Steel Strips Wheels Limited

SUPPLIER RELATIONSHIP MANAGEMENT POLICY

Document Number: SSWL/IT/SRM/ 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/SRM 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. Scope

This document applies to all third-party service providers and suppliers who can influence confidentiality, integrity and availability of SSWL's sensitive information.

2. Purpose

The purpose of this document is to define the rules for relationship with third party service providers, suppliers and partners

3. Relationship with Suppliers and Partners

3.1 Identifying the Risks

- Security risks shall be identified during the risk assessment process. During the risk assessment, special care shall be taken to identify risks related to information and communication technology and product supply chain.
- The Information Securing Department decides whether it is necessary to additionally assess risks related to individual suppliers or service providers.

3.2 Addressing Security within Supplier Agreements

Supplier agreements shall be established and documented to ensure there is no misunderstanding regarding both parties' obligations to fulfill relevant security requirements.

Supplier agreements shall include clear and concise information regarding:

- The types of data being accessed and methods of access.
- The organization's data classification requirements as it applies to the supplier.
- Definition of acceptable uses for the data handled by the supplier.
- Processes and procedures for monitoring compliance with the contract requirements.
- A "right to audit" the supplier or regular access to external assessments.
- Conflict and defect resolution.
- Required screening, training or other obligations of the supplier's staff.
- The use of sub-contractors to provide services and the extension of security requirements to them.
- Data retention period clause shall be added.

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.

The risk in the procurement phase of the services of external parties shall be identified so that roles, responsibilities and expectations can be clearly defined in agreements or contracts.

Information and Communication Technology Supply Chain

- Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chains

- Points related to the use of technology, both hardware and software, shall be addressed in the agreement with suppliers. The SSWL shall trace origins and maintain compliance with security requirements for assuring both integrity and availability. The SSWL shall address the risks of a component or service becoming unavailable or no longer supported.

Monitoring and Review of Supplier Services

- SSWL shall regularly monitor, review and audit supplier service delivery.

- The service provider shall be continuously monitored to assure that services provided are meeting the terms of the contract and security is maintained.

- There shall be ongoing review of service reports, a process to address concerns and issues and periodic audits.

- Service capability levels shall be monitored to ensure that the service provider continues to meet the contract terms and needs of the business.

- In addition to regular review and monitoring of the services provided, the contracting organization shall:

    - Conduct audits of suppliers in conjunction with outside assessments if required.

    - Require the supplier to promptly notify regarding security incidents o Provide regular records for security events.

    - Have a conflict resolution process that can be invoked if requirements are not met.

3.3 Managing Changes to Supplier Services

Due to technology systems undergoing continuous upgrade, change and repair, changes to service provisions by suppliers shall be managed and documented, taking into account the sensitivity of information and services and re-assessment of risks.
Following parameters shall be considered in agreement with supplier or service provider to integrate change management process:

- Service enhancements
- Bug fixes
- Use of new technology

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.

- New development tools
- Enhanced security measures
- Change of sub-contractor
- Change of physical sites
- Business Continuity and Disaster Recovery

3.4 Information Exchange Agreements

- An agreement should be established for the exchange of information or software (Electronic or manual) with the organization before the exchange of information or software.

- The agreement should clearly specify ownership and responsibilities for data protection, software copyright compliance and similar considerations.

- The agreement should include the third-party management's responsibilities for controlling and notifying transmission, dispatch and receipt and any special controls that may be required to protect sensitive items.

- Standards should be defined for packaging and transmission of such information or software.

3.5 Non-Disclosure Agreements

- Each third-party employee, consultant, or contractor working directly for SSWL either on-site or off-site must sign a Non-Disclosure Agreement. This agreement must be completed prior to issuing an access card or network access and third-party access to any SSWL information.

- All non-disclosure agreements signed by contractors and third parties must be kept on file by the Respective Department.

- Following elements should be considered in non-disclosure agreements:

    - A definition of the information to be protected (e.g. confidential information).

    - Expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely.

    - Required actions when an agreement is terminated.

    - Responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know').

    - Ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information.

    - The permitted use of confidential information, and rights of the signatory to use Information.

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.

- Terms for information to be returned or destroyed at agreement cessation.
- Expected actions to be taken in case of a breach of this agreement.

4. Policy Compliance

4.1 Compliance Measurement

The InfoSec 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.

4.2 Exceptions

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

4.3 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.

5. ISO 27001:2022 References

- A.5.5 Contact with authorities
- A.5.6 Contact with special interests groups
- A.5.14 Information transfer
- A.5.19 Information security in supplier relationships
- A.5.20 Addressing information security within supplier agreements
- A.5.21 Managing information security in the information and communication technology (ICT) supply chain
- A.5.22 Monitoring, review, and change management of supplier services

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

STEEL STRIPS WHEELS LTD. Chandigarh

** 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.