Customer Agreement

1. Introduction

This Customer Agreement ("Agreement") is made between [Company Name], located at [Company Address] ("Company"), and [Customer Name], located at [Customer Address] ("Customer"). This Agreement becomes effective as of [Effective Date].

2. Services Provided

The Company agrees to provide the services described in [Service Description or Scope of Work] to the Customer. These services will be provided in line with the terms and conditions specified in this Agreement.

3. Security Requirements

The Company is dedicated to maintaining a high level of security for the services provided to the Customer. The following security requirements apply:

3.1 Data Protection

- The Company will comply with all relevant data protection laws, including but not limited to the General Data Protection Regulation (GDPR), for handling and processing personal data.
- Customer data will be encrypted during transmission using TLS 1.2 or higher and stored using industry-standard encryption protocols.

3.2 Access Control

- Only authorized personnel will have access to Customer data. Access will be managed using a role-based access control (RBAC) system, ensuring that individuals only access data necessary for their responsibilities.
- Multi-factor authentication (MFA) will be required for all Company personnel accessing critical systems or customer information.

3.3 Network Security

- The Company will maintain network security through firewalls, intrusion detection systems (IDS), and regular vulnerability assessments.
- Security monitoring will be conducted continuously, and any unauthorized access attempts will be promptly investigated and mitigated.

3.4 Incident Response

- The Company will have an established Incident Response Plan (IRP) and will notify the Customer of any security incident affecting Customer data within 24 hours of discovery.
- The Company will take all reasonable steps to mitigate risks and restore services as quickly as possible following an incident.

3.5 Compliance Frameworks

- The Company will align its security practices with industry-recognized frameworks, including the NIST Cybersecurity Framework (CSF), CIS Security Controls, and ISO 27001.
- Security policies will be reviewed and updated annually or as needed to comply with regulatory changes.

3.6 Third-Party Risk Management

- The Company will ensure that any third-party vendors handling Customer data comply with equivalent security requirements.
- The Company will perform regular assessments of vendors to verify ongoing compliance.

3.7 Security Awareness and Training

- All Company employees will receive annual security awareness training on topics such as phishing, data handling, and privacy regulations.
- Specialized training will be provided for employees handling sensitive Customer information.

4. Term and Termination

This Agreement will begin on the Effective Date and will remain in effect until either party terminates it with [number] days' written notice.

5. Limitation of Liability

The Company will not be liable for any indirect, incidental, or consequential damages arising out of or in connection with this Agreement, except in cases of gross negligence or intentional misconduct.

6. Governing Law

This Agreement will be governed by and construed in accordance with the laws of [State/Country].

7. Entire Agreement

This Agreement represents the entire understanding between the Company and the Customer, superseding all prior agreements, whether written or verbal.

8. Signatures

[Authorized Representative of Company]
Name:
Title:
Date:

[Authorized Representative of Customer]
Name:
Title:
Date: