Dr. Babasaheb Ambedkar Open University, Ahmedabad

(Established by Government of Gujarat)

PROJECT GUIDELINES FOR STUDENTS

Programme: (MSCCS)

Course Type: Case Study/Dissertation **Course Code: MSCCS-404 (8-Credits)**

Weightage for Project Report:100% **(Project Report:75%, Viva-Voce:25%)**

Most professional curricula incorporate a substantial amount of project work. Students are encouraged to apply their innovative ideas to develop solutions that address the needs of the Cyber Security. Projects should be designed in a way that efficiently resolves present-day challenges. Rather than treating projects merely as a program requirement, students should leverage their innate abilities to create meaningful solutions, enhancing their value during IT industry interviews. Here's a breakdown of project guidelines for MSc Cybersecurity students:

A. Project Guide Eligibility Criteria:

Full Time Faculties in the Department of Computer Science/ Information Technology of BAOU/ Colleges/ Institutions affiliated to any Indian University recognized by UGC and having minimum 2 years teaching experience.

OR

A person having minimum M. Tech, MCA, M.Sc. in Computer Science/Information Technology from a UGC recognized universities with 4 years' experience in Industry/teaching.

Please note that spouse, direct relatives, and blood relations are not permitted to be the guide.

B. Points to remember while preparing the project proposal

1. The creation of the project report:

The project report should include the following:

(i) An original copy of the project proposal and the approved proforma.
(ii) Originality Certificate
(iii) Project documentation
(iv) Students need to send the project report to the guide via mail and upload the project report on the dedicated drive as well.

2. The project documentation might consist of between 100 and 150 pages(code not included). The project documentation's specifics shouldn't be overly standardised. It is necessary to properly record

your project report, including how you conducted your project's planning, scope definition, reconnaissance, assessment, analysis usage of testing techniques/strategies, etc. To be more precise, whatever theory is presented in the reference books about these areas should be disregarded as much as possible. Only your project should be covered in the project documentation.

3. On A4 paper (just one side), the project report should typically be produced with single line spacing. Numbering is required for all the pages, tables, and figures. Titles should be present in tables and figures.

4. The Regional Centre/Study Centre must receive just one copy of the original project report in bound form and send all the mentioned documents with the project report to the respective mail-id. The student must keep one photocopy of the identical Project Report which must be presented to the examiner during the viva-voce.

5. A Project cannot be submitted as Softcopy only. It is mandatory to mention your Course code, Course Name and type i.e. "**MSCCS-404**" "**Case Study/Dissertation"** and **Academic Year** on the first page so sorting will be easier for Regional Centre/Study Centre.

6. Ideally, only one student should be allowed to work on a project at a time. However, if a project is sufficiently extensive that it will take one human year or more to complete, only two students at most may work on it due to the requirement of six human months per student. Prior approval is required in this respect, and it must be acquired from the relevant Project Guide.

7. If two students are permitted to collaborate on a project, their project reports must only list the several modules that they both undertook or worked on independently. The project reports for each student's modules must be submitted separately. Project reports that are wholly similar are not permitted. Only the introduction and, potentially, the conclusion may be identical. In this situation, the preceding suggestion from the project coordinator or project guide must be attached by both students. It is not acceptable to submit a single copy of a project report that combines the work of two or more students. The project may be rejected if these standards are broken.

8. Every stage of the project development should engage the student. The project may be rejected or disqualified at any step if it is discovered that a student was not active in any phase, such as the Analysis phase.

9. Each student has to submit his/her Title of the Project within the first month of the Semester to the Project Guide or Project Coordinator.

10. Title of the project should be kept the same throughout the project.

C. Assessment Guidelines project Evaluation

1. Viva Voce

Students have the opportunity to showcase their knowledge and skills to the expert in this evaluation component. The student can be asked to present the project demo in addition to questions on the project-related topics and the relevant courses. Additionally, you can be instructed to develop the code for an issue to show off your analysis skills. The student must provide project report while appearing for the viva-voce.

2. Project Evaluation

Viva-voce is compulsory and forms part of evaluation. A student in order to be declared successful in the project must appear in both

(i) Project Evaluation and
(ii) Viva-voce. Pass in both the components is compulsory. If a student submitted the project report as per the schedule and fails to attend viva, her/his Project will remain incomplete and should contact the Regional Centre concerned.

3. Project Scope and Focus

- Practical Application: Projects should prioritize hands-on experience and problem-solving, rather than solely theoretical research.
- Real-World Scenarios: Projects should simulate real-world cybersecurity challenges and vulnerabilities.
- Ethical and Legal Considerations: Projects must adhere to ethical hacking principles and legal frameworks.
- Skill Development: Projects should focus on developing specific cybersecurity skills, such as penetration testing, malware analysis, network security, and incident response.

4. Project Ideas:

- **Penetration Testing:**
  - Conduct vulnerability assessments on web applications or network infrastructure.
  - Simulate real-world attacks to identify weaknesses.
  - Develop tools or scripts for automated vulnerability scanning.

- **Malware Analysis & Threat Detection**
  - Analyse malicious software samples to understand their behaviour and functionality.
  - Develop tools or scripts for malware detection and prevention.
  - Investigate the root cause of malware infections.
  - A Chrome/Firefox extension that warns users about dangerous sites.
  - Create a decoy system to attract and analyse hacker activity.

- **Network Security:**
  - Implement and configure network security devices, such as firewalls and intrusion detection systems.
  - Analyse network traffic to identify malicious activity.
  - Develop tools or scripts for network monitoring and security auditing.

- **Mobile Security**
  - Build an AI-powered malware scanner for mobile device.
  - Implement an end-to-end encrypted payment system.
  - A secure browser that blocks phishing attempts in real time.

- **Ethical Hacking:**
  - Simulate phishing attacks and social engineering techniques.

- Develop tools or scripts for password cracking and brute-forcing.
- Investigate the security of different systems and applications.

- **Cloud Security:**
- Assess the security posture of cloud environments.
- Develop tools or scripts for cloud security automation.
- Investigate cloud security threats and vulnerabilities.

- **Cybersecurity Awareness Training:**
- Develop and deliver cybersecurity awareness training programs for end-users.
- Create phishing simulations and awareness campaigns.
- Assess the effectiveness of cybersecurity awareness training.

- **IoT and Embedded Security**
- Detect intrusions using AI-based motion sensors.
- Implement a blockchain-based authentication system for IoT devices.
- Develop a lightweight encryption protocol for IoT devices.

- **Cybersecurity Policy Framework:**
- Develop and implement a cybersecurity policy framework for an organization.
- Conduct risk assessments and identify security gaps.
- Develop security incident response plans.

5. Project Resources:

- **Faculty Guidance:** Students should seek guidance from faculty members throughout the project lifecycle.
- **Online Resources:** Utilize online resources, such as cybersecurity blogs, forums, and tutorials.
- **Open-Source Tools:** Leverage open-source cybersecurity tools and frameworks.
- **Industry Experts:** Seek advice from industry professionals or cybersecurity experts

D. Project Proposal (Synopsis)

The project proposal or the synopsis is the frame work for carrying out the project. It should be prepared in consultation with Guide. The necessary parts of a project proposal are given in the following form:

- Title of the Project.

- Introduction and Objectives of the Project.

- Project Category.

- Tools, Platform, Hardware and Software Requirement specifications.

- Whether the project is done for any Industry/Client? The Name and

Address of the Industry or Client is to be mentioned.

- Expected output

- Conclusion

E. Application Areas & Related Tools

A list of selected area for developing the project work is given below:

Applications Areas:

Network Security
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Secure Wireless Communication
- Firewall Development and Optimization
- Virtual Private Networks (VPNs)

Web Security
- Secure Web Application Development
- Web Penetration Testing Tools
- SQL Injection and XSS Prevention
- Secure Authentication Mechanisms

Data Security & Cryptography
- End-to-End Encrypted Messaging Apps
- File Encryption and Decryption Tools
- Blockchain for Secure Transactions
- Steganography for Data Hiding

Malware Analysis & Threat Detection
- Ransomware Detection and Prevention
- AI-Based Malware Classification
- Honeypots for Cyber Threat Monitoring
- Botnet Detection Systems

Mobile Security
- Mobile App Vulnerability Scanners
- Secure Mobile Payment Systems
- Anti-Phishing Mobile Browser Extensions
- Android/iOS Malware Detection Tools

Digital Forensics
- Data Recovery & Incident Response Tools
- Mobile Forensics Applications
- Digital Evidence Collection & Analysis
- Social Media Crime Investigation Tools

Tools can be used :

Name of the tool	Functionality	Link for Download	OS Platform Availability
Burp Suit	Security assessments, vulnerability discovery, and ethical hacking	https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install	Windows & Linux OS
Metasploit	Vulnerability scanning and post-exploitation	https://www.metasploit.com/download	Windows & Linux OS
Nessus	Vulnerability scanning	https://www.tenable.com/products/nessus	Windows & Linux OS
Acunetix	Vulnerability scanning	https://www.acunetix.com/support/docs/wvs/installing-acunetix-wvs/	Windows & Linux OS
Nmap	Network scanning	https://nmap.org/download	Windows & Linux OS
Wireshark	Packet analyser	https://www.wireshark.org/download.html	Windows & Linux OS
SQLmap	SQL injection testing tool	https://sqlmap.org/	Linux OS
Aircrack-ng	Wi-Fi network penetration testing	https://www.aircrack-ng.org/downloads.html	Linux OS
OWASP ZAP	Web application security testing tool.	https://www.zaproxy.org/download/	Windows & Linux OS
Nikto	A web server vulnerability scanner	https://www.cirt.net/Nikto2	Windows & Linux OS
Ghidra	Malware analysis	https://ghidra-sre.org/	Windows & Linux OS
OllyDbg	Malware analysis	https://www.ollydbg.de/	Linux OS
Sysinternal	Malware analysis	https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite	Windows OS
IDA Pro	Malware analysis, vulnerability assessment	https://hex-rays.com/ida-free	Windows & Linux OS
Immunity Debugger	Malware analysis,	https://github.com/kbandla/ImmunityDebugger	Windows & Linux OS

	vulnerability assessment		
Volatility Framework	Malware analysis, digital forensics, and incident response	https://github.com/volatilityfoundation/volatility	Windows & Linux OS
Autopsy	Digital forensics	https://www.autopsy.com/download/	Windows & Linux OS
FTK Imager	Digital forensics	https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81	Windows OS
ExifTool	Digital forensics	https://exiftool.org/	Windows OS
Hashcat	Password cracking tool	https://hashcat.net/hashcat/	Windows & Linux OS
John the Ripper	Password security auditing tool	https://www.openwall.com/john/	Linux OS
Shodan	Search engine for finding exposed devices	https://www.shodan.io/	Windows & Linux OS
VirusTotal	Malware analysis	https://www.virustotal.com/gui/	Windows & Linux OS

Note: Students can also create projects using tools / languages / software not listed above, if they are part of latest technologies. Use the latest versions of the software packages for the project development.

F. The following suggested Guidelines must be followed in preparing the project Reports

Good quality white A4 size Paper should be used for project Report

Binding Specification: Spiral Binding

Page Specification:

Left margin: 3.0 cm	Right margin: 2.0 cm
Top margin: 2.55 cm	Bottom margin: 2.55 cm

- **Page numbers -** All Report page should be numbered at the bottom Centre of the pages.
- **Normal Body Text:** Font Size: 12, Time New Roman, justified.
- **Paragraph heading font Size:** 14, Times New Roman, Left Aligned.
- **Chapter Heading Font Size:** 20, Times New Roman
- **Coding Font size:** 10, Courier New, Normal(If available)

The Project Report should include:

- One hard Copy of the Project Report
- Soft copy of Project must be Sent and Upload to Mail and Drive.
- The Project may be between **100 and 150 pages** (excluding coding)

FORMAT OF THE MSCCS PROJECT REPORT

1. Cover page as per format	7. List of Figures
2. Originality Certificate	8. List of Tables
3. Declaration	9. Project Report
4. Acknowledgment	10. Conclusion And Future Enhancement
5. Abstract	11. List of Abbreviations
6. Table of Contents	12. Bibliography/References

Certificate of Originality from the Guide

This is to certify that the project report entitled

……

……submitted to **Dr. Babasaheb Ambedkar Open University** in partial fulfilment of the requirement for the award of the degree of **Master of Science in Cyber Security,** is an original work carried out by

Mr./ Ms. ……..

Enrolment No.: ……. under the supervision of Mr./Mr./Ms. ……

…….

The matter embodied in this project is a genuine work done by the learner and has not been submitted either to this University or to any other University/Institute for the fulfilment of the requirement of any course of study.

Signature of the Learner:	Signature of the Guide:
Name:	Name:
Address:	Designation:
Enrolment No.:	Address:
Date:	Date:

Seal of the Learner Support Centre

Format of the Software Project Report

A Project Report on Title of the Project

In fulfillment of the requirement for the 4th Semester of
Master of Science in Cyber Security

Submitted by

.....
(Name of the Learner)

Enrollment No.: .....

Session: .....

Under the Guidance of

.....
(Name of the Project Guide)

Learner Support Centre

.....
(Name of the Learner Support Centre)

.....
(Location)