SOP: Feedback Data Storage, Security, and Access Control

This SOP details the procedures for **feedback data storage, security, and access control**, encompassing secure data collection methods, encrypted storage solutions, user access management, data privacy compliance, regular security audits, and incident response protocols. The objective is to safeguard feedback data integrity, confidentiality, and availability while ensuring authorized access and preventing unauthorized data breaches.

1. Purpose

To establish standardized procedures for storing, securing, and controlling access to feedback data, ensuring compliance with relevant data protection laws and organizational policies.

2. Scope

This SOP applies to all personnel, contractors, and systems involved in the collection, storage, management, and security of feedback data within the organization.

3. Responsibilities

- **Data Owners:** Ensure compliance and oversee feedback data management.
- **IT Department:** Manage technical controls, implement encryption, and conduct audits.
- **All Users:** Adhere to access controls and report incidents.
- **Security Team:** Conduct risk assessments and respond to security incidents.

4. Procedures

1. **Secure Data Collection**
    - Use secure (HTTPS/TLS) web forms, applications, or APIs for feedback collection.
    - Limit data fields to essential information required for feedback analysis.
2. **Encrypted Storage Solutions**
    - Store all feedback data in approved, encrypted databases or file systems (AES-256 or higher).
    - Implement secure backups with identical encryption standards.
3. **User Access Management**
    - Grant access based on roles, following the principle of least privilege.
    - Maintain and regularly review access lists. Remove or update access as roles change.
    - Use multi-factor authentication (MFA) for privileged access.
4. **Data Privacy Compliance**
    - Adhere to applicable data protection regulations (e.g., GDPR, CCPA).
    - Maintain clear consent documentation for all feedback collected.
5. **Regular Security Audits**
    - Conduct biannual security audits of feedback data storage and access controls.
    - Remediate findings promptly and document actions taken.
6. **Incident Response Protocols**
    - Immediately report suspected data breaches to the security team.
    - Follow the established incident response plan: identification, containment, eradication, recovery, and lessons learned.
    - Notify affected parties per legal and policy requirements.

5. Record Keeping

- Maintain logs of all access, modifications, and transfers of feedback data.
- Archive audit reports, consent forms, and incident reports securely for a minimum of 3 years.

6. Review and Update

This SOP will be reviewed annually, or sooner if significant changes to technology, policy, or regulation occur.

7. References

- Data Protection Regulation Documents (GDPR, CCPA, etc.)
- Organizational IT Security Policy
- Incident Response Policy

8. Revision History

Version	Date	Description	Author
1.0	2024-06-20	Initial SOP release	Policy Team