True North Receivables

True North Receivables Group
contact@truenorthreceivables.com
www.truenorthreceivables.com

Privacy and Data Security Policy

Effective Date: May 29, 2025

Approved By: Ethan Domangue, Managing Member

1. Purpose

This policy outlines how True North Receivables Group protects consumer and vendor information from unauthorized access, use, disclosure, or destruction in accordance with FDCPA, FCRA, and data protection best practices.

2. Scope

This policy applies to all personal, financial, and account-level data received, stored, processed, or transmitted by the company or its authorized vendors.

3. Data Classification

Data is classified into the following categories:

- Public: Company website content, general policy documents

- Internal: Vendor agreements, training materials

- Confidential: Consumer account data, SSNs, balances, dispute records

4. Data Security Controls

The following controls shall be enforced:

- Use of password-protected folders for confidential files

- Role-based access control: only authorized users may access sensitive data

- Encrypted storage for any cloud-based data

- Secure file sharing via encrypted email or secure portals

- Antivirus and firewall software on all company devices

5. Data Handling Procedures

- No consumer data shall be printed or stored on personal devices

- Data shared with vendors must be transmitted securely

- Employees must log off devices when not in use

- All removable media must be encrypted or approved for use

6. Breach Notification

In the event of a data breach:

- The Compliance Officer must be notified within 24 hours

- Affected parties and any regulatory bodies will be informed within the legally required timeframe

- An incident report will be completed and mitigation steps taken

7. Vendor Compliance

All vendors must sign a confidentiality agreement and demonstrate technical and procedural safeguards before receiving consumer data. Vendor compliance will be reviewed annually.

8. Training & Enforcement

All employees and contractors must complete privacy and security training before handling sensitive data. Any violation of this policy may result in disciplinary action or termination of contract.

9. Policy Review

This policy shall be reviewed and updated at least annually or in response to changes in laws, technology, or business practices.