University of Mumbai

Website - mu.ac.in
Email id - dr.aams@fort.mu.ac.in
aams3@mu.ac.in

Academic Authorities,
Meetings & Services (AAMS)
Room No. 128, M. G. Road, Fort,
Mumbai – 400 032.
Tel. 022-68320033

Re- accredited with A ++ Grade (CGPA 3.65) by NAAC
Category- I University Status awarded by UGC

No. AAMS_UGS/ICD/2024-25/468 Date : 24th March, 2025.

To,
The Director,
Garware Institute of Career Education
and Development,
Vidyanagari
Santacruz (East)
Mumbai – 400 098.

Sub : Post Graduate Diploma in Cyber Security.
(One year) (Sem – I & II).

Sir,

With reference to the subject noted above, this is to inform you that the recommendations made by the **Advisory Committee & Board of Management** of Garware Institute of Career Education & Development at its Meeting held on **4th September, 2023** & resolution passed by the **Board of Deans** at its meeting held on **9th August,2023 vide** Item No. **9.2** have been accepted by the **Academic Council** at its meeting held on **1st November, 2023 vide** Item no. **9.3 (B) 13 (N)** and subsequently approved by the **Management Council** at its meeting held on **14th August, 2024 vide** Item No. **6** that in accordance therewith, in exercise of the powers conferred upon the Management Council under Section 74(4) of the Maharashtra Public Universities Act, 2016 (Mah. Act No. VI of 2017) the following program with Ordinance for Title of the Program, Eligibility and Regulation numbers for Duration of Program, Intake Capacity, Scheme of Examinations, Standard of Passing and Credit Structure along with syllabus of **Post Graduate Diploma in Cyber Security (Sem I & II)** (Appendix – 'A') have been introduced and the same have been brought into force with effect from the academic year **2023-24**.

The New Ordinances & Regulations as per NEP 2020 is as follows :-

Sr. No	Name of the Programme	Ordinance no. for Title	Ordinance no for Eligibility	Duration
A	P.G Diploma in Cyber Security	O.GPA – 53 A	O.GPA – 54 A	One year

2/-

University of Mumbai

Website - mu.ac.in
Email id - dr.aams@fort.mu.ac.in
aams3@mu.ac.in

Academic Authorities,
Meetings & Services (AAMS)
Room No. 128, M. G. Road, Fort,
Mumbai – 400 032.
Tel. 022-68320033

Re- accredited with A ++ Grade (CGPA 3.65) by NAAC
Category- I University Status awarded by UGC

No. AAMS_UGS/ICD/2024-25/468 Date : 24th March, 2025.

Regulation Nos	
Duration	R. GPA – 126
Intake Capacity	R. GPA – 127
Scheme of examination	R. GPA – 128
Standard of Passing	R. GPA – 129
Credit Structure	R. GPA – 130 A
	R. GPA – 130 B

(Dr. Prasad Karande)
REGISTRAR

A.C/9.3(B) 13 (N) /01/11/2023
M.C/6/14/8/2024

****

Copy forwarded with Compliments for information to:-

1) The Chairman, Board of Deans
2) The Dean, Faculty of Interdisciplinary Studies,
3) The Director, Board of Examinations and Evaluation,
4) The Director, Board of Students Development,
5) The Director, Department of Information & Communication Technology,
6) The Co-ordinator, MKCL.

Copy forwarded for information and necessary action to :-	
1	The Deputy Registrar, (Admissions, Enrolment, Eligibility and Migration Dept)(AEM), dr@eligi.mu.ac.in
2	The Deputy Registrar, Result unit, Vidyanagari drresults@exam.mu.ac.in
3	The Deputy Registrar, Marks and Certificate Unit,. Vidyanagari dr.verification@mu.ac.in
4	The Deputy Registrar, Appointment Unit, Vidyanagari dr.appointment@exam.mu.ac.in
5	The Deputy Registrar, CAP Unit, Vidyanagari cap.exam@mu.ac.in
6	The Deputy Registrar, College Affiliations & Development Department (CAD), deputyregistrar.uni@gmail.com
7	The Deputy Registrar, PRO, Fort, (Publication Section), Pro@mu.ac.in
8	The Deputy Registrar, Executive Authorities Section (EA) eau120@fort.mu.ac.in He is requested to treat this as action taken report on the concerned resolution adopted by the Academic Council referred to the above circular.
9	The Deputy Registrar, Research Administration & Promotion Cell (RAPC), rapc@mu.ac.in
10	The Deputy Registrar, Academic Appointments & Quality Assurance (AAQA) dy.registrar.tau.fort.mu.ac.in ar.tau@fort.mu.ac.in
11	The Deputy Registrar, College Teachers Approval Unit (CTA), concolsection@gmail.com
12	The Deputy Registrars, Finance & Accounts Section, fort draccounts@fort.mu.ac.in
13	The Deputy Registrar, Election Section, Fort drelection@election.mu.ac.in
14	The Assistant Registrar, Administrative Sub-Campus Thane, thanesubcampus@mu.ac.in
15	The Assistant Registrar, School of Engg. & Applied Sciences, Kalyan, ar.seask@mu.ac.in
16	The Assistant Registrar, Ratnagiri Sub-centre, Ratnagiri, ratnagirisubcentar@gmail.com
17	The Director, Centre for Distance and Online Education (CDOE), Vidyanagari, director@idol.mu.ac.in
18	Director, Innovation, Incubation and Linkages, Dr. Sachin Laddha pinkumanno@gmail.com
19	Director, Department of Lifelong Learning and Extension (DLLE), dlleuniversityofmumbai@gmail.com

Copy for information :-	
1	P.A to Hon'ble Vice-Chancellor, vice-chancellor@mu.ac.in
2	P.A to Pro-Vice-Chancellor pvc@fort.mu.ac.in
3	P.A to Registrar, registrar@fort.mu.ac.in
4	P.A to all Deans of all Faculties
5	P.A to Finance & Account Officers, (F & A.O), camu@accounts.mu.ac.in

To,

1	The Chairman, Board of Deans pvc@fort.mu.ac.in
2	**Faculty of Humanities,** **Dean** 1. Prof.Anil Singh Dranilsingh129@gmail.com **Associate Dean** 2. Dr.Suchitra Naik Naiksuchitra27@gmail.com 3.Prof.Manisha Karne mkarne@economics.mu.ac.in
	Faculty of Commerce & Management, **Dean** 1. Dr.Kavita Laghate kavitalaghate@jbims.mu.ac.in **Associate Dean** 2. Dr.Ravikant Balkrishna Sangurde Ravikant.s.@somaiya.edu 3. Prin.Kishori Bhagat kishoribhagat@rediffmail.com

	Faculty of Science & Technology **Dean** 1. Prof. Shivram Garje ssgarje@chem.mu.ac.in **Associate Dean** 2. Dr. Madhav R. Rajwade Madhavr64@gmail.com 3. Prin. Deven Shah sir.deven@gmail.com
	Faculty of Inter-Disciplinary Studies, **Dean** 1.Dr. Anil K. Singh aksingh@trcl.org.in **Associate Dean** 2.Prin.Chadrashekhar Ashok Chakradeo cachakradeo@gmail.com
3	Chairman, Board of Studies,
4	The Director, Board of Examinations and Evaluation, dboee@exam.mu.ac.in
5	The Director, Board of Students Development, dsd@mu.ac.in DSW direcotr@dsw.mu.ac.in
6	The Director, Department of Information & Communication Technology, director.dict@mu.ac.in

AC-1/11/2023
Item No- 9.3(B) - 13

As Per NEP 2020

University of Mumbai

Syllabus for
Post Graduate Diploma in Cyber Security

(Garware Institute of Career Education and Development)

Semester- Sem I & II

Ref: GR dated 16th May, 2023 for Credit Structure of PG

(with effect from the academic year 2023-24)

UNIVERSITY OF MUMBAI

(AS PER NEP 2020)

Sr. No.	Heading	Particulars
1	O: GPA- 53A Title of the Course	Post Graduate Diploma in Cyber Security
2	O: GPA- 54A Eligibility	Graduate In Any Faculty
3	Duration of Program R: GPA- 126	1 Years
4	R: GPA- 127 Intake Capacity	60
5	R: GPA- 128 Scheme of Examination	50 Internal – Continuous Evaluation 50 External- Semester End Exam
6	Standards of Passing R: GPA- 129	50% in each component
7	Credit Structure R: GPA- 130A R: GPA- 130B	Attached herewith
8	No. of Years / Semesters :	One year, Sem I & II
9	Program Level :	60
10	Pattern :	Semester
11	Status :	New
12	To be implemented from Academic Year.	From Academic Year 2023-24

Dr. Keyurkumar M. Nayak,
Director,
UM-GICED

Prof.(Dr.) Anil Kumar Singh
Dean,
Faculty of Interdisciplinary Studies

SYLLABUS FOR POST-GRADUATE DIPLOMA IN CYBER SECURITY

Introduction:

The Post Graduate Diploma in Cyber Security is a specialized program designed to equip students with the knowledge and skills required to combat evolving cyber threats in today's digital landscape. This program provides a comprehensive understanding of cybersecurity principles, technologies, and best practices, enabling students to protect sensitive information, secure network infrastructures, and effectively respond to cyber incidents.

Aims and Objectives:

The program objectives of the Post Graduate Diploma in Cyber Security are to develop expertise in identifying and mitigating cyber threats, design and implement secure network infrastructures, understand legal and regulatory aspects of cybersecurity, and effectively respond to and recover from cyber incidents.

Course Objectives:

The course objectives of the Post Graduate Diploma in Cyber Security aim to equip students with the necessary skills and knowledge to effectively address cyber threats. Students will develop expertise in identifying and mitigating vulnerabilities, gaining in-depth knowledge of cybersecurity frameworks and best practices. These objectives collectively prepare students to excel in the field of cybersecurity and contribute to protecting sensitive information and ensuring secure digital environments.

Learning Outcomes:

CO1: Demonstrate a comprehensive understanding of cybersecurity principles, methodologies, and technologies.

CO2: Apply industry-standard techniques and tools to assess, prevent, and detect cyber threats.

CO3: Design and implement secure network architectures, ensuring confidentiality, integrity, and availability of data.

CO4: Evaluate and recommend security measures to protect against vulnerabilities and emerging cyber threats.

CO5: Effectively communicate and collaborate with stakeholders on cybersecurity issues and solutions.

SEMESTER-WISE SYLLABUS

Post Graduate Diploma in Cyber Security

Year (1 Yr PGD CS)	Level	Sem (1 Yr)	Major		RM	OJT / FP	RP	Cum.Cr.	Degree
			Mandatory*	Electives Any set					
I	6.0	Sem I	Course 1 : Fundamentals of Computer Security and Cryptography (Credits 4) Course 2 : Network Security and Attacks (Credits 4) Course 3 : Web Application Security and Attacks (Credits 4) Course 4 : Cyber security and ethical Hacking (Credits 2)	Set 1 Course 1 : Vulnerabilities and Attacks (Credits 2) AND Course 2 : Cloud Fundamentals and Cloud Security (Credits 2) OR Set 2 Course 1 : Internet of Things Security (IoT) (Credits 4)	Research Methodology (Credits 4)			22	PG Diploma
		Sem II	Course 1 : Principles of Security Models, Design, and Capabilities (Credits 4) Course 2 : Cyber Security Analysis & Counter measures and Advance Security Analysis (Credits 4) Course 3 : Penetration Testing (Credits 4) Course 4 : Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques (Credits 2)	Credits 4 Set 1 Course 1 : Information Security Compliance Management (Credits 2) AND Course 2 : Cyber Crime Investigation (Credits 2) OR Set 2 Course 1: Mobile Eco-System Security (Credits 4)		OJT / FP (Credits 4)		22	
Cum. Cr. For PG Diploma			28	8	4	4	-	44	

Dr. Keyurkumar M. Nayak,
Director,
UM-GICED

Prof.(Dr.) Anil Kumar Singh
Dean,
Faculty of Interdisciplinary Studies

SEMESTER-WISE SYLLABUS

Post Graduate Diploma in Cyber Security							
	Subject Code	Core Subjects	Assessment Pattern			Teaching Hours	
			Internal Mark	External Marks	Total Marks	Total Hrs	Total Credits
	Major Mandatory						
SEM I	PGDCSSIMJP1	Fundamentals of Computer Security and Cryptography	50	50	100	60	4
	PGDCSSIMJP2	Network Security and Attacks	50	50	100	60	4
	PGDCSSIMJP3	Web Application Security and Attacks	50	50	100	60	4
	PGDCSSIMJP4	Cyber security and ethical Hacking	25	25	50	30	2
	Major ELECTIVES: Set 1						
	PGDCSSIMJP5A	Vulnerabilities and Attacks	25	25	50	30	2
	PGDCSSIMJP5B	Cloud Fundamentals and Cloud Security	25	25	50	30	2
	OR						
	Major ELECTIVES: Set 2						
	PGDCSSIMJP5C	Internet of Things Security (IoT)	50	50	100	60	4
	RM						
	PGDCSSIP6	Research Methodology	50	50	100	60	4
		TOTAL	275	275	550	330	22
	Major Mandatory						
SEM II	PGDCSS2MJP7	Principles of Security Models, Design, and Capabilities	50	50	100	60	4
	PGDCSS2MJP8	Cyber Security Analysis & Counter measures and Advance Security Analysis	50	50	100	60	4
	PGDCSS2MJP9	Penetration Testing	50	50	100	60	4
	PGDCSS2MJP10	Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques	25	25	50	30	2
	Major ELECTIVES: Set 1						
	PGDCSS2MJP11A	Information Security Compliance Management	25	25	50	30	2
	PGDCSS2MJP11B	Cyber Crime Investigation	25	25	50	30	2
	OR						
	Major ELECTIVES: Set 2						
	PGDCS2MJP11C	Mobile Eco- System Security	50	50	100	60	4
	OJT/ FP						
	PGDCSS2P12	OJT/ FP	100	0	100	60	4
		TOTAL	275	275	550	330	22
FINAL TOTAL			600	500	1100	660	44

Sem.- I

SUBJECT-WISE SYLLABUS
Semester 1

Subject Code	Subjects	Total Hours	No of Sessions of 3 Hours
	SEMESTER I: Mandatory		
1.1	**Fundamentals of Computer Security and Cryptography** **Fundamentals of Computer Security** **Unit 1. Introduction to Cyber Security** Cyber Security Fundamentals Enterprise Architecture and Components Information System Governance and Risk Assessment Incident Management **Unit 2. Use appropriate software tools to assess the security posture of an organization.** Command line tools (ping, netstat, tracert, Arp, ipconfig/Ip/ifconfig) **Unit 3. Implement secure network architecture concepts.** Segregation/segmentation/isolation (Virtualization) . Summarize cloud and virtualization concepts. Hypervisor (Type I, Type II, Application cells/containers), VM sprawl avoidance, VM escape protection, VDI/VDE **Unit 4. Using resiliency and automation strategies reduce risk.** Non-persistence (Snapshots, revert to known state, Rollback to known configuration), Elasticity, Scalability . Compare and contrast various types of controls. Deterrent, Preventive, Detective, Corrective, Compensating, Technical, Administrative, Physical . Compare and contrast basic concepts of cryptography. **Unit 5. Common use cases** (Supporting confidentiality, Supporting integrity, supporting obfuscation, Supporting non-repudiation **Cryptography** **Unit 1 -** Classical Ciphers Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher. Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation, **Unit 2 -** Secret Key Cryptography Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced	60	20

	Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family **Unit 3 -** Public Key Cryptography and Bitcoins Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis. **Unit 4 -** Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining. **Unit 5 -** Message authentication code and Hash Functions Message authentication code Authentication functions, Hash Functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.		
1.2	**Network Basics and Network Security and Network Attacks** **Network Basics and Network Security** **Unit 1 -** Introduction to Network Security Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers, Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based). **Unit 2 -** Virtual Private Networks VPN and its types – Tunnelling Protocols – Tunnel and Transport Mode – Authentication Header Encapsulation Security Payload (ESP)-IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation (GRE). Implementation of VPNs. **Unit 3 -** Network Attacks Part 1 Network Sniffing, Wireshark, packet analysis, display and capture filters, Ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta, Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting, **Unit 4 -** Network Attacks Part 2 Network Exploitation OS Detection in network, Nmap, open ports, filtered ports, service detection, Metasploit framework, interface of Metasploit framework, network vulnerability assessment, evade anti viruses and firewalls, Metasploit scripting, exploits, vulnerabilities, payloads, custom payloads, Nmap configuration, Social	60	20

	Engineering toolkit, Xero sploit Framework, exploits delivery. Endpoint Security. **Unit 5 -** Wireless Attacks Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentications, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework **Network Attacks** **Unit 1 -** Email Hacking & Tracing, Malware Attacks, Backdoors, & Handheld Devices Analysis **Unit 2 -** DoS, DDoS, Buffer Overflow Attacks**,** Network Packet Analysis, Sniffing, & Spamming **Unit 3 -** Compare and contrast types of attacks. ● Application/service attacks (ARP poisoning, DNS poisoning) - Install and configure network components, to support organizational security. ● Firewall (ACL, Application-based vs. network-based, Stateful vs. stateless, Implicit deny), Router (ACLs, Anti Spoofing), Switch (Port security, Layer 2 vs. Layer 3, Loop prevention, Flood guard), Proxy (Forward and reverse proxy, Transparent, Application/multipurpose), Mail gateway (Spam filter, DLP, Encryption), Bridge, Media gateway **Unit 4 -** Use appropriate software tools to assess the security posture of an organization. ● Command line tools(nslookup/dig) **Unit 5 -** Troubleshoot common security issues. ● Misconfigured devices (Firewall, Content filter) - Analyse and interpret output from security technologies. Host-based firewall, UTM, Web application firewall		
1.3	**Fundamentals of Web Designing and Web Application Security and Application Attacks** **Fundamentals of Web Designing and Web Application Security** **Unit 1 -** Web Designing and Penetration Testing Process Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting-Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis.	60	20

	Unit 2 - PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup **Unit 3 -** Web Application and Information Gathering HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ. **Unit 4 -** Web Application Attacks Part I: SQL Injections & Cross Site Scripting SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation. Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation **Unit 5 -** Web Application Attacks Part II Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks. **Application Attacks** **Unit 1 –** Windows-8 Analysis and Hacking **Unit 2 –** Google Hacking **Unit 3 –** Application Password Hacking **Unit 4 –** Reverse Engineering **Unit 5 -** Software Cracking Techniques		
1.4	**Cyber Security and Ethical Hacking** **Unit 1 –** Basics of Networking	30	10

	Unit 2 – Introduction to Cyber Security **Unit 3 –** Information Gathering **Unit 4 –** Physical Security **Unit 5 –** Mini Group Project		
Semester 1: ELECTIVES			
SET 1: Electives			
1.5	**Vulnerabilities & Attacks** **Unit 1 -** Web Application Vulnerabilities **Unit 2 -** Session Hijacking & SQL Injection **Unit 3 -** Phishing & Financial Frauds **Unit 4 -** Security Protocols	30	10
1.6	**Cloud Fundamentals and Cloud Security** **Unit 1 -** Introduction to Cloud Computing Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefit challenges of cloud computing, public vsprivateclouds, role of virtualiza enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications. **Unit 2 -** Cloud Application Architecture Technologies and the processes required when deploying web services; Deploying a web service from in and outside a cloud architecture, advantages and disadvantages. **Unit 3 -** Cloud Services Management Reliability, availability and securi services deployed from the cloud. Performance and scalability of service tools and technologies used to manage cloud services deployment; Clou Economics: Cloud Computing infrastructures available for implementin cloud-based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints a business needs. Discuss industry cases including open sources. **Unit 4 -** Cloud Application Development Service creation environments develop cloud-based applications. Development environments for servic development; Amazon, Azure, Google App. Applicability of laws to dat stored outside the nation's boundary. **Unit 5 -** Cloud IT Model Analysis of Cases while deciding to adopt secu cloud computing architecture. Appropriate cloud requirements. Secure C based service, Applications and development platform deployment so as improve the total cost of ownership (TCO)	30	10

	OR		
	SET 2: Electives		
1.7	**Internet of Things Security (IoT)** **Unit 1 -** Introduction Requirement and Basic Properties in Internet of Things, Primary challenges in security maintenance, Confidentiality, Integrity, Availability, Non-Repudiation. **Unit 2 -** Architecture of Internet of Things Device - device, Device - Cloud, Device - Gateway, Gateway - Cloud, Cloud – Backend - Applications **Unit 3 -** Security Classification and Access Control Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity **Unit 4 -** Attacks and Implementation of Internet of Things Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices **Unit 5 -** Security Protocols and Management Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management	60	20

Sem.- II

Semester 2

Subject Code	Subjects	Total Hours	Session of 3 Hours
SEMESTER II: Mandatory			
2.1	**Principles of Security Models, Design, and Capabilities** **Unit 1 -** Implement and manage engineering processes using secure design principles **Unit 2 -** Understand the fundamental concepts of security models **Unit 3 -** Select controls based upon systems security requirements **Unit 4 -** Understand security capabilities of information systems	60	20
2.2	**Cyber Security Analysis and Countermeasures and Advance Security Analysis** **Cyber Security Analysis and Countermeasures** **Unit 1 -** Firewall Technologies **Unit 2 -** IDS, IPS & Honeypots Analysis	60	20

	Unit 3 - Hacking Routers, Cable Modems, and Firewall **Unit 4 -** Cryptography with different Applications **Advance Security Analysis** **Unit 1 -** Internet Content Filtering Techniques **Unit 2 -** Securing Gadgets **Unit 3 -** Introduction to ISO 27001 & Security Policies **Unit 4 -** Disaster Recovery & Planning		
2.3	***Penetration Testing*** **Unit 1 -** Linux Hacking **Unit 2 -** Hacking Wireless Networks. **Unit 3 -** Exploit Analysis. **Unit 4 -** Network & Web Audits	60	20
2.4	**Supervisory Control and Data Acquisition (SCADA) System and Information Hiding Techniques** **Unit 1 -** Introduction Network Segmentation and Segregation , Boundary Protection, Firewalls , Logically Separated Control Network , Network Segregation, Recommended Defence-in-Depth Architecture, General Firewall Policies for ICS , Recommended Firewall Rules for Specific Services , Network Address Translation (NAT), Specific ICS Firewall Issues , Unidirectional Gateways , Single Points of Failure, Redundancy and Fault Tolerance , Preventing Man-in-the-Middle Attacks , Authentication and Authorization , Monitoring, Logging, and Auditing, Monitoring, Logging, and Auditing , Response, and System Recovery **Unit 2 -** Network Segregation Dual-Homed Computer/Dual Network Interface Cards (NIC), Firewall between Corporate Network and Control Network, Firewall and Router between Corporate Network and Control Network, Firewall with DMZ between Corporate Network and Control Network, Paired Firewalls between Corporate Network and Control Network, Network Segregation Summary **Unit 3 -** Recommended Firewall Rules for Specific Services Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), FTP and Trivial File Transfer Protocol (TFTP), Telnet, Dynamic Host Configuration Protocol (DHCP), Secure Shell (SSH), Simple Object Access Protocol (SOAP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Distributed Component Object Model (DCOM), SCADA and Industrial Protocols: DNP3 Protocol. Smart Grid Security. **Unit 4 -** Information Hiding Techniques Introduction to Steganography, Watermarking. Differences between Watermarking and Steganography, A Brief History. Digital Steganography, Applications of Steganography, Covert Communication, Techniques of steganography (for Text and	30	10

	Image) . Steganographic Software: S-Tools, StegoDos, EzStego, Jsteg-Jpeg. **Unit 5 -** Digital Water Marking Classification in Digital Watermarking, Classification Based on Characteristics: Blind versus Nonblind, Perceptible versus Imperceptible, Private versus Public, Robust versus Fragile, Spatial Domain-Based versus Frequency Domain-Based. Classification Based on Applications: Copyright Protection Watermarks, Data Authentication Watermarks, Fingerprint Watermarks, Copy Control Watermarks, Device Control Watermarks. Watermarking Techniques for Visible and Invisible Watermarks. Watermarking tools: uMark, TSR Watermark. Steganalysis		

Semester 2: ELECTIVES			
SET 1: Electives			
2.5	**Information Security Compliance Management** **Unit 1 -** Introduction to Information Security Management System (ISMS) - ISO/IEC 27001 Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information security, ISO/IEC 27001 certification process, Information Security Management System (ISMS), detailed presentation of the clauses 4 to 8 of ISO/IEC 27001 **Unit 2 -** Planning and Initiating an ISO/IEC 27001 audit Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting **Unit 3 -** Conducting an ISO/IEC 27001 audit Communication during the audit, Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities. Concluding and ensuring the follow-up of an ISO/IEC 27001 audit, Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans, ISO/IEC 27001 Surveillance audit, internal audit management program **Unit 4 -** PCI DSS, HIPPA Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from Malicious Software, Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption **Unit 5 -** Intellectual Property Rights Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.	30	10
2.6	**Cyber Crime Investigation** **Unit 1 -** Cyber Crime Investigation	30	10

	Unit 2 - Cyber Warfare, Terrorism & Social Networking **Unit 3 -** Cyber Forensics and Incident Handling **Unit 4 -** Case Study		
	OR		
SET 2: Electives			
2.7	**Mobile Eco- System Security** **Unit 1 -** Introduction to Mobile Eco-System Security Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm. **Unit 2 -** Mobile Eco-System Technology Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery **Unit 3 -** Mobile Eco-System Networks Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications **Unit 4 -** Management Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools **Unit 5 -** Scenario Testing Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS	60	20

PASSING PERFORMANCE GRADING :
The Performance Grading of the learner shall be on ten point scale be adopted uniformly.

Letter Grades and Grade Point

Semester GPA/ Program CGPA Semester / Program	% of Marks	Alpha-Sign/Letter Grade Result	Grading Point
9.00 – 10.00	90.0 - 100	O (Outstanding)	10
8.00 - < 9.00	80.0 < 90.0	A+ (Excellent)	9
7.00 - < 8.00	70.0 < 80.0	A (Very Good)	8
6.00 - < 7.00	60.0 < 70.0	B+ (Good)	7
5.50 - < 6.00	55.0 < 60.0	B (Average)	6
5.00 - < 5.50	50.0 < 55.0	C (Pass)	5
Below 5.00	Below 50	F (Fail)	0
AB (Absent)		Absent	

NOTE : VC : Vocational Courses, SEC : Skill Enhancement Courses, AEC : Ability Enhancement Courses, VEC : Value Education Courses, VSC : Vocational Skill Course, IKS : Indian Knowledge System, OJT: On The Job Training, FP: Field Projects.

The performance grading shall be based on the aggregate performance of Internal Assessment and Semester End Examination.

The Semester Grade Point Average (SGPA) will be calculated in the following manner: SGPA = $\sum CG / \sum C$ for a semester, where C is Credit Point and G is Grade Point for the Course/ Subject.

The Cumulative Grade Point Average (CGPA) will be calculated in the following manner: CGPA = $\sum CG / \sum C$ for all semesters taken together.

PASSING STANDARD:

Passing 50% in each subject /Course separate Progressive Evaluation (PE)/Internal Evaluation and Semester-End/Final Evaluation (FE) examination.

A. Carry forward of marks in case of learner who fails in the Internal Assessments and/ or Semester-end examination in one or more subjects (whichever component the learner has failed although passing is on total marks).
B. A learner who PASSES in the Internal Examination but FAILS in the Semester-end Examination of the Course shall reappear for the Semester-End Examination of that Course. However, his/her marks of internal examinations shall be carried over and he/she shall be entitled for grade obtained by him/her on passing.
C. A learner who PASSES in the Semester-end Examination but FAILS in the Internal Assessment of the course shall reappear for the Internal Examination of that Course. However, his/her marks of Semester-End Examination shall be carried over and he/she shall be entitled for grade obtained by him/her on passing

ALLOWED TO KEEP TERMS (ATKT)

A. A learner shall be allowed to keep term for Semester II irrespective of the number of heads/courses offailure in the Semester I.

B. A learner shall be allowed to keep term for Semester III wherever applicable if he/she passes each ofSemester I and Semester II.

OR

C. A learner shall be allowed to keep term for Semester III wherever applicable irrespective of the numberof heads/courses of failure in the Semester I & Semester II.

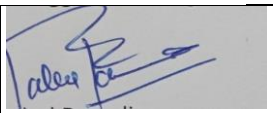
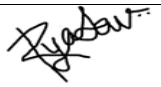
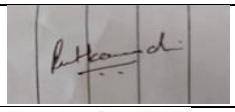
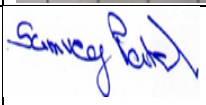
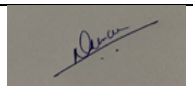
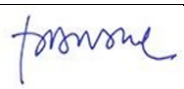
D. A learner shall be allowed to keep term for Semester IV wherever applicable if he/she passes each ofSemester I, Semester II and Semester III.

OR

E. A learner shall be allowed to keep term for Semester IV wherever applicable irrespective of number ofheads/courses of failure in the Semester I, Semester II, and Semester III

****

University of Mumbai's
Garware Institute of Career Education and Development
Board of Studies – Committee members
Course Name: Post Graduate Diploma In Cyber Security
Date- 5th June, 2023 & Time- 11.00 am

Sr. No.	Name	Signature
1	Dr. Keyurkumar Nayak Director, UM-GICED and Chairman- BOS	
2	Smt. Shilpa Borkar, Placement Officer	
3	Rahul Ranadive Course Coordinator Member Secretary	
4	Mr. Roshani Yadav Industry Experts	
5	Mr. Afshan Dadan Industry Experts	AB
6	Mr. Parth Shah Alumni	AB
7	Ms. Reet Kanodia Alumni	
8	Dr. Samveg Patel NMIMS	
9	Dr. Abhilas Nair Professor IIMK	AB
10	Mr. Rakesh Nair Subject Experts	
11	Dr. Pallavi Gupta Subject Experts	

Dr. Keyurkumar M. Nayak,
Director,
UM-GICED

Prof.(Dr.) Anil Kumar Singh
Dean,
Faculty of Interdisciplinary Studies

Appendix B

Justification for (P.G Diploma in Cyber Security)

1.	Necessity for starting the course	The University of Mumbai's Garware Institute of Career Education & Development plans to introduce a one year Post Graduate Diploma in Cyber Security. Information technology boom has made Cybersecurity critical as it protects organizations and individuals from cyber attacks, preventing data breaches, identity theft, and other types of cybercrime. Every organization requires protecting infrastructure, including securing data and information, running risk analysis and mitigation, architecting cloud-based security, achieving compliance and much more which will be fulfilled by candidates after completion of this course.
2.	Whether the UGC has recommended the course:	Yes, UGC has recommended the course as per gazette no. DL(N)-04/0007/2003-05 dated 11th July 2014. UGC encourages the incorporation of skill oriented and value-added courses to develop skilled manpower.
3.	Whether all the courses have commenced from the academic year 2023-2024	Yes, it would be commencing from the Academic year 2023-24 as per NEP 2020. However, the course was launched in the year 2021.
4.	The courses started by the University are self-financed, whether adequate number of eligible permanent faculties are available?	Yes, this course is self-financed. The expert visiting faculty from industries come to teach this course.
5.	To give details regarding the duration of the Course and is it possible to compress the course?	The duration of the course is One year (Two Semester). It cannot be further compressed.
6.	The intake capacity of each course and no. of admissions given in the current academic year:	The intake capacity of this course is 60 students.The admission procedure is still ongoing.
7.	Opportunities of Employability/ Employment available after undertaking these courses:	Employment opportunities in FinTech Companies as Cyber Security Analyst, Security Architect, Cyber Security Manager, Information Security Officer, Ethical Hackers, Cybersecurity Consultant, Cloud Security Officer

Dr. Keyurkumar M. Nayak,
Director,
UM-GICED

Prof.(Dr.) Anil Kumar Singh
Dean,
Faculty of Interdisciplinary Studies