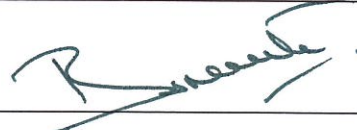


STATEMENT OF CONFIDENTIALITY

This document is confidential to Transpek Industry Ltd. This document contains information and data that Transpek Industry Ltd consider confidential and proprietary (“Confidential Information”).

Any disclosure of Confidential Information to, or use of it by any party, will be damaging to Transpek Industry Ltd. Ownership of all Confidential Information, no matter in what media it resides, remains with Transpek Industry Ltd.

Confidential Information in this document shall not be disclosed outside the organization and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this document without specific written permission of an authorized representative of Transpek Industry Ltd.

Prepared By : Praful Soni**Approved By: Shri Bimal Mehta**

1.0 Disclaimer

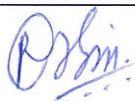
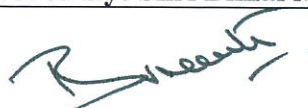
The Internet is a constantly growing worldwide network of computers and servers that contain millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users are further cautioned that it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Employees and users accessing the Internet do so at their own risk and understand and agree that Transpek Industry Ltd. (TIL) is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at TIL is governed by the following policy:

2.0 Permitted Use of Internet and Company computer network : The computer network is the property of TIL and is to be used for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain Users may also be provided with access to the Internet through the computer network. All Users have a responsibility to use TIL's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

3.0 Computer Network Use Limitations

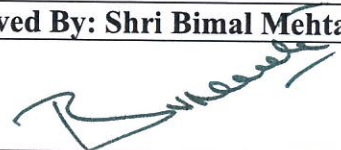
3.1 Prohibited Activities : Without prior written permission from TIL, TIL's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not : a) interfere with the User's or any other employee's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of the company. Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

3.2 Personal Email access : Users at TIL are not allowed to receive or transfer any email communication to their personal email access. Users are also not allowed to access their personal email portals like gmail.com, yahoo.com, rediffmail.com etc.

Prepared By : Praful Soni**Approved By: Shri Bimal Mehta**

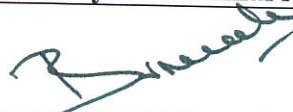
- 3.3 Illegal copying :** Users may not **illegally** copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.
- 3.4 Communication of trade secrets :** Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to TIL. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under government laws.
- 4.0 Duty not to Waste or Damage Computer Resources**
- 4.1 Accessing the Internet :** To ensure security, avoid the spread of viruses & malware, and to maintain TIL's Internet Usage Policies or Acceptable Use Policies, employees may only access the Internet through a computer attached to TIL's network and approved Internet firewall or other security device(s). Bypassing TIL's computer network security by accessing the Internet directly by personal connections such as (but not limited to) Cellular Networks, WiFi, modems, or proxy avoidance techniques or by any other means is strictly prohibited.
- 4.2 Inconsiderable use :** Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups or other social media, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.
- 4.3 Virus detection :** Users are not allowed to connect external storage device like Pen Drive, Hard Disk, Mobile etc. to TIL computer/network. In case user is allowed to use external device with approval from concern authority, he/she has to scan the material with company approved anti virus software. If you suspect that a virus has been introduced into TIL's network, notify TIL EDP personnel immediately.

Prepared By : Praful Soni

Approved By: Shri Bimal Mehta


- 4.4 No Expectation of Privacy :** Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using TIL's computer equipment. The computer network is the property of TIL and may be used only for Company purposes. Employees are not allowed to use company resources like computer, internet, printers, external storage media etc. for their personal use. TIL has rights to restrict use of removable media or printers to protect confidential data sharing.
- 4.5 Waiver of privacy rights :** User expressly waives any right of privacy in anything they create, store, post, send or receive using TIL's computer equipment or Internet access. User consents to allow company authorised personnel access to and review of all materials created, stored, sent or received by User through any Company network or Internet connection.
- 4.6 Monitoring of computer and Internet usage :** TIL has the right to monitor and log and archive any and all aspects of its Computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users via Email, IM & Chat & Social Networking.
- 4.7 Blocking Sites With Inappropriate Content :** TIL has the right to utilize hardware and software that makes it possible to identify and block access to any Internet sites including those containing sexually explicit or other material deemed inappropriate in the workplace. Access of those sites/material by any means may result in disciplinary action, including civil and/or criminal liability.
- 4.8. Blocking Sites With Non-productive Content :** TIL has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing non-work-related content such as (but not limited to) Drug Abuse; Hacking; Illegal or Unethical; Discrimination; Violence; Proxy Avoidance; Child Abuse; Alternative Beliefs; Adult Materials; Advocacy Organizations; Gambling; Extremist Groups; Nudity; Pornography; Tasteless; Weapons; Sexual Content; Sex Education; Lingerie and Swimsuit; Sports; Hunting; War Games; Online Gaming; Freeware and Software Downloads; File Sharing and Offsite Storage; Streaming Media; Peer-to-peer File Sharing; Internet Radio or TV; Internet Telephony; Online Shopping; Malicious Websites; Phishing; SPAM; Advertising; Brokerage and Trading; Web-Based Personal Email; Entertainment; Job Search; Medicine; News and Media; Social Networking; Political Organizations; Reference; Religion; Travel; Personal Vehicles; Dynamic Content; Folklore; Web Chat; Instant Messaging or IM; Newsgroups and Message Boards; Real Estate; Restaurant or Dining etc.

Prepared By : Praful Soni

Approved By: Shri Bimal Mehta


5.0 Password Policy :

Do not use the same password for TIL accounts as for other non-TIL access (e.g., personal e-mail, on-line banking, and social media).

Where possible, do not use the same password for various TIL access needs. For example, select one password for e-mail systems and a separate password for access to systems that store sensitive or confidential data.

Do not share TIL passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential TIL information.

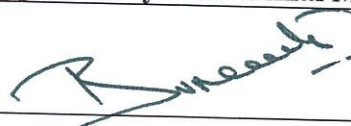
Please remember:

- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not reveal a password to the boss or subordinates.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- User must change their password at every 60 days.

If someone demands a password, refer them to this document or have them call someone the IT Department. Do not use the "Remember Password" feature (e.g. browsers, software applications).

Passwords must not be written down. Do not store passwords in a file on ANY computer system or hand held devices without encryption. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during one of these reviews, the user will be required to change it.

Prepared By : Praful Soni**Approved By: Shri Bimal Mehta**

6.0 IT Asset Accountability :

This policy is applicable to everyone who works for TIL, irrespective of type or duration of contract. TIL personnel are provided, the necessary tools and equipment to achieve their work objectives and the goals of the Organization. TIL personnel are expected to take all reasonable precautions to protect this property, as if it were their own.

TIL personnel must exercise due diligence and care to protect from loss, theft and damage the organization's property and assets, including Computer, Laptop, Data Card, Mobile etc. These assets, while belonging to TIL, must be safeguarded in the same manner that people would ordinarily use to protect their own personal property.

TIL personnel who are entrusted with property or equipment belonging to the Organization must take the necessary safeguards to protect this property from loss, theft or damage. Those who fail to do so will be held financially responsible for lost or damaged property and will be required to reimburse the Organization.

A loss, theft or damage to the Organization's assets may be the result of accidental loss or damage, or unavoidable theft or robbery. Alternatively, it may be due to circumstances within a person's control, such as simple negligence, gross negligence or willful misconduct on the part of individuals or groups of individuals.

Simple negligence is a failure to act as a reasonably prudent person would have acted under the same or similar circumstances.

Gross negligence is a failure to exercise even a slight degree of care, or an extreme departure from the course of action expected of a reasonable person, all circumstances considered.

Willful misconduct is an intentional or deliberate violation of rules or policies, including fraud and dishonesty.

Prepared By : Praful Soni	Approved By: Shri Bimal Mehta
	