Southland Rubber
Think Good, Better Will Follow

Southland Rubber Information Security Policy 20220101

1) Purposes

a) This document sets internal management rules of documentary and information security of hardware and software in order to protect confidential information of Group Companies and personal data to respect the privacy of individuals.

b) A designated Director of each Group Company and/or the Head of a branch unit/factory shall be responsible for the collective implementation of and compliance with this Policy.

2) Premises Security

a) Employees must ensure that company items such as mobile phones and computers issued to them for official use are secure when not in use.

b) The doors of our factory, office or rooms are to be secured with locks, card or coded access controls to protect loss of assets or information whenever such places are not in use or closed for the day.

3) Information Security (documentary or digital)

a) Hard copies of confidential documents are to be kept under lock and key, when not in use and if an Employee is away from the workstation.

b) Faxed documents containing confidential information should not be recycled as scrap papers for re-use.

c) Equipment such as personal computers, notebooks, laptops, etc. and hard disks with confidential digital data should be protected with passwords.

d) Workstations used must be protected by password to prevent access when the user is away.

e) Whenever practical, electronic and electrical equipment must be switched off when leaving the office for the day.

4) Restrictions on Confidential Information

a) Every Employee undertakes that both during and after the term of employment with the Company, the Employee will not use, divulge or communicate to any person (other than those whose job duty is to know the same or with proper authority to do so) any of the trade secrets or other confidential information of the Company, including the particular lists or details of customers and clients of the Company.

5) IT Security, Policies and Practices

a) The term “computer resources” shall refer to all computers, IT infrastructure, and information, communication equipment, operating business systems and IT services.

b) The term “electronic information” refers to all information that is created, distributed, published, and stored using computer resources including information that has been stored on external devices such as floppy disks, thumb drives, CD-ROM media as well as printed paper via computer resources.

c) Prohibitions Relating to Emails:

i) Do not write down user ID and password or tell them to another person.

ii) Do not open suspicious scam and other viral emails or attachments, but delete them immediately.

iii) Do not send emails pretending to be someone else.

iv) Be sure of the right to
(1) Be able to email out third-party information;
(2) To solicit, promote or advertise product or service through email.

v) Do not send out any emails construed as harassment or disparagement of others.

vi) Do not send or open any emails containing information which is immoral, menacing or offensive, or relating to religious, communal or political propaganda, or with contents which are abusive, indecent, obscene, or pornographic.

vii) Do not forward or propagate chain emails.

d) Prohibitions Relating to **Internet/Intranet/Extranet**

i) Do not publish or link information on Company’s website without the approval of a Director or CEO.

ii) Do not access any websites unrelated to your work (e.g., games, pornography, blogs and etc.).

iii) Do not download, possess, exchange, make copies of, or distribute any copyrighted contents without the permission of the author as these actions violate copyright laws.

iv) Do not write any libellous comments about other people on any electronic message boards.

v) Do not give out any personal information including credit card numbers on the Internet unless the site is known to be safe and information to be encrypted (e.g. web URL format as “https://” - with an “s”).

vi) Do not transmit or retrieve information containing obscene, indecent, lewd, or lascivious material.

vii) Do not use company Internet access for personal financial gain and/or profits including online gambling, online betting and online trading of shares/stocks and bonds.

e) Procedures Relating to PCs **(Desktop or Laptop Computers, Notebook, etc.)**

i) Set up PCs with monitors that require passwords to access.

ii) Turn off PCs when leaving work.

iii) Check that updated versions of anti-virus software are installed.

iv) Run windows update to patch up windows operation system regularly.

v) Do not install any software or hardware that is not related to work.

vi) Take all precautions if a laptop or storage device is taken out of office to ensure that the device or information is not lost or stolen.

vii) If a device containing information is lost or stolen, the Employee has to notify the supervising Director or the CEO immediately.

viii) Ensure that files from PCs are automatically saved on company servers.

f) **Printers, Scanners, Fax and Photocopy machines**

i) Collect all documents without delay from printer, fax machine and photocopier.

ii) Avoid using company printers, scanners, fax machine and photocopy machine for non-work-related matters.

iii) Use only original or approved cartridges.

g) **Administration of Data and Information Security**

i) At each Group Company, an Administrator, who is either a Director or branch/unit Head, is designated to focus on information security.

ii) The responsibilities of the Administrator are:

(1) To ensure compliance with the relevant laws and regulations relating to protection of personal data;

(2) To oversee implementation of this Information Security Policy.

(3) To ensure compliance and issue warnings or take disciplinary actions in the event that non-compliant practices are found.

(4) To immediately inform a Director that devices or information go missing, being virus-infected, cyber-attacked or damaged.

(5) To manage user accounts, data access and transmission of sensitive and personal information through internal or external networks by password protection or encryption, e.g. SSL (Secure Socket Layer) and VPN (Virtual Private Network).

(6) To train and instruct Employees (and recruits) proper use and protection of information and information systems.

(7) To set procedures to ensure software licensing and protection of rights of intellectual property owners.

(8) To assist in internal audits relating to information security, as deemed necessary.

h) **Personal Data Protection**

i) Administrator shall set up systems to ensure personal data of individuals be collected, kept, accessed and used in a lawful, safe, careful and confidential manner in accordance with the laws and regulations of each location.

ii) A Group Company will request and transmit only legitimate personal data for the purpose of its management.

iii) A Government agency may be provided Personal Data required by law, for example, to satisfy needs for social security, revenue, labour protection, etc.

iv) Every disclosure of Personal Data will be recorded for audit.

v) The Personal Data retained by the company is considered as company's asset which must be protected.

vi) No one is allowed to breach, disclose, or access the Personal Data for personal exploitation or to destroy the personal data without the approval of a Director of a Group Company.

vii) Violation may be subject to the maximum punishment and/or be prosecuted under relevant laws.

viii) Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, bio-metric data is prohibited, without the explicit consent from the data subject, except for the case allowed by law.

ix) In the case of the collection of the Personal Data relating to criminal record, such collection shall be carried out under the control of a Director of the Group Company and as prescribed by local law.

x) The data subject is entitled to request access to and obtain copy of the Personal Data related to him or her, which is under the responsibility of the Director of the Group Company.

xi) Administrator shall maintain records in order to enable the data subject and the Group Company to check by either written or electronic form:
(1) The collected Personal Data;
(2) The use or disclosure under the right of the data subject;
(3) Explanation of the appropriate measures to protect the Personal Data.

xii) The data subject has the right to file a complaint for non-compliance with this Policy, regulations, and laws as prescribe in Southland Rubber Whistle-blower Policy.

xiii) Southland Rubber shall provide protection measures to the complainant in accordance with the Whistle-blower Policy.

xiv) Disciplinary actions:
(1) For any supplier, visitor, or other stakeholder who fails to comply with this Policy, relevant agreement, regulations and laws may face investigations and punishment imposed by law.

(2) For any Employee who discloses, breaches, or uses Personal Data for personal interests without the permission from the Group Company may be considered a serious misconduct and punishable in accordance with the Group Company Employees' Handbook.

Updated by the Management of Southland Rubber
1 January 2022