Standard Operating Procedure (SOP)

Access Control and Document Security Measures

This SOP details the **access control and document security measures** implemented to protect sensitive information and restrict unauthorized entry. It covers user authentication protocols, physical and digital access restrictions, secure document handling and storage, regular access audits, and incident response procedures to ensure the confidentiality, integrity, and availability of organizational documents.

1. Purpose

To establish standardized access control and document security procedures to safeguard organizational documents against unauthorized access, loss, or compromise.

2. Scope

This SOP applies to all personnel, contractors, and visitors accessing sensitive documents (both physical and electronic) within the organization.

3. Responsibilities

- **IT and Security Team:** Implement and monitor technical and physical controls.
- **Department Managers:** Authorize document access and review permissions.
- **All Employees:** Adhere to access protocols and security measures.

4. User Authentication Protocols

- All users must have unique credentials (username and password) to access digital systems.
- Passwords must meet complexity requirements (minimum 8 characters, including upper/lowercase, numbers, and symbols).
- Multi-factor authentication (MFA) is required for access to sensitive systems.
- User credentials are not to be shared under any circumstances.

5. Physical and Digital Access Restrictions

- Secure all physical document storage areas with locks and access cards/keys.
- Restrict entry to document storage areas to authorized personnel only; maintain visitor logs.
- Implement role-based access controls (RBAC) for digital documents; permissions granted on a need-to-know basis.
- Regularly review and update access lists.

6. Secure Document Handling and Storage

- Label sensitive documents as "Confidential" or "Restricted" as appropriate.
- Store physical documents in locked cabinets or secure rooms when not in use.
- Ensure electronic documents are stored in encrypted storage locations.
- Never leave sensitive documents unattended in public or shared spaces.

7. Regular Access Audits

- Conduct formal access reviews **quarterly** to confirm only authorized users have access to sensitive information.
- Document findings and correct any discrepancies immediately.
- Maintain audit logs for a minimum of 1 year.

8. Incident Response Procedures

- Report all suspected or confirmed access violations immediately to the IT and Security Team.
- Initiate an investigation within 24 hours of incident notification.
- Contain and mitigate threats; document response actions and outcomes.
- Review and revise security protocols post-incident as necessary.

9. Training and Awareness

- All staff must receive annual training on access control and document security best practices.
- Refresher sessions will be provided after any major update to procedures.

10. Review and Maintenance

- This SOP will be reviewed annually or as necessary following security incidents or organizational changes.
- Any amendments must be approved by senior management.

11. References

- ISO/IEC 27001 - Information Security Management Systems
- Company Information Security Policy

12. Document Control

Version	Date	Prepared By	Reviewed By	Approved By
1.0	2024-06-07	[Name]	[Name]	[Name]