**JD Analytics and Solutions — Safety & Security Audit Form**

**Audit Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Auditor:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Department/Area:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Version:** 1.0

**Section 1 – Business Overview**

1. **Business Scope Check**
   * LLC purpose statement reviewed and current.
   * All active services align with LLC scope.
   * New services or platforms evaluated for legal compliance.

**Section 2 – Cybersecurity**

1. **Account & Authentication**
   * Multi-factor authentication enabled for all accounts.
   * Strong, unique passwords for each service.
   * Access levels reviewed (least privilege principle).
2. **Device Security**
   * All company devices encrypted (BitLocker or equivalent).
   * Auto-lock set for inactivity (≤ 15 min).
   * Antivirus and endpoint protection active.
3. **Network Security**
   * Business-grade firewall/router in use.
   * VPN available for public Wi-Fi use.
   * Wi-Fi secured with WPA3 or WPA2 and strong password.
4. **Data Protection**
   * Daily backups for client and business data.
   * Backup restore process tested in the last 6 months.
   * Secure deletion used for old or unnecessary data.
5. **Breach Preparedness**
   * Incident response plan exists and is up to date.
   * Breach notification procedures comply with state laws.

**Section 3 – Physical Security**

1. **Office Protection**
   * Lockable office door and/or secure entry system.
   * Security camera(s) or monitoring (if applicable).
2. **Asset Protection**
   * Laptops, tablets, and external drives secured when not in use.
   * Fireproof lockbox or cabinet for important documents.
   * Surge protectors and/or UPS units in place.
3. **Work-from-Home Protocol**
   * Dedicated work devices separate from personal devices.
   * Clear desk policy for sensitive documents.

**Section 4 – Legal & Compliance**

1. **Policies**
   * Privacy Policy and Terms of Service current.
   * Data retention schedule documented.
   * NDAs in place for sensitive client engagements.

**Regulatory**

* + FTC reasonable data security measures in place.
  + State and federal compliance requirements reviewed.

**Section 5 – Project/Platform Specific Checks**

1. **Risk Assessment**
   * Platform has been reviewed for fraud prevention needs.
   * Content moderation policies documented.
2. **User Data**
   * Minimal data collection principle applied.
   * Consent gathered for any stored personal data.
   * Clear process for deleting user accounts and data.

**Section 6 – Employee & Vendor Security**

1. **Training**
   * Security awareness training completed in the last 12 months.
   * Phishing simulation or equivalent training acquired
2. **Vendor Controls**
   * Vendors reviewed for security posture.
   * Data processing agreements in place (if applicable).

**Auditor Notes:**

**Follow-Up Actions:**

**Next Audit Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_