Standard Operating Procedure (SOP)

Secure Storage and Confidentiality of Performance Review Records

This SOP details the procedures for the **secure storage and confidentiality of performance review records**, ensuring that all employee evaluations are handled with the utmost privacy and protection. It covers the methods for safeguarding physical and electronic records, access control measures, data encryption, authorized personnel responsibilities, and protocols for record retention and disposal. The objective is to maintain the integrity and confidentiality of performance information to comply with legal requirements and protect employee privacy.

1. Scope

This SOP applies to all personnel responsible for creating, storing, accessing, and processing performance review records, whether in physical or electronic form.

2. Definitions

- **Performance Review Records:** All documents, forms, and data related to employee evaluations.
- **Authorized Personnel:** Employees granted access to records based on their job functions.
- **Confidential Information:** Any data regarding individual employee performance, ratings, comments, and related documentation.

3. Secure Storage Procedures

Medium	Storage Method	Access Control
Physical Records	Store in locked, fire-resistant file cabinets within a secure area. Limit access to rooms containing records using electronic or key locks.	Only authorized HR personnel and management. Record log of access.
Electronic Records	Store in secure servers with file-level and disk-level encryption. Utilize organization-approved document management systems.	Access via individual login credentials. Multi-factor authentication (MFA) required. Restrict permissions based on role.

4. Data Encryption

- All electronic records must be encrypted at rest and in transit using current industry standards (e.g., AES-256).
- Email transmission of performance records is prohibited unless encrypted.

5. Access Control and Confidentiality

- Access only granted to HR staff, relevant managers, and legal/compliance officers as required.
- Annual review of access rights must be conducted by HR.
- Unauthorized access or disclosure is subject to disciplinary action.
- Personnel with access must sign confidentiality agreements.

6. Retention and Disposal

- Retain records in accordance with legal and regulatory retention schedules (typically 7 years, or as mandated).
- Shred physical records using a cross-cut shredder when disposal is authorized.
- Permanently delete and securely wipe electronic records when disposal is authorized.
- Log all disposal actions with date, method, and person responsible.

7. Responsibilities

- **HR Department:** Overall custodian of performance records, ensures SOP compliance and maintains access logs.
- **IT Department:** Maintains electronic storage security and provides encryption tools.
- **Managers:** Ensure records are not disclosed or misused.
- **All Employees:** Report any confidentiality breaches or security incidents promptly.

8. Review and Audit

- This SOP is to be reviewed annually or whenever there are changes to relevant laws or company policy.
- Regular audits must be conducted to ensure compliance with storage and confidentiality requirements.

9. Related Documents

- Confidentiality Policy
- Information Security Policy
- Record Retention Schedule
- Access Control Policy

10. Document Control

- **Version:** 1.0
- **Effective Date:** [Insert Date]
- **Reviewed By:** [Insert Reviewer]
- **Next Review Date:** [Insert Date]