Steel Strips Wheels Limited

ACCESS CONTROL POLICY

Document Number: SSWL/ IT/AC/ 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	Access Control Policy
Document Number	SSWL/IT/AC/ 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

Access to information assets is a privilege granted to all Steel Strips Wheel Ltd employees and stakeholders and is vital to performing their daily tasks. Therefore, proper access and authorization to Steel Strips Wheel Ltd information assets.

2. Scope

The policy applies to all platforms being used at Steel Strips Wheel Ltd including but not limited to operating systems, applications, software, middleware, databases, network device operating systems and tools. This policy's terms have retrospective application, that is, the obligations expressed within this policy also apply to assets existing prior to the publication date

3. Policy Statement

Access to Steel Strips Wheels Ltd information systems and computing resources shall be based on a specific business need (i.e. on "need to know" and "need-to-do" basis). Access Controls will ensure that even legitimate users cannot access information unless they are authorized to do so.

4. Business Requirements of Access Control

4.1 Access control policy

We limit access to information and information processing facilities in accordance with our Access Control Policy.

- IT Team will provide all employees and other users with the information they need in order to carry out their responsibilities in as effective and efficient manner as possible.
- Access to information, facility, functionality, asset, resources of Steel Strips Wheel Ltd will be limited to authorized persons whose job responsibilities require it, as determined by an appropriate approval process at Steel Strips Wheel Ltd, and to those authorized to have access to the same as per the laws.
- Access is given through the establishment of a unique account in accordance with account request.
- Users are expected to become familiar with and abide by Steel Strips Wheels Ltd policies and procedures for appropriate and acceptable usage of the networks, systems and other resources of Steel Strips Wheel Ltd. All users will have access to expectations, knowledge, and skills related to information security.

Access control policy should be periodically reviewed on the basis of business and security requirements.

4.2 Access to networks and network services

Users are only provided with access to the networks and services that they have been specifically authorized to use.

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.

4.3 User Access Management

Our user access arrangements ensure that only authorized users have access to systems and services.

- User registration and de-registration and user access provisioning
- Using unique user IDs to enable users to be linked to and held responsible for their actions
- The use of group IDs to only be permitted where they are necessary for business or operational reasons, and when permitted must be documented
- Checking that the user has authorization from the system owner for the use of the information system or service
- Checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy
- Requiring users to accept statements indicating that they understand the conditions of access
- Ensuring service providers do not provide access until authorization procedures have been completed
- Maintaining a formal record of all persons registered to use the service
- Promptly removing or blocking access rights of users who have changed roles or jobs or left the organization
- Periodically checking for, and removing or blocking, redundant user IDs and accounts
  Ensuring that redundant user IDs are not re-issued each system administrator manages access in accordance with this procedure.

This registration and de-registration procedure is periodically reviewed on the basis of business and security requirements.

4.4 Management of privileged access rights

A formal procedure for the allocation and use of privileged access rights is in place and each system administrator manages privileged access in accordance with this procedure.

- The access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should all be identified
- Privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy, i.e. the minimum requirement for their functional role only when needed
- Authorization process and a record of all privileges allocated should be maintained - privileges should not be granted until the authorization process is complete
- The development and use of programs / system routines which avoid the need to run with privileges should be promoted.
- Privileges should be assigned to a different user ID from that used for normal business use.

This management of privileged access rights procedure is periodically reviewed on the basis of business and security requirements.

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.

4.5 Management of secret authentication information of users

A formal procedure for allocation of secret authentication information (such as passwords) and each system administrator manages the allocation of secret authentication in accordance with this procedure.

Where passwords are employed, they are required to comply with our Password Policy.

- Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization - other technologies, for example biometrics or the use of hardware tokens, e.g. smart cards, may also be employed
- Users should be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group – it would be appropriate for this requirement to also be included in their terms and conditions of employment
- When users are required to maintain their own passwords, they should initially be provided with a secure temporary password, which they are forced to change immediately
- The identity of a user should be verified (by sending a secret code to the user's official email ID and asking him / her to confirm the secret code) prior to providing a new, replacement or temporary password
- Temporary passwords should be given to users in a secure manner (such as sending via SMS to his / her mobile phone - the use of third parties or unprotected (clear text) electronic mail messages is avoided
- Temporary passwords should be unique to an individual and should not be guessable.
- Users should be required to acknowledge receipt of passwords, by email or reply SMS
- Passwords must never be stored on computer systems in an unprotected form - they must always be masked / encrypted and stored
- Default vendor passwords should be promptly changed following installation of systems or software

4.6 Review of user access rights

Asset Owners review users' access rights at regular intervals (quarterly basis) and also after any changes of role, such as promotion, secondment or posting elsewhere within the organization.
Those empowered to grant special privileged access rights, review those rights at regular intervals (quarterly basis).

4.7 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

4.8 User Responsibilities

Users are required to follow our practices in the use of secret authentication information (such as passwords) and made formally accountable for safeguarding their authentication 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.

4.9 System and Application Access Control

We prevent unauthorized access to systems and applications.

4.10 Information access restriction

Access to information and application system functions are restricted in accordance with our access control policy. Where required by the access control policy, access to systems and applications are controlled by secure log management procedure.

4.11 Password management system

Please refer password protection policy

4.12 Use of privileged utility programs

The use of utility programs (such as anti-virus programs) that might be capable of overriding system and application controls is restricted and tightly controlled.

4.13 Access control to program source code

Steel Strips Wheels Ltd is not involve into the development activity.

4.14 Granting Administrative rights shall adhere to the following:

- Local Administrator Rights was given as per business need with department head approval.
- Comply with all existing policies of the Steel Strips Wheel Ltd IT Department.
- Do not apply changes to a desktop, laptop or other end user device that has not been assigned to the grantee.
- Do not install any unauthorized or non-standard software. Take all reasonable steps to ensure that the device with administrative rights is secured from malware or intrusion.
- Do not install any trial versions / freeware versions /malware which are in form of web, exe or full installations.
- In the event of failure of the device with administrative rights, the grantee will be responsible for restoring any applications, configurations and associated data beyond what has been approved as a standard base image.
- Ensure that the desktop is properly connected to Steel Strips Wheel Ltd network so that it receives schedule software patches and upgrades.
- Administrative rights can be terminated at any time

5. Policy Compliance

51. 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.

52. Exceptions

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

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.

53. 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.

6. ISO 27001:2022 References

- A.5.15 Access control
- A.5.16 Identity management
- A.5.17 Authentication information
- A.5.18 Access rights
- A.8.2 Privileged access rights
- A.8.3 Information access restriction
- A.8.4 Access to source code
- A.8.5 Secure authentication
- A.8.18 Use of privileged utility programs
- A.8.15 Logging
- A.8.19 Installation of software on operational systems

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.