SOP: Record Confidentiality and Access Authorization Protocols

This SOP details **record confidentiality and access authorization protocols**, outlining the procedures for safeguarding sensitive information, defining access levels, and ensuring authorized personnel only can view or modify records. It covers data protection measures, user authentication processes, permission management, and compliance with privacy regulations to prevent unauthorized access and maintain the integrity and confidentiality of organizational records.

1. Purpose

To establish standardized procedures for maintaining confidentiality of records and ensuring access is strictly limited to authorized personnel in compliance with applicable data protection and privacy laws.

2. Scope

This SOP applies to all employees, contractors, and third-party users who access, handle, or manage organizational records in any form (electronic or physical).

3. Definitions

- **Confidential Records:** Documents or data containing sensitive information protected by law or policy.
- **Access Authorization:** The formal process for permitting specific individuals to view or modify records.
- **User Authentication:** The technical process used to verify the identity of users requesting access.

4. Responsibilities

- **Data Owner:** Assigns access levels and approves authorizations.
- **IT Administrator:** Implements technical safeguards and monitors access activities.
- **All Personnel:** Adhere to this protocol and report suspected breaches.

5. Procedures

1. **Record Classification**
    - Classify records according to sensitivity (e.g., public, internal, restricted, confidential).
    - Label records appropriately to indicate required security measures.
2. **Access Authorization**
    - Grant access on a need-to-know basis; principle of least privilege applies.
    - Obtain written approval from data owner before providing access to restricted/confidential records.
    - Maintain an up-to-date access control list (ACL).
3. **User Authentication**
    - Require strong, unique passwords and, where possible, multi-factor authentication (MFA).
    - Regularly review and update authentication methods.
4. **Permission Management**
    - Review permissions periodically and revoke access when no longer needed (e.g., change of role, termination).
    - Log all access and modification activities for review and audit.
5. **Data Protection**
    - Apply encryption to records at rest and in transit where applicable.
    - Ensure physical records are stored in locked, access-controlled environments.

6. **Compliance and Training**
    - Comply with relevant privacy laws and internal policies (list specific regulations if needed).
    - Train all personnel annually on data confidentiality and access protocols.
7. **Incident Response**
    - Report suspected breaches or unauthorized access immediately to data owner or IT security team.
    - Investigate incidents according to organizational incident response procedures.

6. Access Levels Matrix (Sample)

Role	View	Edit	Delete	Approval Required
Employee	Own Records	No	No	No
Manager	Team Records	Team Records	Own Records	Yes
Data Owner	All Records	All Records	All Records	Yes
IT Admin	System Logs, All Records	System Only	System Only	Yes

7. Revision & Review

- This SOP is to be reviewed annually or upon significant change in legislation or operational practices.
- Revision history must be documented and changes communicated to all stakeholders.

8. References

- [List relevant legislation/regulations, such as GDPR, HIPAA, internal policy IDs]
- Organizational IT Security Policy
- Data Privacy and Protection Protocols

9. Appendices

- Access Authorization Form
- Incident Report Template
- Record Classification Guide