Data Policy

Effective Date: 4/22/25

This Data Policy (“Policy”) governs the collection, processing, storage, retention, and deletion of data by TrueForce (“Company,” “we,” “us,” or “our”) in connection with the TrueForce machine and application (collectively, the “Services”). By accessing or using the Services, you (“User,” “you,” or “your”) agree to this Policy.

1. Scope and Applicability

This Policy applies to all data collected through the Services, including personal information, device connectivity data, and performance-related data generated through the TrueForce system.

2. Categories of Data Collected

We collect and process only data reasonably necessary to operate the Services, including:

- **Account Data:** Name, contact information, login credentials
- **Performance Data:** Strength, output, and other metrics generated through the TrueForce machine
- **Usage Data:** Interactions with the application and system functionality
- **Device Data:** Bluetooth connectivity information required to pair and communicate with the TrueForce device

3. Purpose of Data Processing

Your data is processed for legitimate business purposes, including:

- Providing, maintaining, and improving the Services
- Enabling secure authentication and account management
- Facilitating Bluetooth communication between the application and device
- Enhancing system performance and user experience

We do not process data beyond what is necessary for these purposes.

4. Health and Performance Data Handling (HIPAA-Style Language)

Certain performance metrics may be considered health-related information.

- We apply safeguards consistent with industry standards for protecting sensitive data
- TrueForce is **not a Covered Entity** under the Health Insurance Portability and Accountability Act ("HIPAA") and does not represent itself as HIPAA-compliant unless explicitly stated in a separate agreement
- Where required by contract (e.g., a Business Associate Agreement), additional protections may be implemented

5. Data Security Measures

We implement commercially reasonable safeguards designed to protect your data, including:

- **Administrative Safeguards:** Internal policies, employee access controls, and data handling procedures
- **Technical Safeguards:** Password-protected accounts, secure system architecture, and restricted access
- **Operational Safeguards:** Limiting data access to authorized personnel only

Despite these efforts, you acknowledge that no method of transmission or storage is completely secure.

6. User Account Responsibility

You are responsible for maintaining the confidentiality of your account credentials. Any activity conducted under your account is your responsibility. The Company is not liable for unauthorized access resulting from compromised credentials.

7. Bluetooth Data Transmission

The Services rely on Bluetooth technology for device connectivity. By using the Services, you consent to this method of communication. While we take reasonable precautions, wireless transmissions may not be fully secure.

8. Data Retention and Deletion

- Data is retained for as long as necessary to provide the Services
- Upon account deletion, data is retained for **thirty (30) days**
- After this period, data is **permanently deleted and cannot be recovered**

We are not responsible for restoring data after permanent deletion.

9. User Rights (Iowa Residents)

Subject to applicable law, including the Iowa Consumer Data Protection Act (ICDPA), you may:

- Request confirmation of data processing
- Access personal data associated with your account
- Request deletion of your data

We reserve the right to verify your identity and deny requests as permitted by law.

10. Data Minimization and Access Control

We adhere to a “minimum necessary” approach:

- Data collection is limited to what is required for service functionality
- Access to data is restricted to authorized personnel with a legitimate business need

11. Data Breach and Incident Response

In the event of a data breach:

- We will take prompt action to contain and investigate the incident
- Notifications will be made as required by applicable law
- Reasonable steps will be taken to mitigate potential harm

12. Third-Party Service Providers

We may engage third-party vendors to support our Services. These providers:

- Are contractually obligated to protect your data
- May only use data for specified service-related purposes

13. Limitation of Liability

To the maximum extent permitted by law, including the laws of the State of Iowa, TrueForce shall not be liable for:

- Indirect, incidental, or consequential damages
- Loss of data or business interruption
- Unauthorized access beyond our reasonable control

14. Governing Law and Jurisdiction

This Policy shall be governed by the laws of the State of Iowa.
Any disputes arising from this Policy shall be resolved exclusively in the courts located within Iowa.

15. Updates to This Policy

We reserve the right to modify this Policy at any time. Changes will be effective upon posting. Continued use of the Services constitutes acceptance of the updated Policy.

16. Contact Information

For questions or requests related to this Policy, please contact:

True Force Technologies
support@trueforcetechnologies.com
(515) 317-7564