TakeLoan.

Third-Party Organization Terms and Policy for DSA Agent – Secure Document Handling

1. Purpose

This policy defines the terms, responsibilities, and security measures to be followed by third-party organizations and their DSA agents in collecting, processing, transmitting, and storing customer documents and data on behalf of the principal organization (the "Company").

2. Scope

This policy applies to all DSA agents, contractors, vendors, and partner organizations who:

- Collect customer information or documents (physical or digital)
- Access, store, or transmit personal, financial, or confidential data on behalf of the Company

3. Compliance Requirements

The third-party organization and its agents shall:

- Comply with applicable data protection laws (e.g., IT Act 2000, DPDP Act 2023, or GDPR if applicable)
- Follow all Company security protocols, confidentiality clauses, and audit requirements
- Obtain written consent from customers before collecting or sharing personal information

4. Document Security

a. Collection

- Documents must only be collected for authorized purposes.
- Customer consent must be obtained and recorded at the time of collection.
- No unnecessary data should be copied, photographed, or retained.

b. Storage

- Physical documents must be kept in locked, access-controlled facilities.
- Digital copies must be encrypted and stored in secure, approved systems.
- Access should be granted only to authorized personnel based on the principle of least privilege.

c. Transmission

- Documents must be transmitted using secure, encrypted channels (e.g., HTTPS, SFTP).
- No sharing of customer data over unsecured emails, messaging apps, or personal devices.

d. Disposal

- Documents must be securely destroyed (shredding for physical, secure deletion for digital) once retention timelines expire or the purpose is fulfilled.
- Destruction must be logged and verified.

5. Confidentiality

- The third-party organization shall treat all customer information as strictly confidential.
- Agents must sign a Non-Disclosure Agreement (NDA) before handling any documents.
- Breach of confidentiality will result in immediate termination of contract and potential legal action.

6. Audit and Monitoring

- The Company reserves the right to conduct regular or surprise audits to ensure compliance.
- Third-party organizations must maintain records of data handling activities and make them available upon request.

7. Incident Management

- Any data breach, document loss, or unauthorized access must be reported to the Company within 24 hours of discovery.
- The third-party must cooperate fully in investigation and remediation efforts.

TakeLoan.

8. Liability

- The third-party organization is fully responsible for the actions of its agents and sub-contractors.
- Any damages, legal costs, or penalties arising from negligence, data breaches, or policy violations will be borne by the third-party.

9. Training and Awareness

All DSA agents must undergo Company-approved training on data privacy, information security, and document handling procedures before deployment.

10. Termination

The Company may terminate the engagement with immediate effect in case of non-compliance, breach of confidentiality, or data security incident.

11. Acknowledgment

By signing this policy, the third-party organization acknowledges its responsibility to protect customer data and agrees to adhere to the above terms without exception.

Regards

Sahil Mukherjee

Founder

TakeLoan.