रांची विश्वविद्यालय
RANCHI UNIVERSITY

CyberPeace

Supplementary Memorandum of Understanding

This Supplementary Memorandum of Understanding is made on this day of May 1st, 2023 Ranchi, Jharkhand:

BETWEEN

Ranchi University, having its campus at Ranchi, Jharkhand, so Represented by its Registrar hereinafter referred to as "**Ranchi University**", which expression shall mean and include its successors and permitted assigns; on the **ONE PART**;

AND

CyberPeace Council is incorporated under the Non Profit Section 8 Company with the Corporate Identity Number of U85300DL2020NPL373733, through its Authorised Signatory Director, Major. Vineet Kumar, which shall, unless the context having its Office at L-29, First Floor, Connaught Place, New Delhi - 110001 and **The Institution of Electronics and Telecommunication Engineers**, through its Authorised Signatory, Chairman IETE, Mr. Umesh Prasad Sah, having its offices at Office of the Advanced Regional Telecom Training Centre, BSNL, Near Jhumar Bridge, Rm.No.B202, H.B.Road, Ranchi-835217; hereinafter referred to as "**IETE-CPC**"; on the **OTHER PART**.

Both "**Ranchi University**" and "**IETE-CPC**" shall be collectively referred to as the '**Parties**'.

WHEREAS, the Ranchi University and IETE-CPC have entered a subsisting Memorandum of Understanding dated 19.05.2022.

WHEREAS, in pursuance of the said Part 1, 2 and 3 of Clause 1 in Memorandum of Understanding the Parties herein have decided to formulate Interdisciplinary PG Diploma in Cyber Security Course.

WHEREAS, in such lines the Parties herein have come to terms and conditions to govern the said method, management and structure of the said Interdisciplinary PG Diploma in Cyber Security Course as per this Supplementary MOU subject to approval of competent authorities in due course

NOW, THEREFORE, IT IS HEREBY AGREED TO BY AND BETWEEN RANCHI UNIVERSITY AND IETE-CPC AS FOLLOWS:

1. **STRUCTURE**

   (i) Regulation for Interdisciplinary PG Diploma in Cyber Security Course. The Syllabus as per guidelines of UGC for the same Course will be prepared by the Joint Expert Group for further needful and to be approved by the concerned competent bodies/authorities of Ranchi University.

   (ii) The Joint Expert Group shall be constituted of 5 officials nominated by the Vice-Chancellor, Ranchi University in consultation with IETE – CPC.

   (iii) This constituted Joint Export Group is also authorized to supervise/monitor the Academic aspect of this course under Provision of Jharkhand State Universities Act, 2000 (adapted) as amended up to date and other relevant order of competent bodies/authority/Vice-Chancellor related to Self-finance Course.

2. **REGULATION FOR THE POSTGRADUATE DIPLOMA CYBER SECURITY COURSE**

A. SESSION 2022-23

These regulations-are to be read in conjunction with regulations under 'Examinations' Chapter-III of Ranchi University Code, Part-IV.

B. Eligibility for Admission in Diploma Programme

Graduate in Science, IT, Mathematics, B.Tech, BCA, MCA, M.Tech or any other equivalent degree as recognized by UGC and the graduate who have

maths at Inter/12th level.

C. Mode of Selection:

The admission shall be based on merit drawn from Marks obtained at Graduates level followed by Interview.

The admission process will follow the Government of Jharkhand rules related to reservation.

D. Course Fee (Per Semester)

Open Rs. 25,000/-

SC/ST Rs. 20,000/-

E. Examination Fees:

As per Ranchi University rules.

No. of Seats — 60

F. Course Structure:

1. The Postgraduate Diploma Course shall be of one year with 2 (two) Semesters.
2. Two Semesters of 6 months each.
3. The Postgraduate Diploma Course will be under self-financing scheme. At the end of a semester, there shall be a University Examination as prescribed in the Course of Study.
4. Each paper shall cover course for theoretical and practical examination as laid down by the Board of Courses of Studies in the subject and approved by the Academic Council. There will be one Mid Semester Examination and One End Semester Examination in every Semester. The Mid Semester and End Semester Examination will be of one hour and three hours duration respectively.

5. The Post Graduate Diploma Course shall follow the semester pattern of instructions and examination and shall have 40 credits where one Credit would mean equivalent of 14-15 periods of 60 minutes each.

6. The Theory paper examination will be of 70 marks in which 60 marks will be for End semester Examination whereas End Semester Practical/Viva Voce Examination will be of 25 marks. The system required for practical purposes is decided for the time being the facilities of MCA, R.U. may be availed by the students of Cyber Security course with due consultation and permission of the Director, MCA, RU. However, for proper arrangement of system etc. for practical purposes necessary action will be taken in due course.

7. The structure of curriculum and the content therein shall be subject to revision from time to time by the Board of courses of Study subject to approval of Academic Council of the University.

G. Guidelines for examinations:

1. A candidate to be admitted in Diploma examination must have

(i) Completed a regular course of study in the University in the subject in which he/she wishes to be examined,

(ii) Attended at least 70% of the lectures delivered and practical held, and has been registered in the University as a student.

2. The practical/viva voce examination of the student shall be evaluated by two examiners, one external and one internal examiner, to be appointed by the Ranchi University.

H. Tabulation and publication of results:

1. That the final result of End Semester Examination of a candidate will be as per the Grade and Marks criteria laid in CBCS examination.

Class interval of Marks %	**Grade Point**	**Letter Grade**	**Grade**	**Conventional Equivalent**
90% and above	10	0	Outstanding	First Class with Distinction
75 to less than 90	9	A+	Excellent	
60 to less than 75	8	A	Very Good	First Class
55 to less than 60	7	B+	Good	Second Class
50 to less than 55	6	B	Above Average	
45 to less than 50	5	C	Average	
40 to less than 45	4	P	Pass	
Below 40	0	F	Fail	Fail
Absent	0	Ab	Absent	

2. A candidate shall be required to clear all the paper means One Sem or Two Sem within three academic years from the date of entry. Thereafter, the registration will stand automatically cancelled.

3. A candidate who appeared in the Diploma but failed to secure the requisite pass marks, shall be allowed to appear in the next examination to be conducted by the University after the publication of the result in those papers in which he/she failed on payment of prescribed fees per paper/subject, quantum of which shall be decided by the Syndicate/University from time to time.

4. The result of examination shall be notified by the Controller of Examinations of Ranchi University on Ranchi University Web Site and shall also be placed in department notice board.

5. Each successful candidate shall receive his/her marks sheet and certificate in the prescribed form specifying the subject in which he/she was examined and the class in which he/she was placed.

6. If a student is found to have indulged in any kind of malpractice or caught indulging in any malpractice, as per the regulations under 'Examination's Chapter-III of Ranchi University Code, Part-IV, the examination taken by the student will be cancelled and the candidate will be awarded zero marks and declared as "FAIL". The candidate has to reappear for the subject (paper) in the subsequent examination as a non-collegiate candidate.

I. SYLLABUS FOR THE POST GRADUATE DIPLOMA IN CYBER SECURITY COURSE

Duration : 12 Months (One Year) Total Credit: 40

Semester 1 (PGDCS)		
Theory		
Course Code	**Course Title T-P-L-I**	**Credits**
	Fundamentals of Computer Security 101 T	02
	Communications & Networking 102 T	05
	Cyber Security 103 T	05

Project/Laboratory/Internship		
	Practical/Lab Exercise/CyberPeace range L	05
	CyberPeace Volunteering / Mini Project P	03
Total Semester Credits		**20**

Semester 2 (PGDCS)		
Theory		
Course Code	**Course Title T-P-L-I** Cybersecurity - Ethical/White Hat Hacking T	**Credits** 05
	Cybersecurity - Open-Source Intelligence (OSINT) T	05
Project/Laboratory/Internship		

	Practical/Lab Exercise L	05
	Capstone Project P	03
	Social Internship I	02
Total Semester Credits		**20**
Total Programme Credits		**40**

Semester 1:

Fundamentals of Computer Security 101

Unit I: Digital Devices and Cyber Security

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Basic operations in Windows, Basic Linux terminology, Kernel, Linux/Mac Terminal and Commands, Basic Computer Terminology, Mobile Devices - features and security concerns, Platforms, Android, Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes,

Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT, Smartphone Operating systems.

Unit II: Basic concept of Programming, Type of programming Languages, Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages. Advance Python Scripting Exception Handling File I/O, Sys

Module, OS Module, Long-Tail/Short-Tail Analysis, Geolocation Acquisition, Blacklists and Whitelists, Packet Analysis, Packet Reassembly, Payload Extraction. Forensic Python: Acquiring Images from Disk, Image Forensics and PIL, SQL Queries, HTTP Communications with Python Built in Libraries, Web Communications with the Requests Module.

Unit III: Web Application Architecture

HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache, Virtualization, Server Configurations, Web Application Firewalls..

Communications & Networking 102:

Introduction to Data communication and Networking: Fundamentals of data communication and networking, Network Reference Models: OSI and TCP/IP Models, Transmission media and network devices. Analog and Digital Signals, Encoding, Internetworking, and IP addressing, IP address class, ARP, RARP, ICMP, IGMP. TCP & UDP, HTTP, HTTPs, SMTP, POP, DNS, TELNET, FTP Intranet, Extranet, www, Email, DNS

VPN and its types –Tunneling 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.

Cyber Security 103:

Cybersecurity Concepts and Cryptography:

Cybersecurity *Concepts:* Information security issues, goals, architecture, Attacks, Security Services and Mechanisms.

Introduction to Cryptography: Network security model, Cryptographic systems, Cryptanalysis, Steganography. Types of Cryptography: Symmetric key and

Asymmetric Key Cryptography, Encryption and Decryption Techniques.

Cryptographic Algorithms: Cryptographic hash, Message Digest, Data Encryption Standard, Advanced Encryption Standard, RSA, DSA, AES.

Security Threats and Vulnerabilities:

Overview of Security threats and Vulnerability: Types of attacks on Confidentiality, Integrity and Availability. Vulnerability and Threats.

Malware: Viruses, Worms, Trojan horses Security Countermeasures; Intrusion Detection, Antivirus Software

Practical/Lab Exercise/CyberPeace range: Practical exercises

of Theorypapers.

CyberPeace Volunteering and Mini Project

Semester 2:

WHITE HAT HACKING:

Introduction: Hacking, Types of Hacking/Hackers, Cybercrime, Types of cybercrime, Threats, Concept of ethical hacking, Phases, Role of Ethical Hacking, Common Hacking Methodologies, Profiles of Hackers, Benefits of Ethical Hacking, Limitations of Ethical Hacking.

Foot Printing & Reconnaissance: Introduction, Use, Types, Information gathering process, Tools

System Hacking: System hacking, Types of System hacking, hacking tools,

Computer Hole, Hacking Process, Various methods of password cracking, Remote Password Guessing, Role of eavesdropping, Keystroke Loggers, Types of Keystroke Loggers, Detection, Prevention and Removal. Trojans, Backdoors, Viruses, and Worms: Trojans and Backdoors, Types of Trojans, Reverse-Connecting Trojans, Netcat Trojan

, Indications of a Trojan Attack, Wrapping, Trojan, Antivirus Evasion Techniques

Network Security: Introduction, Sniffer, Types of Sniffer, Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Spoofing, ARP Spoofing, ARP Poisoning, DNS Spoofing Techniques, MAC Flooding, Sniffing Countermeasures, Netcat,
Social Engineering Social Engineering, Common Types of Attacks, Insider Attacks, Identity Theft, Phishing Attacks, Online Scams, URL Obfuscation, Social-Engineering Countermeasures.

Denial of Service: Denial of Service, Types of DoS Attacks, DDoS Attacks, BOTs/BOTNETs, "Smurf" Attack, "SYN", Flooding, DoS/DDoS Countermeasures.

Web app Security: Hacking Web Applications and Web Servers, Types of Web Server Vulnerabilities, Patch Management Techniques, Web Server Hardening Methods, OWASP Top 10, Fuzzing, Directory listing, XSS Exploitation, Cookie Stealing, SQL Injection, Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Dictionary and brute force attacks, Session ID, LFI and RFI, CSRF (Cross Site Request Forgery).

Wireless security: Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS, attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing, Wireless Networks.

Mobile phone Security: Android security, Mobile application security, Android Payload.

IDS, Firewalls & Honey pots, Cyber Threat Intelligence

Concept of IOT/SCADA Security

ML/DL for Cyber Security

Introduction to Role of ML in Cyber Security, Malware Detection & Classification, Anomaly Detection, Pen Testing using ML, Social Engineering, ML based Intrusion, Detection and other Applications of ML in Cyber Security

OSINT - Open-Source Intelligence (Basic Introduction)

Basic of OSINT: Basic Knowledge – What is OSINT? History of OSINT, why does OSINT matter? Type of OSINT.

Browsers, Anonymous networks, Communications Creating UC accounts, Install and testing browsers, Setup VPNs Reverse Image search and source identification.

Google DORKS, Techniques of Google DORKS and advanced google search Web OSINT, Archiving.

Geo OSINT

Social media OSINT

Practical/Lab Exercise: Practical exercises of Theory papers.

Capstone Project & Social Internship

IN WITNESS WHEREOF, THE PARTIES HAVE CAUSED THIS SUPPLEMENTARY MEMORANDUM OF UNDER UNDERSTANDING TO BE EXECUTED IN DUPLICATE BY PROPER OFFICIALS AS OF THE DATE HEREOF.

For and on behalf of CPC	For and on behalf of IETE	For and on behalf of Ranchi University
Major Vineet Kumar Founder and Global President Date:	Mr. Umesh Prasad Sah Chairman IETE Date:	Dr. Mukund Chandra Mehta Registrar Date: