Rules of Engagement (RoE) for Penetration Testing

1. Objective

The primary objective of this penetration test is to identify and exploit vulnerabilities within the network environment to demonstrate potential impacts and provide actionable remediation recommendations.

2. Scope

- **In-Scope Systems**: All systems, applications, and networks explicitly listed in the engagement agreement.
- **Out-of-Scope Systems**: Any systems not explicitly listed in the engagement agreement, including production systems that could impact business operations if disrupted.

3. Methodology

The penetration test will follow the vPenTest methodology, which includes the following phases:

- **OSINT Gathering**: Collecting publicly available information about the organization without triggering security alerts.
- **Host Discovery**: Identifying active systems within the network using various techniques.
- **Enumeration**: Enumerating services running on identified systems to find potential vulnerabilities.
- **Exploitation**: Attempting to exploit identified vulnerabilities to gain access to systems.
- **Post-Exploitation and Lateral Movement**: Gathering additional information and escalating privileges to demonstrate the potential impact of vulnerabilities.

4. Rules and Constraints

- **Testing Window**: The penetration test will be conducted during the agreed-upon time frame to minimize disruption.
- **Intrusiveness**: While the test aims to demonstrate maximum impact, care will be taken to avoid causing service interruptions. Any potentially disruptive actions will be coordinated with the client.
- **Data Handling**: Sensitive data discovered during the test will be handled with the utmost confidentiality and will not be disclosed outside the engagement team.
- **Reporting**: A detailed report will be provided at the end of the engagement, outlining the findings, exploited vulnerabilities, and remediation recommendations.

5. Communication Plan

- **Point of Contact**: [Client's Point of Contact Name and Contact Information]
- **Environment Impact Reporting**: Any suspected impact to client networks during the test should be reported immediately Secure Cyber Defense.

6. Legal and Compliance

- **Authorization**: Written authorization from the client is required before commencing the penetration test.
- **Compliance**: The test will comply with all relevant laws and regulations, including data protection and privacy laws.

7. Termination Conditions

- **Early Termination**: The test may be terminated early if critical issues are discovered that require immediate remediation or if the client requests termination.
- **Completion**: The test will be considered complete once all in-scope systems have been tested and the final report has been delivered.