SOP Template: Visitor and Third-Party Document Handling Instructions

This SOP details **visitor and third-party document handling instructions**, outlining the proper procedures for managing, reviewing, and securely storing documents exchanged with visitors and external parties. It emphasizes confidentiality, compliance with data protection regulations, accurate record-keeping, and authorized access to sensitive information to ensure organizational security and operational efficiency.

1. Purpose

To establish standardized procedures for handling, reviewing, and securing documents exchanged with visitors and third parties, ensuring confidentiality, data protection, and organizational integrity.

2. Scope

This SOP applies to all employees and contractors who manage, review, or store documents supplied by or exchanged with visitors or external parties.

3. Responsibilities

- **Document Handlers:** Ensure correct receipt, review, and storage of documents.
- **Supervisors/Managers:** Oversee compliance and maintain proper record-keeping.
- **IT/Security Personnel:** Provide secure storage solutions and access control.

4. Procedure

4.1 Document Receipt

1. Verify the identity and authorization of the visitor or third party presenting documents.
2. Record details of the document received (date, source, purpose, and type).
3. Log the receipt in the designated register or electronic system.

4.2 Document Review

1. Check documents for completeness, accuracy, and relevance.
2. Report any discrepancies or unauthorized documents to the appropriate supervisor.
3. Ensure only authorized personnel review sensitive or confidential information.

4.3 Secure Storage

1. Store physical documents in locked cabinets with limited access.
2. Scan and archive electronic copies in secure, access-controlled digital repositories.
3. Label and track documents to ensure traceability and prevent unauthorized access.

4.4 Access Control

1. Grant document access only to staff with documented authorization.
2. Regularly review and update access permissions.
3. Maintain an audit trail of all accesses and modifications.

4.5 Retention and Disposal

1. Retain documents according to organizational and legal requirements.
2. When retention period lapses, securely destroy physical documents (e.g., shredding) and purge digital copies per policy.
3. Record disposal actions in the document register.

5. Confidentiality and Data Protection

- Handle all documents per applicable data protection laws and organizational privacy policies.
- Do not share documents or information with unauthorized parties.
- Immediately report any data breach or incident to the Data Protection Officer.

6. Training and Awareness

- All staff must receive training on document handling procedures and data protection requirements.
- Refresher training will be conducted annually, or as required by regulatory changes.

7. Documentation and Records

- Maintain an accurate log of all visitor and third-party documents received, reviewed, accessed, stored, and destroyed.
- Store logs securely and make them available for audit.

8. References

- Data Protection Regulations (e.g., GDPR, local laws)
- Company Confidentiality and Security Policies
- Internal Audit Requirements

9. Revision History

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