Standard Operating Procedure (SOP)

Routine Security Audit and Compliance Checks

Purpose:

This SOP details the process for conducting **routine security audit and compliance checks**, including scheduling regular audits, assessing security controls, verifying adherence to policies and regulations, documenting findings, addressing vulnerabilities, and ensuring continuous improvement of security measures. The objective is to maintain robust security posture and ensure compliance with organizational and legal requirements.

Scope

This SOP applies to all information systems, employees, and contractors involved in the management, operation, and support of the organization's information security.

Roles and Responsibilities

Role	Responsibility
Security Officer	Coordinates audit activities, reviews audit results, and ensures remediation of vulnerabilities.
IT Team	Assists auditors, implements required security controls, and participates in compliance verifications.
Internal/External Auditors	Conduct security audits, assess controls, and document findings.
Compliance Manager	Ensures all legal and regulatory standards are evaluated and met.

Procedure

1. **Audit Scheduling**
    - Develop and maintain an audit calendar ensuring audits are conducted at least annually or as required by policy/regulations.
    - Notify relevant stakeholders about upcoming audits.
2. **Preparation**
    - Confirm audit scope, objectives, and criteria.
    - Assemble audit team and necessary documentation.
3. **Assessment of Security Controls**
    - Review implementation and effectiveness of administrative, technical, and physical security controls.
    - Conduct interviews, review documentation, and perform technical testing as appropriate.
4. **Compliance Verification**
    - Cross-check adherence to organizational security policies and applicable laws/regulations (e.g., GDPR, HIPAA).
5. **Documentation of Findings**
    - Record all findings, categorize by risk level and responsible parties.
    - Provide detailed audit reports to management and stakeholders.
6. **Remediation and Follow-Up**
    - Assign accountability for addressing vulnerabilities and recommendations.
    - Track progress of remediation efforts and validate closure of findings.
7. **Continuous Improvement**
    - Review audit outcomes to identify trends and opportunities for enhancing security controls and compliance posture.
    - Update policies, controls, and training as needed.

Documentation and Records

- Maintain audit plans, checklists, reports, and evidence for required retention periods and for review by regulators or management.
- Securely store all documents according to data protection standards.

References

- Information Security Policy
- Applicable regulatory requirements (e.g., GDPR, HIPAA, ISO 27001)
- Previous audit reports

Revision History

Version	Date	Description	Author
1.0	2024-06-09	Initial SOP release	[Your Name/Title]