Cyber Security and Data Privacy Policy

1. Objectives

Kewal Kiran Clothing Limited (KKCL) acknowledges the importance of safeguarding information in all its forms and recognizes the vital role played by information technology in the company's operations. In light of the increased digital usage and sharing of information among authorized users of KKCL's IT resources, there is a greater need to enhance information and technology resource protection efforts. To address this, KKCL has formulated a Policy that encompasses privacy guidelines and usage regulations for the company's Information Technology Resources.

Our company's cyber security policy outlines the guidelines and provisions for ensuring the security of our data and technology infrastructure. As we increasingly rely on technology for data collection, storage, and management, our vulnerability to significant security breaches grows. Human errors, hacker attacks, and system failures have the potential to compromise our company's reputation and cause substantial financial damage. Therefore, we have implemented various security measures and prepared instructions to mitigate security threats.

The objective of this policy is to ensure that all users utilize KKCL's Information and Information Systems in a lawful, ethical, and professional manner to further the interests of KKCL.

2. Scope and Applicability

This policy is applicable to all individuals who have access to KKCL's Information Technology Resources within India. It is the responsibility of the Factory Managers at respective factories and the IT Head at the corporate office to ensure that this policy is effectively communicated, understood, and followed by all users.

Furthermore, this policy extends to all contracted staff, vendors, and suppliers who provide services to KKCL and come into contact with KKCL's Information Technology resources. The HR/Admin department, along with the respective Factory Managers responsible for contracting these services, are accountable for providing a copy of this policy to the contractors, vendors, and suppliers before granting them access.

This policy encompasses the usage of all company-owned or leased information technology and communication resources under the possession, custody, or control of the company. This includes, but is not limited to:

a. Computer-related equipment such as desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecom equipment, networks,

databases, printers, servers, and shared computers, as well as the networks and hardware connected to this equipment.

b. Electronic communications equipment, including telephones, pagers, radio communicators, voicemail, email, fax machines, PDAs, wired or wireless communication devices and services, internet and intranet services, and other online services.

c. Software, including purchased or licensed business software applications, KKCL-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on KKCL-owned equipment.

d. Intellectual property and other data stored on KKCL's Information Technology equipment.

e. These policies also apply to all users, regardless of whether they are on company property or accessing the resources remotely through any networked connection or using company equipment.

f. Additionally, the usage of KKCL website (https://kewalkiran.com/) is governed by these policies.

Definitions

Information Technology Resources: Information Technology Resources for purposes of this Policy include, but are not limited to, KKCL owned or those used under license or contract or those devices not owned by KKCL but intentionally connected to KKCL - owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

User: Anyone who has access to KKCL's Information Technology Resources, including but not limited to, all employees, temporary employees, probationers, contractors, vendors and suppliers.

Sensitive Personal Data: Sensitive Personal Data of a person, under the Indian Information Technology Rules 2011, means such Personal Data which consists of information relating to:

i. Password
ii. Financial Information such as bank account or credit card or debit card or other payment instrument details
iii. Physical, physiological and mental health condition
iv. Medical records and history
v. Biometric Information
vi. Sexual orientation
vii. Any other details relating to the above mentioned, provided by any person to KKCL for providing services

3. Policy

Cyber Security

Preserving the confidentiality of sensitive data is of utmost importance to KKCL. This includes unpublished financial information, data of customers/partners/vendors, patents, formulas, new technologies, and customer lists (existing and prospective). To prevent security breaches, this policy serves as a guideline for our employees.

Protection of Personal and Company Devices

Using personal devices to access company accounts or emails introduces security risks to our data. We advise employees to secure both their personal computers, tablets, mobile phones, and company-provided devices by:

- Setting passwords for all devices
- Employing comprehensive antivirus programs and keeping them up to date
- Avoiding leaving devices unattended or exposed
- Installing browser and system security updates regularly
- Using private, secure networks to access company accounts and systems Furthermore, employees should not borrow devices from others or access internal systems and accounts using them.

Ensuring Email Safety

Emails can harbor malicious software and scams. To avoid falling victim to scams and virus infections, employees should:

- Exercise caution when opening attachments or clicking on links with insufficient explanation
- Be skeptical of clickbait titles
- Verify the legitimacy of messages by checking email addresses and recipient names
- Look for inconsistencies or signs of phishing attempts If an employee is uncertain about the safety of an email, they should consult the IT Head or IT Team.

Password Management

Password leaks pose significant risks to our infrastructure. Employees should:

- Use strong passwords with a minimum of eight characters, including uppercase and lowercase letters, numbers, and symbols, avoiding easily guessable information
- Memorize passwords instead of writing them down. If written, the document should be kept confidential and destroyed after use
- Only share credentials when absolutely necessary, preferably in person or through recognized phone calls
- Change passwords every two months

Secure Data Transfer

Data transfer presents security risks. Employees must:

- Minimize transferring sensitive data to other devices or accounts unless absolutely necessary. In such cases, employees should seek assistance from the IT helpdesk
- Utilize the company network or system to share confidential information rather than private connections or public Wi-Fi
- Ensure that recipients have appropriate authorization and adhere to adequate security policies
- Report scams, privacy breaches, and hacking attempts to the IT team. Prompt reporting enables the IT team to safeguard our infrastructure through immediate investigations and issuing company-wide alerts.

Additional Precautions

Employees should take the following precautions to minimize the likelihood of security breaches:

- Lock screens and secure devices when leaving desks
- Immediately notify the HR or IT department of any lost or damaged equipment
- Change all account passwords in the event of device theft
- Report potential security flaws or perceived threats
- Avoid installing suspicious, illegal, or unauthorized software on company equipment
- Refrain from visiting suspicious websites
- Comply with the Information Technology Policy

Responsibilities of the IT Team

The IT team is responsible for:

- Installing firewalls, anti-malware software, and access authentication systems
- Providing security training to all employees
- Regularly informing employees about new scam emails or viruses and methods to combat them
- Conducting thorough investigations of security breaches
- Following the provisions outlined in this policy, as other employees do
- Ensuring the company has physical and digital safeguards to protect information

Remote Employees

Remote employees must adhere to the instructions outlined in this policy. They are required to comply with all data encryption, protection standards, and settings as they access company accounts and systems from remote locations. Additionally, they must ensure the security of their private networks.

Taking Security Seriously

To instill confidence and trust in the security of stakeholders' data, we must actively safeguard our databases and systems. This can be achieved by maintaining vigilance and prioritizing cyber security at all times.

Privacy Policy

KKCL recognizes the potential risks associated with failing to protect personal data and comply with data privacy regulations. In addition to financial penalties, such breaches can lead to operational inefficiencies, regulatory intervention, and a permanent loss of consumer trust. This Privacy Policy applies to all data collected, received, possessed, owned, controlled, stored, dealt with, or handled by KKCL in relation to stakeholders.

Information Collection

To provide efficient service to stakeholders, we may collect necessary sensitive information from various sources, including:

- Our website: Information entered on our website, accessed resources, and completed transactions
- Subscriptions: Information provided by stakeholders to receive newsletters or updates
- Correspondence: Any communication received from stakeholders, including marketing representatives, procurement personnel, associates, employees, consultants, sales affiliates, distributors, agents, etc.
- Vendor or Supplier data collected during commercial transactions
- Other sources: Information obtained from unrelated sources such as public information from social networks and market research. Additionally, the Internet protocol (IP) address, browser type and version, time zone settings, browser plug-in types and versions, operating system and platform, and anonymous data collected by the hosting server for statistical purposes may also be stored.

Data Storage

All collected data is securely stored in our databases or the databases of our service providers, protected by reasonable organizational, technical, and security measures. Data is encrypted in accordance with our security policy to facilitate safe transfers when necessary.

Data Usage and Disclosure

We use collected data in a legal, fair, and transparent manner to serve our legitimate business interests. The data may be used for purposes such as marketing, internal administration, managing relationships with prospects and customers, demographic characterizations, internal

marketing surveys, facilitating contract performance, generating data analytics, and any other specified purpose at the time of collection. KKCL reserves the right to transmit data to other interested parties in various situations, including with consent, to provide products or services, to businesses acting on behalf of KKCL, in response to court orders or legal processes, to protect and defend rights or property, or to enforce terms and conditions.

Policy for Website usage

Confidentiality of personal information shared on our website is assured. Such information is used solely for the intended business purposes. By visiting our website, visitors implicitly consent to KKCL Limited storing and utilizing the provided information.

KKCL reserves the right to collect, analyze, and share aggregated site usage patterns of all visitors to improve services. This includes sharing information within KKCL and with business associates as a standard business practice.

During the course of business, KKCL may conduct online contests and surveys in accordance with the law. Information collected in these activities may be used and shared to enhance services to visitors.

Cookies may be used on KKCL's website to personalize visitor experiences or support promotional activities. Cookies improve website performance by personalizing experiences or facilitating convenience during visits. Accepting a "cookie" from KKCL Limited's website does not compromise privacy or security. Visitors who do not wish to receive cookies can adjust their browser preferences accordingly.

4. Disciplinary Actions

KKCL may consider any violation of this policy to be misconduct. Any infractions of this code of conduct will result in disciplinary action. These actions will vary based on the nature of the violation. All of the below mentioned disciplinary measures are up to management discretion and may not be taken in the order listed. Concerning the appropriateness of the disciplinary action for the violation, Human Resources shall be consulted.

Individual or collective violations of this policy may result in disciplinary measures such as the following, but are not limited to:

- Counselling;
- A warning in writing or verbally;
- Complete or partial removal of system privileges and access; and
- Any combination of the preceding.

Disciplinary measures may include, but are not limited to, the following in the event of a serious or persistent violation of this policy:

- Demotion
- Termination or Suspension
- Loss of benefits for a specific period of time or indefinitely

- Any combination of the above
- Taking legal action

5. Cyber Security and Data Privacy Governance

Cyber Security and Data Privacy Governance Structure consists of the IT Head, Site IT Head and System Admins.

IT Head shall also be part of the overall Cyber Security and Data Privacy Governance Structure.

These personnel are responsible for development, implementation, operation, maintenance and continual improvement of Cyber Security and Data Privacy at KKCL.

6. Raise your concern

Grievance Officer

In accordance with the Information Technology Act, 2000 and the rules framed thereunder, the name and contact details of the Grievance Officer are provided below:

IT Head,

Kewal Kiran Clothing Limited (HO)

460/7, I.B. Patel Road, Kewal Kiran Estate, Goregaon, Mumbai, Maharashtra 400063

9AM - 5PM (on all working days)

Please get in touch with a member of KKCL's IT team if you have any inquiries regarding this policy.

Please get in touch with KKCL's Compliance team at abhijit.warange@kewalkiran.com if you think someone may have violated this policy.

Retaliation, reprosal, or subsequent discrimination against anyone who raises a concern or reports possible misconduct is strictly prohibited at KKCL.

In accordance with its internal procedures for investigations, KKCL will conduct an investigation into alleged misconduct relating to this Policy. Any KKCL employees who violated this policy may face disciplinary action, including termination from their employment.