Maharashtra State Board of Technical Education, Mumbai

Teaching and Examination Scheme

Programme Name : Advanced Diploma in Cyber Security Management

Programme Code :CB — **With Effect From Academic Year: 2023 - 24**

Duration of Programme :One Year (Two Semesters) — **Pattern : Semester (Part Time)** — **Duration : 16 Weeks**

Semester : First — **Scheme : I**

S. N.	Course Title	Course Abbreviation	Course Code	Teaching Scheme			Credit (L+T+P)	Examination Scheme													Grand Total
								Theory							Practical						
								Exam Duration in Hrs.	ESE		PA		Total		ESE		PA		Total		
				L	T	P			Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	
a	b	c	d	E	f	g	h(e+f+g)	i	j	k	l	m	n(j+l)	o	p	q	r	s	t(p+r)	u	v(n+t)
1	Cyber Security Essentials	CSE	28104	3	--	4	7	1.5	70*#	35	30*	00	**100**	50	50@	25	50	25	**100**	50	**200**
2	Mobile Application and Cloud Security	MAC	28105	3	--	4	7	1.5	70*#	35	30*	00	**100**	50	50@	25	50	25	**100**	50	**200**
3	Network and Web Application Security	NWA	28007	2	--	4	6	-	-	-	-	-	-	-	50@	25	50	25	**100**	50	**100**
			Total	**08**	**--**	**12**	**20**	3	**140**	--	**60**	--	**200**	--	**150**	--	**150**	--	300	--	**500**

Student Contact Hours Per Week: **20Hrs. Theory and practical periods of 60 minutes each.** Medium of Instruction: **English** Total Marks : **500**

Abbreviations: ESE- End Semester Exam, PA- Progressive Assessment, L - Lectures, T - Tutorial, P - Practical

@Internal Assessment, # External Assessment, *# On Line Examination

* The average of 2 test to be taken during the semester for the assessment.

#$ External PR ESE and average of 2 Skill tests / Practicals.

@$ Internal PR ESE and average of 2 Skill tests / Practicals.

If student remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE.

- **Candidates not securing minimum marks for passing the "PA" part of practical of any course is declared as "Detained" for that semester.**
- **During Internship and Project period students shall attend Institute one day in a week to meet the mentor and appraise about the progress. The log book, Project Diary and Internship performance shall be recorded by the mentor for progressive assessment.**

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION MUMBAI

Maharashtra State Board of Technical Education, Mumbai

Teaching and Examination Scheme

Programme Name : Advanced Diploma in Cyber Security Management

Programme Code :CB **With Effect From Academic Year: 2023 - 24**

Duration of Programme :One Year (Two Semesters) **Pattern : Semester (Part Time)** **Duration : 16 Weeks**

Semester : Second **Scheme : I**

S. N.	Course Title	Course Abbreviation	Course Code	Teaching Scheme			Credit (L+T+P)	Examination Scheme													Grand Total
								Theory							Practical						
								Exam Duration in Hrs.	ESE		PA		Total		ESE		PA		Total		
				L	T	P			Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	
a	b	c	d	e	f	g	h(e+f+g)	i	J	k	l	m	n(j+l)	o	p	q	r	s	t(p+r)	u	v(n+t)
1	Cyber Law and Compliance	CLC	28203	4	--	--	4	1.5	70*#	35	30*	00	**100**	50	--	--	--	--	--	--	**100**
2	Project	PCB	28058	--	--	6	6	--	--	--	--	--	--	--	50#	25	50	25	**100**	50	**100**
3	Industrial Training	ITR	28059	--	--	10	10	--	--	--	--	--	--	--	100#	50	100	50	**200**	100	**200**
			Total	**04**	**--**	**16**	**20**	--	**70**	--	**30**	--	**100**	--	**150**	--	**150**	--	**300**	--	**400**

Student Contact Hours Per Week: **20Hrs. Theory and practical periods of 60minutes each.** Medium of Instruction: **English** Total Marks : **400**

Abbreviations: ESE- End Semester Exam, PA- Progressive Assessment, L - Lectures, T - Tutorial, P - Practical

@Internal Assessment, # External Assessment, *# On Line Examination

* The average of 2 test to be taken during the semester for the assessment.

#$ External PR ESE and average of 2 Skill tests / Practicals.

@$ Internal PR ESE and average of 2 Skill tests / Practicals.

If student remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE.

- **Candidates not securing minimum marks for passing the "PA" part of practical of any course is declared as "Detained" for that semester.**
- **During Internship and Project period students shall attend Institute one day in a week to meet the mentor and appraise about the progress. The log book, Project Diary and Internship performance shall be recorded by the mentor for progressive assessment.**

Note : The Institute is required to sign MOU with related local industries for Internship/Industrial Training

w.e.f. Academic Year 2023-24

'I' Scheme

PROGRAMME NAME : ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT

PROGRAMME CODE : CB

SEMESTER : FIRST

COURSE TITLE : CYBER SECURITY ESSENTIALS

COURSE CODE : 28104

1. RATIONALE

This subject focus on fundamentals needed for Cyber Security Management /Information technology (IT) security, cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

In implementation of cyber security, it is necessary to understand the importance of fundamental knowledge of computer, operating system such as Linux and windows, programming and testing. Focus on hardware, software components, networking and encryption in cyber security aspects. Installation of open-source platform like Linux operating system, be aware of its directory structure, different permissions and apply various commands. Focus on Windows operating system as client, server, Active directory roles and handle files relevant to cyber security.

Develop basic level programs in C and Python and Web development like HTML, Java Script, and PHP, MySQL using database along with functional testing with respect to SDLC, apply testing standards and use documentation to monitor security to study threats and vulnerabilities in several phases. Multiple types of assets can be tested.

2. COMPETENCY

Apply Cyber Security management in different aspects of hardware, software and programming environment.

3. COURSE OUTCOMES

- Study of hardware, software component, networking and encryption aspects in cyber security aspects.
- Install Linux operating system, its directory structure, set different permissions and apply various commands.
- Install Windows operating system as client, server, Active directory roles and handle files relevant to cyber security.
- Develop basic level programs in C and Python and Web development like HTML, Java Script, PHP, MySQL using database
- Apply functional testing with respect to SDLC.
- Apply testing standards and use documentation to monitor security to study threats and vulnerabilities in several phases.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme											
				Theory							Practical				
					ESE		PA		Total		ESE		PA		Total	
L	T	P	(L+T+P)	Paper Hrs.	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	--	4	7	1.5	70*#	35	30*	00	100	50	50@	25	50	25	100	50

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

(#$) or (@$) : Under the practical ESE - 50 Marks (100%)

1) 30 Marks (60%) - For Practical – ESE

2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the

CB

semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

Legends: ***L****-Lecture,* ***T*** *– Tutorial/Teacher Guided Theory Practice,* ***P*** *–Practical,* ***ESE*** *-End Semester Examination,* ***PA*** *- Progressive Assessment*

*@Internal Assessment, #External Assessment, *#Online Examination*

5. LIST OF PRACTICALS/ EXERCISES/ASSIGNMENTS/CASE STUDIES

Sr. No.	Name of Practical/ Exercise/ Assignment/ Case Study
1	Identification of Components and Assemble Computer from scratch
2	Conversion of text to bits, binary, hexadecimal and vice versa
3	Create a network topology diagram using cisco packet tracer
4	Encode and decode text, multimedia files using different encoding techniques
5	Create, Extract and Crack hashes of the files, text
6	Install Linux in Virtual Machine
7	Install WSL2 Linux in Windows
8	Solve 20 challenges from https://overthewire.org/wargames/bandit/
9	Linux Hardening
10	Create a bash script to automate your tasks
11	Install Windows 11 Client and create a user
12	Install Windows Server in Virtual Machine and Keep Server Awake 24*7
13	Create a Active Directory and add systems in the Domain
14	Set up secured file sharing in your network
15	Windows and Windows Server Hardening
16	Setup Connectivity-IPv4 and DNS configuration
17	Create a power shell script to automate your tasks
18	Allow ICMPv4 Request in Firewall and Setup TimeZone, date and Clock
19	Create a dynamic webpage using HTML, PHP, JavaScript and MySQL
20	Host the website from Linux System using Apache
21	Create a password brute force in Python
22	Create a tool for automate your day-to-day tasks
23	Choose any application and create a flow diagram
24	Perform functionality testing of an application and create a report

6. MAJOR EQUIPMENT/ INSTRUMENTSREQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of experiments, as well as aid to procure equipment by authorities concerned.

Sr. No.	Equipment Name with Broad Specifications
1	Computer system
2	Cisco Packet Tracer
3	Hashcat
4	Jhon the Ripper
5	Virtual Box
6	Lynis (CIS Benchmark)
7	CIS Benchmark for windows
8	SSH

7. THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to attain the identified competencies.

Unit	Topic and contents	Hours	Marks
I	**Fundamental of computers** **Hardware component: -** Motherboard, Central Processing Unit, Random Access Memory, Storage, GPU **Software: -** Operating System, Kernel, Process, Interrupt, Boot Loaders **Numeric System: -** Bits, Decimal, Hexadecimal, Binary, Two's Complement **Networking: -** Types of Networks, Network Hardware- Router, Switch, Network Card and HUB, OSI Model, IP Address-v4, v6, Private and Public Addressing, CIDR, Broadcast, etc., MAC address-ARP, DNS, rDNS, DHCP, Ports, Packets, TCP/IP Model-Protocol, Header, Handshake, etc., UFP-Protocol, Headers, IPv4 and IPv6 Header, ICMP, Link Layer **Encoding and Encryption: -** ASCII, URL, Base64, Symmetric & Asymmetric, HTTP(S), Hashing	06	10
II	**Linux Fundamentals** **What is Linux: -** Linux Distro, Installation, Architecture **Directory Structure: -** /, /bin, /boot, /dev, /etc, /home, /lib, /media, /mnt, /opt, /proc, /root, /sbin, /tmp, /usr, /var, Symlinks & Hidden Files **Permissions: -** OWNER, GROUP, EVERYONE, READ, WRITE, EXECUTE **Commands: -** Basic Commands, Sys & User Info, File Storage and Compressions, Process, Networking and Proxy chain, SSH Setup and Clearing Logs, Schedule Tasks and Set up Web Server, Bash Scripting	04	12
III	**Windows Fundamentals** **Microsoft Windows**-History and Future, Server Roles and Features-Active Directory, DNS Server, DHCP Server, Hyper-V, Network Policy and Access Services, Web Server, File and Storage Service, RDP, Auto Logon, Registry, Event Viewer and CMD **Active Directory**-Roles and Features, Domain Controller, Organization Units, Forest, Groups, etc. Active Directory-Users and Computers, sites & Services, Domain & Trust, User and Computer Properties, GPMC and GPO at Domain & OU, Group Policy Management Editor DNS-FQDS, NetBIOS, Domain Controller, Zones, Resources, Manager, File Sharing-NFS, SMB, FTP, CIFS, file Permissions-Account User, Global Security Group, Universal Security Group, Domain Local Security Group, Permissions **PowerShell**-Basic Commands, Sys & User Info, Process & Networking, Execution Policies, PowerShell Scripting	08	12

Unit	Topic and contents	Hours	Marks
IV	**Programming Fundamentals** Low Level Programming vs High Level Programming & Compiled vs Interpreted **C & Python**- Printing, Variables, Comments, Conditions, Loops, Arrays, Inputs, Functions, Modules, Socket, Threading Web Development- HTML, JavaScript, PHP, MySQL Database	**10**	**12**
V	**SDLC and Application Functional Testing** **SDLC**- Definition & Design, Code Review, Deployment, Maintenance **Functionality Testing-** User Interface Journey, Workflow Design Flaw, Limitation of Every Parameter, Configuration Checks, Platform Modification.	**08**	**12**
VI	**Testing Standards and Documentation** OWASP, OSSTMM, SANS TOP 25, NIST, MITRE, PTES, ISSAF, CIA Traid	**12**	**12**
Total		**48**	**70**

8. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Fundamental of computers	06	04	04	02	10
II	Linux Fundamental	04	04	04	04	12
III	Windows Fundamentals	08	06	02	04	12
IV	Programming Fundamental	10	04	04	04	12
V	SDLC and Application Functional Testing	08	06	04	02	12
VI	Testing Standards and Documentation	12	04	06	02	12
Total		**48**	**28**	**24**	**18**	**70**

Legends: R-Remember, U-Understand, A-Apply and above (Bloom's Revised taxonomy)
Note: The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

9. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication
1	Networking for Dummies	Doug Lowe	12th edition, John Wiley & Sons

10. SOFTWARE/LEARNING WEBSITES

- https://www.packettracernetwork.com/download/download-packet-tracer.html
- https://www.virtualbox.org/wiki/Downloads
- http://downloads.cisecurity.org/

- https://www.microsoft.com/en-in/evalcenter

PROGRAMME NAME : ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT
PROGRAMME CODE : CB
SEMESTER : FIRST
COURSE TITLE : MOBILE APPLICATION AND CLOUD SECURITY
COURSE CODE : 28105

1. RATIONALE

Mobile application penetration testing is the process of testing mobile apps for security vulnerabilities. The goal is to identify any weaknesses that could be exploited by an attacker to gain unauthorized access to sensitive data or perform other malicious actions. This is important because mobile apps often handle sensitive information, such as financial data or personal information, and can be a target for cyber-attacks.

Cloud penetration testing is the process of testing cloud-based systems for security vulnerabilities. The goal is to identify any weaknesses that could be exploited by an attacker to gain unauthorized access to sensitive data or perform other malicious actions. This is important because cloud-based systems often store and process large amounts of sensitive information and can be a target for cyber-attacks. Cloud environments are complex and multi-tenant, and a vulnerability in one tenant's environment can impact other tenants as well.

2. COMPETENCY

- Implement security in **Android Application, iOS Application and cloud Application using penetration testing.**

3. COURSE OUTCOMES

- Understand Android operating system and its security architecture
- Apply Penetration Testing on Android application
- Understand iOS security architecture
- Apply Penetration Testing on iOS application
- Understand Cloud computing architecture
- Apply security in cloud architecture and data.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme											
				Theory							Practical				
L	T	P	(L+T+P)	Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	--	4	7	1.5	70*#	35	30*	00	**100**	50	50@	25	50	25	**100**	50

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

***(#$) or (@$)** : Under the practical ESE - 50 Marks (100%)*
1) 30 Marks (60%) - For Practical – ESE
2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

***Legends:** L-Lecture, T – Tutorial/Teacher Guided Theory Practice, P –Practical, ESE -End Semester*

*Examination, **PA** - Progressive Assessment*
*@Internal Assessment, #External Assessment, *#Online Examination*

5. LIST OF PRACTICALS/ EXERCISES/ASSIGNMENTS/CASE STUDIES

Sr. No.	Name of Practical/ Exercise/ Assignment/ Case Study
1	Set up proxy in Android and connect with burp
2	Connect your phone/emulator using adb
3	Decompile and analyze java, kotlin. Flutter, React Native application
4	Convert split apk to single apk and sign it using self-signed certificate
5	Setup tools Mobsf, Frida and Drozer
6	Solve DIVA Application (OWASP Top 10)
7	Solve InjuredAndroid (Reverse Enginerring)
8	Solve ctf.hpandro.raviramesh.info (Frida, web, websocket, etc)
9	Solve InsecureShop (Kotlin)
10	Solve OverSecured
11	Solve DVHMA (Hybrid- Apache Cordova)
12	Set up proxy in iOS and connect with burp
13	Connect your phone/emulator using idb
14	Decompile and analyze ipa files
15	Solve DVIA-v2
16	Solve OverSecured Vulnerable iOS App
17	Solve Unsafe Bank iOS App
18	Solve Dvca (Cloud Application-AWS)
19	Solve Cloudgoat (AWS)
20	Solve DVFass (AWS Lamda- Function as a Service)
21	Solve DVSA (Serverless Application)
22	Solve DVFaaS (Function as a zService)

6. MAJOR EQUIPMENT/ INSTRUMENTSREQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of experiments, as well as aid to procure equipment by authorities concerned.

Sr. No.	Equipment Name with Broad Specifications
1	Android Studio
2	MobSF
3	Drozer
4	Hrousec
5	Mariana Trench
6	APK Leaks
7	Frida
8	Smali Helper
9	iOS Emulator/ Jail Broken Device
10	3uTools
11	Plist View
12	Objection
13	Needle
14	KeyChain Dumper
15	Passion Fruit
16	Scoute Suite
17	Prowler (CIS Benchmark)
18	AWSRoleJuggler

Sr. No.	Equipment Name with Broad Specifications
19	Cloudsplaining
20	Pmapper
21	RoadTools
22	BurpSuite
23	Jadx, Apktool
24	react-native-decompiler
25	Split Apk Packer

7. THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to attain the identified competencies.

Unit	Topic and contents	Hours	Marks
I	**Android Application Essentials** **Android Architecture** **Security Architecture** **Application Components-** Activities, Services, Broadcast Receiver, Content Providers, Intent Filter **Android Debug Bridge** **Android Startup Process** **Unzipping Vs. Decompiling Application-** Java, Kotil, Flutter, React Native, Xamarin **Signing & Certificate** **Dex to Jar & Java to Smali** **MSTG & OWASP Mobile Top 10 Checklist**	**08**	**10**
II	**Android Application Penetration Testing** **Tools-** Root Device, Android Studio, MobSF, Drozer, Hrousec, Mariana Trench, APK Leaks, Frida, Smali Helper, BurpSuite, etc **Vulnerable Applications-** InjuredAndroid, HpAndro Android AppSec (Kotlin), Damn- Vulnerable-bank, InsecureShop, AndroGoat, Crackmes,Android InsecureBank v2,DIVA Andriod, Oversecured Vulnerable Android App,MSTG Hacking Playground **Static Analysis-** Understanding Smali, understanding dex & solving labs using Reverse Engineeting, Obfuscation & Deobfuscating of APK, Hardcoded Secrets **Analyzing AndroidMAnifest.xml** – API Version, Exploiting Activities and Intents, Exploiting Broadcast Receivers, Servcices, Content Providers, Backup True, Debug, Web Views, Dangerous Permissions, Deep Links, Insecure Firebase, Clear Text Traffic **Dynamic Analysis-**Setup Proxy,SSL & Certificate Unpinning, Memory Dump, Anti Tampering, Background screen caching, Taskbar Snooping, Thirdparty keyboard Enabled, Android Lock/Biometric Bypass, Split APK to Single APK **Root Detection Bypass-**Root management apps, Su Binary, Read write System, Su Exists, Dangerous Props, Test Keys, **Emulator Detection Bypass** – Virtual Phone Number, Hardware Specifications, Emulator Files Check, Emulator Files Check, Ip Check, Debug Flag, Network operator name, QEMU detection, Device ID based Detection. **Sensitive Information in logs** – Informational Logs, Error Logs, Warning Logs, Debug logs, Verbose Logs	**12**	**12**

CB

Unit	Topic and contents	Hours	Marks
III	**iOS Essentials** **iOS Architecture** **iOS Security Architecture** **IPA Build Flow** **File Structure** **Signing & Certificate** **iOS Frameworks**	06	12
IV	**iOS Application Penetration Testing** **Environment Setup-** Jail break, burpSuite, Objection, Cycript, Fuzzer, Passion Fruite, etc **Static Analysis-** Plist Files, Keychain, Webkit Caching, Pasteboard Leakage, Snapshot, Device logging, Decrypting IOS Binaries **Dynamic Analysis-**Database, Cache data, Binary Cookies, Automatic Snapshot, logs, setup proxy, jailbroke bypass, SSL pinning bypass, Emulator Bypass	10	12
V	**Cloud Essentials** Introduction to cloud computing Enumerating IAM Roles Types of Services Advantages & Disadvantages NIST cloud deployment reference architecture Container technology OWASP Top 10 Cloud Security Risk IAM- Fundamentals, Digital Authentication, IAM Compliance	04	12
VI	**Cloud Security** **Identity & Access Management :** AWS organisations, Sevice Control Policy, Secure Token Services, SAML Indentity Federation, AWS cognito, Identity Center, Microsoft AD, AD Connector, Hybrid Directory Solutions, WorkSpace, IAM permission boundaries / Deligate boundaries, Confused Deputy Issues (AWS), S3 Security, Resource Policies, MFA, buckect policy, control tower **Infrastructure Security:** Transit gateways, peering connections, DX gateway, Bastion Host and Authentications, Port Forwarding, NAT Gateway, Side to Side VPN, Virtual Private Gateway, Client VPN, Gateway VPC Endpoint, Interface VPC endpoints, Egress Only Internet gateway, DNS Endpoints, EBS Encryption, CDN, Lambda@edge, AWS Shield, AWS Network Firewall, DNS Sec using route53 **Logging and Monitoring:** Cloudwatch, S3 events, AWS security hub, AWS inspector, Trusted Advisor, Config Web application firewall, Cloudtrail, Athena, Macie, Glue **Data Security :** Encryption, HSM Module, KMS : KMS security Models, Multi region keys, S3 Object Encryption, Secrets Manager, RDS Encryption and IAM Authentication, Load balancer,SSL Offloading	08	12
Total		48	70

8. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Android Application Essentials	08	04	04	02	10
II	Android Application Penetration Testing	12	02	06	04	12
III	iOS Essentials	6	04	06	02	12
IV	iOS Application Penetration Testing	10	04	04	04	12
V	Cloud Essentials	04	06	04	02	12
VI	Cloud Security	08	04	04	04	12
Total		**48**	**24**	**28**	**18**	**70**

Legends: R-Remember, U-Understand, A-Apply and above (Bloom's Revised taxonomy)
Note: The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

9. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication
1	OWASP MASVS	Open-Source	The OWASP Foundation
2	OWASP MASTG	Open-Source	The OWASP Foundation
3	OWASP Cloud-Native Application Security	Open-Source	The OWASP Foundation

10. SOFTWARE/LEARNING WEBSITES

- https://github.com/payatu/diva-android
- https://github.com/B3nac/InjuredAndroid
- http://ctf.hpandro.raviramesh.info/
- https://github.com/hax0rgb/InsecureShop
- https://github.com/oversecured/ovaa
- https://github.com/logicalhacking/DVHMA
- https://github.com/prateek147/DVIA-v2
- https://github.com/oversecured/OversecuredVulnerableiOSApp
- https://github.com/lucideus-repo/UnSAFE_Bank
- https://github.com/m6a-UdS/dvca
- https://github.com/RhinoSecurityLabs/cloudgoat
- https://github.com/torque59/AWS-Vulnerable-Lambda
- https://github.com/OWASP/DVSA
- https://github.com/we45/DVFaaS-Damn-Vulnerable-Functions-as-a-Service
- https://owasp.org/www-project-mobile-app-security/
- https://owasp.org/www-project-cloud-native-application-security-top-10/

PROGRAMME NAME : ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT
PROGRAMME CODE : CB
SEMESTER : FIRST
COURSE TITLE : NETWORK AND WEB APPLICATION SECURITY
COURSE CODE : 28007

1. RATIONALE

Web Application Penetration Testing is a security testing method that simulates an attacker's attempts to exploit vulnerabilities in web applications. It aims to identify, exploit, and mitigate vulnerabilities to protect sensitive information and maintain the normal functioning of the web application.

Network Penetration Testing is a security testing method that simulates an attacker's attempts to exploit vulnerabilities in a network infrastructure. It aims to identify, exploit, and mitigate vulnerabilities to protect sensitive information and maintain the normal functioning of the network.

2. COMPETENCY

Implement security in **Web Application and Network using penetration testing.**

3. COURSE OUTCOMES

- Understanding need of open-source intelligence information gathering
- Apply various security testing methods on Web Applications
- Apply API Security Testing
- Implement Web Socket Security
- Implement Network Security
- Implement Wireless Security

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme											
				Theory							Practical				
					ESE		PA		Total		ESE		PA		Total	
L	T	P	(L+T+P)	Paper Hrs.	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
2	--	4	6	-	-	-	-	-	-	-	50@	25	50	25	100	50

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

(#$) or (@$) : Under the practical ESE - 50 Marks (100%)
1) 30 Marks (60%) - For Practical – ESE
2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

Legends: ***L****-Lecture,* ***T*** *– Tutorial/Teacher Guided Theory Practice,* ***P*** *–Practical,* ***ESE*** *-End Semester Examination,* ***PA*** *- Progressive Assessment*
*@Internal Assessment, #External Assessment, *#Online Examination*

5. LIST OF PRACTICALS/ EXERCISES/ASSIGNMENTS/CASE STUDIES

Sr. No.	Name of Practical/ Exercise/ Assignment/ Case Study
1	Google, Bing, Yandex Dorking - Browser
2	Github, Shodan, Censys Dorking - Browser
3	Web Archive
4	Active and Passive Information Gathering
5	Solve BWAPP Lab-VM
6	Solve Webgoat Lab-VM
7	Solve OSAWP Juice Shop-VM
8	Solve Web Security Portswigger Labs - online (as much as possible)
9	Solve VAmPI Lab-VM
10	Solve vapi Lab-VM
11	Solve DVWS Lab-VM
12	Solve Free Labs of AttackDefense.com
13	Solve Web Socket Security Portswigger Labs - online
14	Solve PWN till Dawn labs (5 Easy, 4 Medium, 3 Hard)-online
15	How to detect port scan
16	Map the target
17	Do network scan on local network
18	Wifi Sniffing
19	Analysing wifi traffic
20	Cracking into WEP, WPS and WPS2
21	Exploit devices in wireless network using mitmf & beef framework
22	Evil twin attack with fake access point

6. MAJOR EQUIPMENT/ INSTRUMENTSREQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of experiments, as well as aid to procure equipment by authorities concerned.

Sr. No.	Equipment Name with Broad Specifications
1	BurpSuite
2	Amass
3	Nuclei
4	Httpx
5	Nessus
6	Nmap
7	Metasploit
8	Airgeddon
9	MITMF Framework
10	BEEF Framework
11	WireShark
12	Postman
13	Browser

7. THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to attain the identified competencies.

Unit	Topic and contents	Hours
I	**Intelligence Gathering** Open-Source Intelligence Search engine Dorking-Google, Github, Wayback, Shodan, Censys, Yandax Active & Passive Information Gathering	02
II	**Web Security** Configuration and Deployment Management Testing, Identity Management Testing, Authentication and Authorization Testing, Session Management Testing, Input Validation Testing, Testing for Error Handling, Testing for Weak Cryptography, Business Logic Testing and Client-side Testing	02
III	**API Security** SOAP API vs REST API Introduction to PostMan Authentication Methods Transformation of API WSDL & XML File Transformation OWASP API Top 10 GraphQL	06
IV	**Web Socket Security** Web Socket Introduction Intercepting Web Sockets Manipulating WebSocket Connections Cross-site WebSocket hijacking Secure-site WebSocket hijacking Secure Web Socket Web Socket MITM Missing Security Headers	08
V	**Network Security** Network Mapping using Nmap, Exploiting Common Services with Metasploit, Brute forcing using hydra, Cracking Hash, Privilege Escalation-Misconfigurations, File permissions, Schedule Tasks, Stored Credential, SUID, SUDO, Paths, Tools-LinPEAS, WinPEAS Detection Mechanism-Firewall, IDS/IPS, DLP, Endpoint Security	06
VI	**Wireless Security** Standards & Amendments Antenna Types & Frequency Wireless Technology WPE, WPA, WPA2 & WPA3 Sniffing De Authentication Attack MITM Reviewer & Bcmon Evil Twin, etc	08
Total		**32**

8. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication
1	OWASP – WSTG	Open-Source	The OWASP Foundation

9. SOFTWARE/LEARNING WEBSITES

- https://owasp.org/www-project-web-security-testing-guide/v42/
- https://www.exploit-db.com/google-hacking-database
- https://pentest-standard.org/index.php/Main_Page
- https://attack.mitre.org/
- https://osintframework.com/
- http://www.itsecgames.com/bugs.htm
- https://github.com/WebGoat/WebGoat/
- https://github.com/juice-shop/juice-shop-ctf
- https://learning.postman.com/docs/getting-started/introduction/
- https://portswigger.net/web-security
- https://online.pwntilldawn.com/
- https://github.com/snoopysecurity/dvws

PROGRAMME NAME: ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT

PROGRAMME CODE : CB

SEMESTER : SECOND

COURSE TITLE : CYBER LAW AND COMPLIANCE

COURSE CODE : 28203

1. RATIONALE

Cyber security management gets more and more crucial as the need to protect sensitive data against the wrong hands grows in importance. For companies of all sizes, because of remote working, the nearly unbelievable rise in cybercrime has led organizations to strengthen their IT infrastructure and boost cyber security through the concepts of Cyber Law, and the application of laws for different kinds of Cyber Crime.

2. COMPETENCY

Follow Cyber Laws to achieve and manage cyber security to control cybercrime.

3. COURSE OUTCOMES

- Implement preventive measures of Cyber Crime and Criminal Justice: IT Act 2000 for contracts in InfoTech World.
- Make Awareness of Jurisdiction and contracts in the Cyber world.
- Avoid trace passers in the Cyber world using Copyright Protection.
- Invent E-Commerce Taxation real problems in the virtual world.
- Implement Digital Signature and E-Governance.
- Apply Indian Evidence Act 1872 vs IT Act 2000.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme											
				Theory							Practical				
L	T	P	(L+T+P)	Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
4	--	--	4	1.5	70*#	35	30*	00	100	50	--	--	--	--	--	--

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

***(#$) or (@$)** : Under the practical ESE - 50 Marks (100%)*
1) 30 Marks (60%) - For Practical – ESE
2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

***Legends:** L-Lecture, T – Tutorial/Teacher Guided Theory Practice, P –Practical, ESE -End Semester Examination, PA - Progressive Assessment*
*@Internal Assessment, #External Assessment, *#Online Examination*

5. THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to attain the identified competencies.

Unit	Topic and contents	Hours	Marks
I	Cyber Crime and Criminal Justice: Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals under the IT Act, 2000, Concept of 'Cyber Crime' and the IT Act, 2000	12	10

Unit	Topic and contents	Hours	Marks
	• Hacking • Teenage Web Vandals • Cyber Fraud and Cyber Cheating • Virus on the Internet • Defamation, Harassment and E-mail Abuse • Cyber Pornography • Other IT Act Offences • Monetary Penalties, Adjudication and Appeals Under IT Act, 2000 • Network Service Provides • Jurisdiction and Cyber Crimes • Nature of Cyber Criminality, Strategies to Tackle • Criminal Justice iCyber Crime and Trends in India and Implication on Cyber.		
II	**Jurisdiction and contracts in the InfoTech World** • Contracts in the InfoTech World • Click-Wrap and Shrink-wrap Contracts: Status under the Indian Contract Act, 1872 • Contract Formation under the Indian Contract Act, 1872 • Contract Formation on the Internet • Terms and Condition of Contracts **Jurisdiction in the Cyber World** • Questioning the Jurisdiction and Validity of the Present • Law of Jurisdiction • Civil Law of Jurisdiction in India • Cause of Action • Jurisdiction and the Information Technology Act,2000 • Foreign Judgments in India • Place of Cause of Action in Contractual and • IPR Disputes • Exclusive Clauses in Contracts • Abuse of Exclusive Clauses • Objection of Lack of Jurisdiction • Misuse of the Law of Jurisdiction • Legal Principle on Jurisdiction in the United States of America Jurisdiction Disputes with respect to the Internet in the United States of America	12	12
III	**Copyright Protection in the Cyber World** • Concept of Domain Name and Reply to Cyber Squatters • Meta-Tagging • Legislative and Other Innovative Moves against Cyber Squatting • The Battle between Freedom and Control on the Internet • Works in Which Copyright Subsists and Meaning of Copyright • Copyright Ownership and Assignment • License of Copyright • Copyright Term and Respect for Foreign Works • Copyright Infringement, Remedies and Offenses	12	12

Unit	Topic and contents	Hours	Marks
	. Copyright Protection and Content on the Internet; Copyright Notice, Disclaimer and Acknowledgement . Downloading for Viewing Contents on the Internet, Hyper-linking and framing . Liability of ISPs for Copyright Violation in the . Cyber World: Legal Developments in the US . Napster and its Cousins: A Revolution on the Internet And the Crisis for Copyright Owners . Computer Software Piracy		
IV	**E-Commerce Taxation: Real Problems In the Virtual World** . A Tug of War on the Concept of 'Permanent Establishment' . Finding the PE in Cross Border E-Commerce . The United Nation Model Tax Treaty . The Law of Double Taxation Avoidance Agreements and Taxable Jurisdiction over Non-Residents, under the Income Tax, 196112 . Tax Agents of Non-Residents under the Income Tax Act, . 1961 and the Relevance to E-Commerce . Source versus Residence and Classification between . Business Incomes . The Impact of the Internet on Custom Duties . Taxation Policies in India	**12**	**12**
V	**Digital Signature, Certifying Authorities and E-Governance** . Digital Signature . Digital Signature Certificate . Certifying Authorities and Liabilities in the Event of Digital Signature . E-Governance in India	**08**	**12**
VI	**Indian Evidence Act 1872 vs. IT Act 2000** . Status of Electronic record as evidence . Proof and management of electronic record . Proving Digital Signature . Proof of Electronic Agreement . Proving of Electronic Message . Introduction to the Computer Misuse Act (CMA)	**08**	**12**
	Total	**64**	**70**

6. SUGGESTED SPECIFICATION TABLE ESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Cyber Crime and Criminal Justice:	12	04	04	02	10
II	Jurisdiction and contracts in the InfoTech World	12	04	04	04	12
III	Copyright Protection in the Cyber World	12	04	04	04	12
IV	E-Commerce Taxation: Real Problems In the Virtual World	12	04	04	04	12
V	Digital Signature, Certifying Authorities and E-Governance	08	02	06	04	12

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
VI	Indian Evidence Act 1872 vs. IT Act 2000	08	04	04	04	12
	Total	**64**	**22**	**26**	**22**	**70**

Legends: R-Remember, U-Understand, A-Apply and above (Bloom's Revised taxonomy)
Note: The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

7. SUGGESTED LEARNING RESOURCES

Sr. No.	Title of Book	Author	Publication
1	Cyber Security by Edward Amoroso Computer Network Security and Cyber Ethics, 2nd edition	Joseph Migga Kizza	Mc Farland & Company
2	Data Warehousing and Data Mining Techniques for Cyber Security (Advances in Information Security)	Anoop Singhal	Springer
3	Security Operations Management, Second Edition	Robert McCrie	Butterworth - Heinemann
4	Risk Management for Computer Security: Protecting Your Network & Information Assets	Andy Jones and Debi Ashenden	Butterworth - Heinemann
5	Risk, Crisis and Security Management	Edward Borodzicz	Wiley
6	Cyber Warfare and Cyber Terrorism (Premier Reference)	Lech J. Janczewski and Andrew M. Colarik	IG1 Global
7	CYBER SECURITY:Economic Strategies and Public Policy Alternatives	Michael P. Gallaher, Albert N. Link, and Brent R. Rowe	Edward Elgar Publishing
8	The Transnational Dimension of Cyber Crime and Terrorism (Hoover National Security Forum Series)	Mariano-Florentino Cuellar, Ekaterina A. Drozdova, David D. Elliott, and Seymour E. Goodman	Hoover Institution Press
9	KNOW Cyber Risk: By Managing Your IT Security!	James P. Litchko and Al Payne	KNOW Book Publishing
10	Cyber Security: Turning National Solutions into International Cooperation (Csis Significant Issues Series)	James Andrew Lewis	Center for Strategic & International Studies
11	International Guide to Cyber Security	Jody R. Westy	American Bar Association
12	Fundamentals of Computer Security Technology	Edward Amoroso	Prentice Hall PTR

8. SOFTWARE/LEARNING WEBSITES

- www.legalserviceindia.com/
- www.mit.gov.in
- http://www.us-cert.gov/cas/tips/ST04-001.html

PROGRAMME NAME : ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT

PROGRAMME CODE : CB

SEMESTER : SECOND

COURSE TITLE : PROJECT

COURSE CODE : 28058

1. RATIONALE

The main aim of the preparation of project is to judge the knowledge gained by the students during their tenure of the programme, the transfer of learning to useful socially relevant application. This will also help in various skills such as Personal, social, professional and lifelong learning. The students will be benefited lot by this exercise of preparation of project on their experiences which will certainly add values in their attitudes such as value for health, work commitment, hardworking, honesty, problem solving, punctuality, loyalty and independent study. The student should also make a brief presentation about the project and the salient observations and findings.

2. COMPETENCY

This will develop various skills such as Personal, social, professional and lifelong learning. The students will be benefited lot by this exercise of preparation of project on their experiences which will certainly add values in their attitudes such as value for health, work commitment, hardworking, honesty, problem solving, and punctuality, loyalty and independent study.

3. COURSE OUTCOMES

The student will be able to

- Unauthorized access to website and its prevention
- Encryption of confidential data exchange with client
- Handle Top virus threats, spy ware threats
- Principles used in Cyber Security breaches to gain access to Cyber Security System.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme												
				Theory							Practical					
L	T	P	(L+T+P)	Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
--	--	6	6	--	--	--	--	--	--	--	50#	25	50	25	**100**	50

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

***(#$) or (@$)** : Under the practical ESE - 50 Marks (100%)*
1) 30 Marks (60%) - For Practical – ESE
2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

***Legends: L**-Lecture, **T** – Tutorial/Teacher Guided Theory Practice, **P** –Practical, **ESE** -End Semester Examination, **PA** - Progressive Assessment*

*@Internal Assessment, #External Assessment, *#Online Examination*

Suggested list of Project Ideas

1. Set up network topology with all home devices and set security measures against Cyber-attacks

2. Find Network/Web vulnerabilities of selected organizations/their college assets and setup security policies against cyber-attacks along with their approval.
3. Analyzing vulnerabilities on mobile device and setting up security policies against cyber-attacks.
4. Create your own vpn and setup all your devices routed through a local proxy to filter malicious contents, ads and offensive keywords.

5. IMPLEMENTATION STRATEGY

Candidate should be assigned Project preferably individually or if at all not possible can form a group of maximum 3 members. Every candidate must maintain the weekly progress diary and the guide should review the progress and sign the diary regularly.

Every candidate has to submit Synopsis Report (of pages not more than 10) and deliver Two Presentations for the completion of the Project.

First Presentation of Synopsis - to the Internal Guide tentatively during Third Week of the Academic Term.

Second Presentation on complete Project - to be given to the Internal Guide during Second Class Test schedule.

Contents of the Synopsis - It should include the following points

1. Cover Page of the Synopsis (Title of the Project, Student and Guide Details, Institute Name, Academic Year, Maharashtra State Board of Technical Education, Mumbai)
2. Index
3. Introduction
4. Need of the Project and Objectives
5. Problem Definition
6. Methodology
7. Action Plan

Evaluation of Practical-PA will be the average of two presentations, synopsis report and weekly progress diary maintained by the candidate.

There should not be any sort of typographical, diagrammatic and any other mistake/s in the final bound copy of the project report submitted by the candidate.

PROJECT REPORT CONTENTS

The Project report should essentially consists of the following

- COVER PAGE OF THE PROJECT
- CERTIFICATE FROM THE INSTITUTE
- ACKNOWLEDGEMENT
- TABLE OF CONTENTS
- ABSTRACT
- INTRODUCTION
- METHODOLOGY
- ABOUT THE ORGANISATION / COMPANY

- PROJECT DETAILS
- OBSERVATIONS AND FINDINGS
- CONCLUSION AND FUTURE SCOPE
- REFERENCES / BIBLIOGRAPHY

GUIDELINES FOR PREPARING THE PROJECT REPORT

Project work is a basic requirement for the award of Advance Diploma. Project shall be prepared based on any one of the subjects of the Programme. The project work should be comprehensive and cover all aspects of the management.

COVER PAGE OF THE PROJECT

The Cover Page of the Project Report must include Title of the Project, Student and Guide Details, Institute Name, Academic Year, Maharashtra State Board of Technical Education, Mumbai.

ACKNOWLEDGEMENT

It should appear on the third page and the report writer should acknowledge the guidance provided by the project guide. Here the author may also acknowledge other persons who might have rendered help or supplied the required data or information for completion of the project. It should be brief and crisp. Generally, one page should suffice for acknowledgement.

TABLE OF CONTENTS

It must consist of Chapter No., Name of the Chapter and Page Number.

ABSTRACT

Abstract should describe the entire project work with its aim, objectives and methodology and conclusion. The abstract should be limited to one or two pages.

INTRODUCTION

Give brief description of need, significance and applications of the Project. It is recommended to limit the description to about 2 to 5 pages.

METHODOLOGY

This is the most important part of the project and forms the main body of the project report. It needs very comprehensive coverage of all aspects.

It will be prudent to mention the methodology used for the project work, e.g., collecting information of various types of equipment/components, questionnaires, detailed study, working principle, operations, block diagram, structure, material used for designing of technical specifications, results etc. thereafter, detail procedure to achieve the project output.

CONCLUSION AND FUTURE SCOPE

Based on the project work draw inferences and recommend measures for improvement. The recommendations should be specific, relevant and practically implementable.

PROJECT REPORT FORMAT

Paper Size - A4

CB

Printing	-	Only on one side of the sheet
Line Spacing of Paragraph	-	1 ½
Font Face	-	Times New Roman
Font Size	-	12 for Normal text, 14 for Sub-headings and 16 for Headings
No of Project Report copies	-	Two
Binding	-	Hard bound copies with Black cover (Golden Embossing)

PROGRAMME NAME : ADVANCED DIPLOMA IN CYBER SECURITY MANAGEMENT
PROGRAMME CODE : CB
SEMESTER : SECOND
COURSE TITLE : INDUSTRIAL TRAINING
COURSE CODE : 28059

1. RATIONALE

Industrial training course is introduced to all Advanced diploma programmes with the aim to imbibe the industry culture and professional practices in the students before they enter into world of work. By exposing and interacting with the real-life industrial setting, student will appreciate and understand the actual working of an industry, best practices adopted in industry and other requirements in the industry or their chosen field of training. The industrial needs such as the soft skills, life skills and hands-on practices are intended to be inculcated in the students through this training. This short association with the industry will be instrumental in orienting the students in transforming them to be industry ready after completion of diploma programme.

2. COMPETENCY

This course is intended to develop the following competencies:

a) Soft Skills i.e. Communication, Presentation and others.
b) Life Skills i.e. Time management, Safety, Innovation, Entrepreneurship, Team building and others
c) Hands-on Practices i.e. Shop floor Implementation and Quality Assurance aspects.

3. COURSE OUTCOMES

The industrial training is intended to acquire the competencies as mentioned above to supplement those attained through several courses up to fourth semester of the program:

a) Communicate effectively (verbal as well as written) to execute the work.
b) Prepare the industry report of the executed work.
c) Exercise time management and safety in the work environment.
d) Work in teams for successful completion of projects assuring quality.
e) Work on case studies/live projects

4. TEACHING & EXAMINATION SCHEME

Teaching Scheme			Credit	Examination Scheme												
				Theory							Practical					
L	T	P	(L+T+P)	Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
--	--	10	10	--	--	--	--	--	--	--	100#	50	100	50	**200**	100

(*): Under the theory PA, 30 marks is the average of 2 class tests of 30 marks each to be taken during the semester for the assessment.

***(#$) or (@$)** : Under the practical ESE - 50 Marks (100%)*
1) 30 Marks (60%) - For Practical – ESE
2) 20 Marks (40%) - Average of 2 Skill tests / Practicals of 30 marks each is to be conducted during the semester, and then should be converted to 20 marks.

Note: If student Remaining absent in PR-ESE shall be considered as ABSENT in PR-ESE

***Legends:** L-Lecture, **T** – Tutorial/Teacher Guided Theory Practice, **P** –Practical, **ESE** -End Semester Examination, **PA** - Progressive Assessment*
*@Internal Assessment, #External Assessment, *#Online Examination*

5. GENERAL GUIDELINES FOR INDUSTRIAL TRAINING

The Industries/Organizations can be Government/Public limited organizations or private family enterprises.

a) **Duration of Industrial Training:** 8 weeks in Final Semester as per the credits of the programme

b) **Training Area:** Students should be trained in Large and Medium scale Industry / Organization. However, despite the best efforts by the Institute, if large and medium scale Industry / Organization are not available to all students then, students can also be placed in Small scale Industry / Organization.

c) **Skill Knowledge Partner(SKP)** :To be identified by the Institute as per their programme areas like

1. Organizations such as government / private banks, investment companies, education sector.
2. Web site development organizations
3. App development organizations
4. IT solution providers

6. EXPECTATIONS FROM Skill Knowledge Partner (SKP)

Helping institute in developing the following competencies among students:

a) Soft Skills i.e. Communication, Presentation and others.

b) Life Skills i.e. Time management, Safety, Innovation, Entrepreneurship, Team building and others

c) Hands-on Practices i.e. Shop floor Implementation and Quality Assurance aspects.

7. ROLE OF PARENT DEPARTMENT OF THE INSTITUTE

- Collecting information about Industry / Organization available for training along with capacity.
- Institutions have to enter in to MOU with number of SKPs (Industries/ Organizations) for accommodating all the enrolled students for the mandatory
- Student and mentor allocation as per the slots available for in-plant training (Desirable mentor-student ratio is 1:15).
- Communication with Industry / Organization available for training along with capacity and its confirmation
- Student enrollment for training.
- Issuing letter to the Industry / Organization for the training along with details of students and mentors.
- Principal/ HOD/ Faculty should address students about industrial safety norms, rules and discipline to be maintained in the Industry/ Organization during the training before relieving students for training.
- The faculty member during the visit to Industry/ Organization will check the progress of the student in the training, his/ her attendance, discipline and project report preparation.
- Mentors to carry out progressive assessment of the students during the training through Progressive Assessment (PA).
- End Semester Examination(ESE) assessment by mentor along with Industry / Organization expert as external examiner

8. ROLES AND RESPONSIBILITIES OF THE STUDENTS

Following should be informed to students in the letter deputing them for the training, an undertaking for this should also be taken from them

- Students would interact with the mentor to suggest choices for suitable Industry / Organization. If students have any contact in Industry / Organization (through their parents, relatives or friends) then same may be utilized for securing placement for themselves and their peers.
- Students have to fill the forms duly signed by authorities along with training letter and submit it to training officer in the industry on the first day of training. Student should also carry with him/her the Identity card issued by institute during training period.

CB

- He/she will have to get all the necessary information from the training officer regarding schedule of the training, rules and regulations of the Industry / Organization and safety procedures to be followed. Student is expected to observe these rules, regulations, procedures.
- Students should know that if they break any rule of industry or do not follow the discipline then industry can terminate the training and send back the student.
- It is the responsibility of the student to collect information from Industry / Organization about quality assurance methods/specifications of machines and raw materials/maintenance procedures/ production planning/work ethics/professional practices/organizational structure etc.
- During the training period students have to keep daily record of all the useful information in Log book
- Maintain the Diary/Logbook and get it signed from mentor as well as Industry / Organization Training in-charge.
- In case they face any major problem in industry such as an accident or any disciplinary issue then they should immediately report the same to the institute.
- Prepare final report about the training for submitting to the department at the time of presentation and viva-voce and get it signed from mentor as well as Industry / Organization training in-charge.

9. FORMAT FOR TRAINING REPORT (Program Experts are requested to make suitable changes depending on the need of courses)

Following is the suggestive format for the training report, actual format may differ slightly depending upon the nature of Industry / Organization. The training report may contain the following

- Title page
- Certificate
- Abstract
- Acknowledgement
- Content Page

Chapter 1. Organizational structure of Industry / Organization and General Lay Out
Chapter 2. Introduction of Industry / Organization (Type of products and services, history, turn over and number of employees etc.)
Chapter 3. Types of major equipment/instruments/ machines/software used in Industry/ Organization with their specification, approximate cost and specific use and their routine maintenance.
Chapter 4. Implementation of various security techniques along with planning and control methods and standard Operating procedures.
Chapter 5. Testing of implemented methods and security standards along with quality assurance procedures.
Chapter 6. Major software handling procedures.
Chapter 7. Safety procedures followed
Chapter 8. Particulars of Practical Experiences in Industry / Organization if any in Installation/Implementation/ Assembly/ Testing/Maintenance.
Chapter 9. Short report/description of the project (if any done during the training)
Chapter 10. Special/challenging experiences encountered during training if any (may include students liking & disliking of work places)

References /Bibliography:

10. SUGGESTED LEARNING STRATEGIES

Students should visit the website of the industry/Private firm where they are undergoing training to collect information about products, processes, capacity, number of employees, turnover etc. They should also refer the handbooks of the major machines and operation, testing, quality control and standard operating procedures and practices used in the industry. Students may also visit websites related to other similar industries as their learning resource. The training activity may vary according to nature and size of Industry / Organization. The details of activities to be completed during 8 weeks should be planned appropriately. The evaluation of Industrial training will be done on the basis of

skills acquired by the student during this 8 weeks period.

ASSESSMENT SCHEME FOR INDUSTRIAL TRAINING

Training duration	PROGRESSIVE ASSESSMENT (Weekly report of all 8 week and attendance)		END SEMESTER ASSESSMENT (Seminar and Oral)		Total marks	
Eight Weeks	Max. marks	Min. marks	Max. marks	Min. marks	Max. marks	Min. marks
	100	50	100	50	200	100

EVALUATION SHEET FOR PA OF INDUSTRIAL TRAINING

Sr. No.	Enrollment Number	Name of Student	Marks by Mentor & Industry Supervisor jointly	Marks by Industry Supervisor	Marks by Mentor Faculty	Total Marks
			Out of 40 (A)	Out of 30 (B)	Out of 30 (C)	Out of 100 (A+B+C)

DISTRIBUTION OF END-SEMESTER-EXAMINATION (ESE) MARKS OF INDUSTRIAL TRAINING

Marks for Industrial Training Report	Marks for Seminar/ Presentation	Marks for Oral/Viva-voce	Total ESE marls
25	25	50	100