Definition of a security policy and security policy frameworks	b) Explain security policies and different types of security policy frameworks		
		c) Basic definitions of Incident management and Incident response	c) Discuss the fundamentals of incident management and incident response e) Discuss the fundamentals of disaster mitigation and containment		
		d) Definition of an incident response plan and incident communications plan	d) Define Business Continuity Plans and fundamentals of Disaster Recovery		

		e) Fundamental concepts of incident monitoring and identification	e) Explain different types of cyber security investigation		
		f) Fundamental concepts of disaster mitigation and containment	f) Define a backup and recovery plan		
		g) Basic definitions of Business Continuity Planning and Disaster recovery	g) Explain the basics of RTO (recovery Time Objective) and RPO (Recovery Point Objective)		
		h) Types of cyber security investigation (such as operational investigation, criminal investigation, civil investigation and regulatory investigation)			
		i) Definition of a back and recovery plan			
		j) Basic concepts of RTO (recovery time objective) and RPO (recovery point objective)			
		Demonstrate how to create a disaster recovery plan for a web application where the database server is affected by a malware. Use standards software, tools and packages such as MySQL, Linux, Apache etc. to create the web application and back-up for the web application's database.			
6	Fundamentals of Security Operations	a) Fundaments of security forensics	a) Discuss the fundamentals and applications of security forensics	3 Hrs	4 Hrs
		b) Types of security forensics (such as System and file forensics, network forensics, software forensics, embedded device forensics etc.)	b) Explain different types of security forensics		
		c) Understanding of system logging and security monitoring	c) Explain how to monitor security of systems using system logs		
		d) Fundamentals of continuous security monitoring	d) Discuss the basic concepts of continuous security monitoring		
		e) Techniques used for continuous security monitoring (such as anomaly analysis, trend analysis, behavioural analysis, availability analysis etc.)	e) Explain different techniques used for continuous security monitoring		
		f) Basics of data loss prevention and its importance	f) Discuss how to prevent loss of data		
		g) Basic understanding of change and configuration management	g) Explain the basics of change management		
		h) Types of tools used for security monitoring	h) Define configuration management and its security implications		

		Deploy a standard web application and demonstrate how to monitor different systems (such as network, servers etc.) using standards security information and event management (SIEM) tools. (such as IBM QRadar, Splunk Enterprise Security etc.)	i) Discuss common tools used for monitoring system security		

17. **Course Outcome:**

- Increased protection of networks and data from unauthorized access. Reduction in number of attack incidents
- Effective implementation of methods and procedures in gathering intelligence leading to applying the right security controls.
- Comprehensive coverage of legal aspects through awareness programs in creating Cyber Security conscious users, well-informed on the legal consequences of not implementing cyber security measures.
- Participants motivated to implement security measures. Implementation of cyber security risk management policies in order to adequately protect an organization's critical information and assets.
- Formulation and updating of short and long-term organizational cyber security strategies and policies.
- Development of knowledge of cyber security tools, techniques and technologies. Development of an understanding of risk assessment and management methods related to cyber security and national critical infrastructure.
- Work effectively with colleagues.
- Maintain a healthy, safe and secure working environment.
- Provide data/information in standard formats.
- Develop knowledge, skills and competence.

18. **Book Recommendation:**

Certificate in Cyber Security textbook by Skills Factory Learning Pvt Ltd.