

Security Audit Agreement

This Security Audit Agreement ("Agreement") is made effective this 16th July, 2025, by and between:

Connected Pakistan

Represented by: Haseeb Ali

("The Company"- Connected Pakistan)

AND

Haroon Allahdad

(Security Audit Conductor)

("The Auditor")

1. Purpose of the Audit:

The purpose of this Agreement is to outline the terms and scope of a one-time, limited-scope security audit to be conducted by The Auditor for The Company, aimed at identifying potential vulnerabilities and providing recommendations to enhance The Company's IT security posture.

2. Scope of Work:

The Auditor shall perform the following activities during the two-day on-site audit, strictly within **ethical boundaries** and with The Company's explicit authorization. This includes scanning, enumeration, and exploitation (where applicable and non-destructive) on the Connected Pakistan Website and its associated Security Protocols.

2.1. Initial Assessment & Information Gathering: Review of existing IT infrastructure, network topology, and available security policies.

2.1.2. Vulnerability Scanning: The Auditor will scan for any vulnerabilities present in the network, website and hosts (if allowed).

2.1.3. Network Scanning: Identification of open ports, services, and vulnerabilities on network devices (external and internal). Tools: Nmap.

2.1.4. Web Application Scanning: Assessment of The Company's website(s) for common web application vulnerabilities and misconfigurations. Tools: OWASP ZAP, Nikto.

2.2 Limited Penetration Testing:

2.2.1. Network Penetration Testing: Basic, non-destructive attempts to exploit identified low-risk network vulnerabilities.

2.2.2. Basic Configuration Testing: Review of common system and device configurations for security misconfigurations.

2.2.3. Password Strength Testing: Assessment of password policies and, with explicit permission, limited technical testing of password strength.

2.2.4. Social Engineering Awareness Test: A very basic, pre-approved phishing simulation on a limited group of employees to assess susceptibility.

2.2.5. Risk Analysis: Preliminary analysis of identified vulnerabilities, assessing their potential impact and prioritizing remediation efforts.

3. Deliverables:

3.1. Upon completion of the on-site audit and subsequent analysis, The Auditor will provide:

3.2. A comprehensive Security Assessment Report detailing findings, risks, and prioritized recommendations.

3.3. A professional presentation summarizing the audit results.

4. Authorization & Confidentiality:

The Company grants The Auditor full authorization to perform the activities outlined in Section 2. The Auditor agrees to maintain **strict confidentiality** of all information accessed during the audit and will not disclose any sensitive data to unauthorized third parties. All testing will be conducted with the utmost care to minimize disruption. **The Auditor will present non-sensitive data from the audit reports and assessment reports to the university for FYP documentation and grading purposes only, strictly in physical form, with no soft copies being provided.**

5. Terms:

This Agreement covers the security audit activities conducted on-site for two (2) days, specifically 16th July, 2025 and 17th July, 2025. Post-audit report generation and presentation will follow.

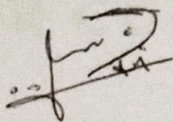
6. Limitation of Liability:

The Auditor's responsibility is limited to identifying and reporting security vulnerabilities and providing recommendations. The Auditor is not responsible for the implementation of any recommended solutions or for the remediation of identified security issues.

7. Cost of Services:

The Auditor agrees to perform the services outlined in this Agreement free of charge. The Auditor shall not seek any compensation or reimbursement for costs incurred in relation to this security audit, now or in the future.

Agreed and Accepted By:



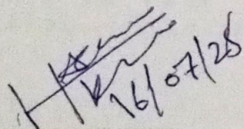
For Connected Pakistan:

Haseeb Ali,

Director

Admin & Partnerships,

Connected Pakistan



For The Auditor:

Haroon Allahdad

Security Audit Conductor