PURPOSE:

To provide a frame work for managing and mitigating cyber security risks, to safeguard information from unauthorized access, protection of individual's personal information and to establish guideline and procedures for safeguarding an organization's / individual's data and system.

SCOPE:

This policy applies to all Wheels India Limited's employees , suppliers, vendors consultants and or individuals with access to Company's electronic system, information and/or hardware.

The cyber security policy is published to all people who are employees of the organization, suppliers, customers, shareholders and anyone who has temporary / permanent access to our systems

Company Policy:

a. Protection to IT devices of the company:

i. Protect company's IT devices using strong credentials

ii. Ensure upgrade of anti virus software from time to time

iii. Carry out physical inventory of all IT assets once in a year

iv. Maintain asset register, add , change , delete the assets wherever applicable

v. Allow only company assets to connect to company network

vi. Ensure company network access given to external people with due verification/ Approval and limited access to the extent of permitting internet only

vii. Enable dual authentication & alert when there is an attempt to access servers

b. Protection to Internal, vendor and customer data:

i. Protect all company data using right authorization to right people

ii. All data access using log in credentials

iii. Periodical data back up with specific schedules

iv. Upgrade patches to all applications

v. Run network scanning tool, identify and list the priorities

vi. Categorize the risks and remove / mitigate the risks

vii. Maintain back to back agreement with vendor for regular upgrade of software

viii. Enable dual authentication & alert when there is an attempt to access servers

c. Policy on data privacy

i. Establish roles and responsibilities. Extend only the required access to perform the activities

ii. Segregate the duties in three categories like Create, Change and display

iii. Enable create only to the document generator, Change to the person who approve with history and display to the rest who are going to consume the data

iv. Establish data retention and safe disposal using archiving tools