Comprehensive Data Security Policy and Program (TikTok Compliance)

1. Executive Summary and Commitment to TikTok Standards

- **Mission Statement:**
  - Our organization is committed to upholding the highest standards of data security and privacy, particularly concerning data related to TikTok users and interactions.
  - We recognize the unique requirements and expectations set forth by TikTok and pledge to implement rigorous safeguards to protect user data.
  - This document outlines our comprehensive data security policy and program, which is designed to ensure compliance with all applicable laws, regulations, and TikTok's specific guidelines.
- **Core Principles:**
  - Transparency: We will maintain open and honest communication with users regarding data collection, usage, and sharing practices, in alignment with TikTok's transparency standards.
  - Accountability: We will establish clear lines of responsibility and accountability for data protection throughout our organization.
  - Continuous Improvement: We will continuously monitor and update our security measures to address evolving threats and maintain alignment with TikTok's evolving policies.
  - Lawfulness, Fairness and Transparency: We will collect and process data in accordance with the law, with fairness and with transparency. We will be very clear with our users about the data we collect.
  - Purpose Limitation: We will only collect data for explict and legitimate purposes.
  - Data Minimization: We will only collect the data which is adequate, relevant and limited to what is necessary.
  - Accuracy: Data will be accurate and where necessary kept up to date.
  - Storage Limitation: Data will be kept in a form which permits identification of data subjects for no longer than is necessary.
  - Integrity and Confidentiality:[1] Data will be processed in a manner that ensures appropriate security of the personal data.[2]
  - 1. www.lfha.co.uk
  - www.lfha.co.uk
  - 2. www.nhsfife.org
  - www.nhsfife.org
  -
  - Responsibility: The data controller, shall be responsible for, and be able to demonstrate compliance.
- **TikTok-Specific Focus:**
  - We acknowledge the sensitivity of TikTok user data and will implement specific safeguards to protect this information from unauthorized access, use, or disclosure.
  - We will comply with all TikTok-mandated security assessments, audits, and reporting requirements.

    - We will ensure that all API usage, and data pulled from TikTok, will be used in accordance to tiktoks terms of service.
    - We will respond rapidly to all customer data requests, as is dictated by all applicable laws, and tiktoks requirements.

2. Detailed Data Security Policy

- **Data Classification and Handling:**
    - Implementation of a granular data classification system to categorize all data based on sensitivity levels (e.g., public, internal, confidential, restricted).
    - Strict data handling procedures for each classification level, including encryption, access controls, and data loss prevention (DLP) measures.
    - Emphasis on protecting TikTok user data with the highest level of security controls.
- **Advanced Access Control Mechanisms:**
    - Multi-factor authentication (MFA) enforcement for all access to sensitive systems and data.
    - Role-based access control (RBAC) with granular permissions to limit user access to only necessary resources.
    - Just-in-time (JIT) access provisioning for temporary access needs.
    - Biometric authentication, where applicable.
- **Robust Data Encryption and Integrity:**
    - End-to-end encryption for data in transit and at rest, using industry-standard encryption protocols.
    - Data integrity checks to prevent unauthorized modifications or tampering.
    - Hashing and salting sensitive data.
- **Comprehensive Data Backup and Disaster Recovery:**
    - Automated and regular data backups with secure offsite storage.
    - Disaster recovery plan with defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
    - Periodic testing of backup and recovery procedures.
- **Strengthened Physical Security:**
    - Multi-layered physical security controls for data centers and server rooms (e.g., access control, surveillance, environmental monitoring).
    - Secure disposal of physical storage media.

3. Enhanced Access Management Program

- **Proactive User Lifecycle Management:**
    - Formalized onboarding and offboarding procedures for user accounts.
    - Automated provisioning and de-provisioning of user access.
    - Regular access reviews to ensure ongoing appropriateness of user permissions.
- **Advanced Security Monitoring and Logging:**
    - Implementation of a security information and event management (SIEM) system for real-time monitoring of security events.
    - Detailed logging of all user activity and data access.
    - Intrusion detection and prevention systems (IDPS).

- **Privileged Access Management (PAM):**
    - Strict control and monitoring of privileged user accounts.
    - Session recording and auditing of privileged access activities.

4. Data Governance and Lifecycle Management

- **Data Minimization and Purpose Limitation:**
    - Implementation of data retention policies to minimize data storage.
    - Regular data purging to remove unnecessary data.
    - Strict adherence to the purpose limitation data principles.
- **Data Sharing and Third-Party Management:**
    - Due diligence process for selecting and managing third-party vendors.
    - Contractual agreements with third parties that include strict data security and privacy requirements.
    - Regular audits of third-party security practices.
- **User Data Rights and Requests:**
    - Established procedures for handling user data access, rectification, erasure, and portability requests.
    - Compliance with all data subject rights under applicable laws and regulations, and tiktok rules.

5. Robust Permissions Management

- **Least Privilege Enforcement:**
    - Regular reviews of user permissions to ensure strict adherence to the principle of least privilege.
    - Automated tools to identify and remediate excessive permissions.
- **Role-Based Access Control (RBAC) Optimization:**
    - Regular reviews and updates to RBAC roles and permissions.
    - Automated tools for managing RBAC assignments.
- **Continual Permission Auditing:**
    - Automated checking of permissions, and alerts for abnormal permissions.

6. Comprehensive Data Breach Response and Prevention

- **Formalized Incident Response Plan:**
    - Detailed incident response plan with clearly defined roles and responsibilities.
    - Regular incident response training and simulations.
    - Rapid incident response times.
- **Transparent Breach Notification Procedures:**
    - Procedures for notifying users and regulatory authorities of data breaches, as required by law and tiktok.
    - Clear communication protocols for breach notifications.
- **Thorough Post-Breach Analysis:**
    - In-depth root cause analysis of all data breaches.
    - Implementation of corrective actions to prevent future breaches.
- **Advanced Threat Detection and Prevention:**
    - Implementation of advanced threat intelligence and security analytics.
    - Proactive vulnerability management and patching.

7. Extensive Training and Awareness Programs

- **Mandatory Security Training:**
  - Mandatory security awareness training for all employees.
  - Regular refresher training to keep employees up to date on security threats and best practices.
  - Training focused on TikToks data security procedures.
- **Phishing Awareness Campaigns:**
  - Regular phishing simulation and awareness campaigns.
- **Security Champion Program:**
  - Identify staff members who will champion security awareness.
- **Regular information disemination:**
  - Keeping staff informed about changes in tiktok data security policies.

8. Rigorous Audit and Compliance

- **Independent Security Audits:**
  - Regular independent security audits to assess compliance with policies and standards.
  - Penetration testing and vulnerability assessments.
  - Audits of tiktok API usage.
- **Continuous Compliance Monitoring:**
  - Automated compliance monitoring tools.
- **Data Protection Impact Assessments (DPIAs):**
  - Completion of DPIAs.

9. Dedicated Data Protection Officer (DPO) and Contacts

- Designated DPO with expertise in data protection laws and practices.
- Clear communication channels for reporting security incidents or asking questions about data privacy.
- Clear escalation process for all data breaches.

This expanded document aims to provide a very thorough outline of data protection.