INFORMATION TECHNOLOGY POLICY

OF

KABRA EXTRUSIONTECHNIK LIMITED

(KET)

April, 2024

1. Introduction

This Information Technology Policy outlines KET's approach to ensuring the security of its information systems and data. The Company is committed to safeguarding its information assets and IT resources to support its operations by implementing proper security measures to prevent data breaches and disruptions.

The policy aims to secure and ensure the appropriate use of Company's IT infrastructure providing a trusted and secure computing environment while protecting the Company's assets, data, members information and intellectual property.

2. Definitions

- **Information Systems :** All hardware, software and network resources used to process, store and transmit data.
- **Data :** Any information processed, stored, or transmitted within the KET's information systems.
- **Cyber Threat :** Any potential malicious attack that seeks to unlawfully access, damage or disrupt information systems and data.
- **VPN :** Virtual Private Network used for secure remote access to the company's network.
- **Electronic Communication :** Electronic communication include but not limited to written correspondence, such as letters and emails, documents and database, plans and drawings, photographs, images, video recordings, voice mails, electronic messages, social media interactions and internet browsing.
- **Devices :** Devices that access, store or transmit company data, including but not limited to laptops, desktops, mobile phones, tablets and removable storage media.

3. Applicability

This policy applies to all employees, contractors, consultants and third parties with access to KET's information systems and data.

4. General Restriction

Any device provided by the Company, including personal devices used for communication involving Company information or data during employment or association with the Company, will be considered as a Company's asset.

All communications made through such devices, whether during office hours, on holidays, or otherwise, will be deemed as made for official purposes.

The Company retains the right to access, copy, share, transfer, remove, and delete all information and data on devices used by Members for official purposes. This includes personal data such as photos and files stored on these devices, for which individuals waive their right to privacy.

5. Responsibility of Users

- Users should read, understand and adhere to Company's cybersecurity guidelines and polices.
- For obtaining Company assets, users must initiate requests through the PR / CAPEX clearly specifying the intended usage. The same needs to be approved by respective manager, department or higher authority.
- Users should ensure that they familiarize themselves with security protocols relevant to their designated computer systems and ensure to take all reasonable precautions to prevent unauthorized access and breaches.
- Users should use available mechanism and procedures to protect their own data and data under their control.
- Users should report any security incidents or concerns to the designated contact person.
- On separation from employment or association with KET, users must ensure that any assets registered to them but currently in use by another associate have their ownership transferred. This transfer request must be initiated with HR department and approved by the Head of the respective department.

6. Policy on Electronic Communication

- Users shall be provided with an official email address with the permission to send and receive both internal and external mail.
- Users shall use the internet, intranet and other email facilities for business purposes except certain circumstances as exempted.
- The Company reserves the right to monitor, inspect and disclose the emails or data of any user when necessary for business interests, legal requirements or suspected violations of any policies and regulations.
- Any users fail to observe appropriate use may be regarded as engaging in misconduct and will be subject to disciplinary procedure in accordance with the Company's policy.

Inappropriate use

- Sending internal, confidential or proprietary communication without proper authorization.
- Personal use that interferes with Company resources or causes inconvenience to recipients.
- Sending emails or messages outside specified guidelines.
- Revealing passwords to unauthorized persons.
- Sending or viewing offensive, discriminatory, inflammatory or defamatory message about individual, group, organization, race, gender, religion, attributes or sexual preferences using official email or Company resources.
- Sending or viewing messages containing obscene, indecent or pornographic material.
- Downloading, transferring or copying data from official email or drive.

The Company reserves the right to take any preventive action, impose fines or withdraw the use of electronic devices in cases of inappropriate use.

7. Remote Access ("VPN") Policy

- Users are permitted to utilize VPN connections to access the Company's computer network from external locations.
- Users with VPN access privileges are accountable for ensuring that their VPN connection is not accessed by unauthorized individuals to enter the Company's information systems. They must recognize that VPN connections extend the Company's computer network and pose potential risks to Company information. Therefore, users must diligently safeguard Company assets.
- VPN account activity will be monitored regularly.

8. Protection of Information

- **Virus Protection**

All Company provided computer systems shall have the designated security software installed to defend against the virus and other harmful programs. All software installation shall be authorized by IT department.

To protect the internal network from external threats and unauthorized access, a firewall is installed at the Head Office and all internet connected data centers.

Any Computer systems without the latest updated antivirus software installed are not permitted to connect with the Company's network. And any virus attacks must be reported to the system administrator.

- **Securing Data on Devices**

To use the work group passwords under authorization of IT department and avoid sharing passwords and recommended to change them periodically.

Encrypt sensitive data both at rest and in transit using approved encryption methods and ensure encryption is enabled for devices and storage media containing sensitive information.

To update operating systems, applications and antivirus software periodically to protect against any exploits.

To be cautions of suspicious link, emails and downloads. Avoid connecting to unsecured or public wi-fi networks without using a VPN.

To ensure that the desktop / laptops assigned is shut down and re-started at least once every week.

9. Compliance Measures

- The Company will undertake all necessary measures to ensure the compliance with the Information Technology Act, 2000.
- The Company will refrain from the deployment, installation, or modification of technical configurations of any Computer Resource that would circumvent existing

laws or regulations, except when necessary for securing Computer Resources and protecting the information contained therein.

- Regular monitoring and review of technical configurations will be conducted to ensure ongoing compliance with the IT Act, 2000, and other applicable laws.

10. Amendment

- This Policy can be amended by the Company at its discretion. The company may notify any draft amendments to the policy on the Company intranet inviting comments and suggestions. The Company may after considering the comments and suggestions may make suitable further amendments. Such further amendments, if any, shall come into force immediately with effect from the date of such notification of the amendment.

***