Steel Strips Wheels Limited

INTERNAL AUDIT POLICY

Document Number: SSWL/ IT/IA/ 01

Classification: Internal

Address:

Steel Strips Wheels Ltd

S.C.O 49-50, Sector 26, Madhya Marg,

Chandigarh-160019, India

CONTROLLED COPY

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Control

Document Name	Internal Audit Policy
Document Number	SSWL/IT/IA/ 01
Effective Date	01.04.2025
Issue No.	01
Revision No.	00
Next Review Date	01.04.2026
Classification	Internal
Custodian Department	IT Department
Prepared By	Dy. Manager - IT
Approved By	General Manager - IT

Revision History

Revision	Requested By	Revision Date	Sections modified/ Summary of Changes	Approved By

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

1. Purpose

Ensure that all the applicable controls within the SSWL environment must be assessed about implementation, operating effectiveness and to provide status to SSWL management.

2. Scope

This policy is applicable to all Employees and information processing facilities of Steel Strips Wheels Limited

3. Policy Statement

The information security policy adherence and control effectiveness at SSWL shall be regularly checked through security audits/reviews by independent party/internal audits.

4. Policy Sections & Clauses

4.1 Internal Audits

Information processing facility in SSWL, S.C.O 49-50, Sector 26, Madhya Marg, Chandigarh-160019, India & plants including people, process and technology systems must be periodically audited for compliance with SSWL's Information Security policies, procedures and Guidelines based on ISO 27001:2022. Security audits/reviews shall be:

- Performed annually
- Performed on predefined schedules
- Performed by independent party (Independent party can be internal or external)
- Performed by trained and competent individuals
- Activities performed in security audit / review must include but not limited to:
- Security configurations and corresponding levels of risk.
- Checks to ensure that security safeguards are implemented as required and are being properly used.
- Process for reporting security audits results must be established. Non-Conformities must be reported using predefined format. All conformities must be documented to extend possible for future reference. Corrective and Preventive action procedures must be followed to close all reported Non-Conformities.
- Security audit / review reports must be shared with the senior management/security committee. Management Review Meeting shall be conducted after the Internal Audit to discuss and accept the findings of Internal Audit.

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

- All Information Security policies must be periodically reviewed for relevance and completeness based on security audit / review report.
- Auditors should not audit their own function.

4.2 Technical Compliance Checking

- Information assets must be checked regularly for compliance with technical implementation standards.
- Third party system vulnerability and penetration tests (VA / PT) must be conducted periodically.
- Technical compliance schedules for different information assets must be defined.
- Any deviations must be noted down in the audit report and appropriate action must be taken to address the same.
- Technical compliance testing must be performed by independent party.
- VA / PT must be performed by qualified individuals.

4.3 System Audit Controls

- Audits must be planned to minimize business disruption.
- Audit requirements and scope must be agreed with management.
- Software and data checks must be limited to read only data. Where access is required otherwise, copies must be made, and the copies deleted immediately after use.
- Technical resources to perform the checks must be identified and made available.
- Requirements for additional processing must be identified and agreed.
- Access to information resources and systems during an audit must be monitored and logged.
- All audit requirements and responsibilities must be defined/discussed.

4.4 Protection of Audit Tools(If required)

- System audit tools must be established and not be held in operational environments.
- Access to the system audit tools must be controlled.

5. Procedure Sections and Clauses

5.1 Internal Audit Procedure

- Internal Audits will be conducted for all departments under the scope of ISMS.
- An audit of the Information Security Management system function will be conducted by independent third-party internal auditors. The scope of Information Security Administrator audit would be to check compliance with the clauses 4 to 10 of the ISO 27K standard (as applicable) and the selected controls as per the SoA.

- Inputs
  - Previous Audit Reports
  - Audit Plan
  - Updated policies and procedures
  - List of Auditors

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

- Outputs
  - Internal Audit findings
  - Management Report
  - Corrective Action (if required)

5.2 Process

- The Internal Audit will be conducted by independent Information Security Auditor.
- The audit criteria and scope for the audit will be defined.
- The Audit will be carried out using according to the best practices of Information Security.
- The Audit will be done to check the compliance level compared to the documented objectives and requirements as per ISO 27001:2022 standards.
- The Audit will be carried out to check whether the security policies and procedures defined are being implemented properly.
- The Auditors will also check whether the controls selected are efficient enough.
- A formal audit report will be drafted listing down the observations/issues from the audit.
- The observations/findings need to be clearly categorized as Major/Minor NC or an observation. This would help the teams take actions as per urgency.
- This report shall enable the department owner to follow up with the concerned people and close or fill the gaps identified.
- In case of any Nonconformity Corrective Action procedure shall be followed.
- The Security team should monitor for corrective action.
- The Audit report should be presented to the ISMS team and appropriate timelines, and owner should be designated to close the findings.

6. Policy Compliance

6.1 Compliance Measurement

The ISMS team will verify compliance to this policy through various methods, including but not limited to, periodic Walkthrough, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

6.2 Exceptions

Any exception to the policy must be approved by the ISMS Team in advance.

6.3 Violations

Any violation or breach of this policy will result in disciplinary action, which may include termination of employment, legal action, or any other measures deemed suitable by the organization.

7. ISO 27001:2022 References

- A.5.35 Independent review of information security
- A.8.34 Protection of information system during audit testing
- A.9.2.2 Internal Audits a, b & c

Prepared By:	Approved By:
Dy. Manager - IT	General Manager - IT

** End of Document**

CONTROLLED COPY

Attention: The information is intended for the internal use of "Steel Strips Wheels Limited". By viewing this document, you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from "Steel Strips Wheels Limited". If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.