Penetration Testing Agreement

This Agreement ("Agreement") is entered into on this date by and between Crumbs of Joy Cookie Factory, hereinafter referred to as "Client," and the Pentesting Company, hereinafter referred to as "Pentester."

1. Scope of Work

1.1 **Client Information:** The Client engages the Pentester to perform a penetration test on the Cookie Manufacturing Shopfloor ICS/OT Network, encompassing all three production lines, including upstream (dough mixer) and downstream automation (stacking robot).

1.2 **Assessment Goal:** The primary objective of the penetration test is to evaluate the cybersecurity posture of the network without resorting to any form of exploitation.

1.3 **Limitations:** No exploitation of any kind is permitted. The focus is solely on reconnaissance and fingerprinting.

1.4 **Scope Expansion:** The Client acknowledges that additional hosts may be included in the testing scope upon recovery or based on the recommendation of the Pentesters.

1.5 **Allowed Subnet:** The testing will focus on the following subnet(s):

- **Production network 10.2.0.0/24**

1.6 **Scanning Tools:** The Pentester is authorized to employ

- **Netdiscover**
- **nmap, including NSE**

2. Penetration Testing Classification as per BSI

2.1 **Information base:** The penetration test will adopt a Black Box approach.

2.2 **Aggressiveness:** The penetration test will be conducted cautiously, emphasizing no exploitation.

2.3 **Scope:** The scope will be focused to the subnet mentioned in **1.5.**

2.4 **Approach**: n/a

2.5 **Technique/Starting point:** The Pentester will initiate the assessment from inside the factory with physical network access to the target production network.

3. Safe Scanning Methodology

3.1 **Legacy Devices:** Due to the presence of legacy devices, a ping sweep will be executed to identify safe devices for port scanning. Only devices responding to ICMP requests will be considered safe for further scanning.

4. Documentation and Reporting

4.1 **Client-provided Inventory:** The Client has attached a basic asset inventory that will serve as the basis for the penetration test and subsequent reporting.

4.2 **Detailed Asset Inventory:** The Pentester will provide a detailed report outlining the results of the penetration test, including an asset inventory, vulnerabilities discovered, and recommendations for mitigating identified risks.

4.3 **Network Topology:** The Pentester will include a network topology overview in the final report.