Computers, Networks, Mobile and Other Electronic Devices

As part of your role with KSH, you may be given a KSH computer, smartphone or other device to use for work. These devices belong to KSH and must only be used for KSH business and in accordance with KSH's policies regarding information security and mobile device use. Laptops and mobile devices may also contain personal and/or business confidential information. Using these devices or accessing KSH systems in order to view, create, or send inappropriate information or materials is strictly prohibited Any personal use of KSH devices and systems must always comply with all of KSH's policies relating to IT security and device usage. KSH has the right to monitor device usage, and if necessary, remove any and all data from KSH devices, which may include any personal documents, photos, and other information stored on them. If you are unsure if a particular use of KSH assets is acceptable, please speak to a member of the IT.

1. Create a strong and memorable password for important user Accounts

Such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

2. Use a separate password for your work account

If an online account gets compromised, you don't want the attacker to also know your work password.

3. Cyber attacks

Cyber attacks can be random to spot so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

4. Report attacks

Don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link). Always report what's happened.

5. Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by typing ERP and SIS email E-Approval something sensitive to the wrong addresses

6. Don't ignore software updates

They contain patch updates that keep your computer and laptop secure. Your organization may manage updates, but if you're prompted to install any, make sure you do.

CONFIDENTIAL INFORMATION CONSENT POLICY

1. Introduction

KSH Automotive Pvt Ltd is committed to protecting the confidentiality and privacy of stakeholders' information. This policy outlines the procedures for obtaining consent regarding the collection, handling, sharing, and storage of confidential information related to individuals and businesses.

2. Purpose

The purpose of this policy is to ensure compliance with applicable data protection laws and ethical standards while safeguarding sensitive information from unauthorized access or misuse.

3. Scope

This policy applies to all stakeholders, including employees, clients, business partners, vendors, and any third parties who share confidential information with KSH Automotive Pvt Ltd.

4. Obtaining Consent

- Stakeholders must be informed of the purpose, scope, and intended use of their confidential information before collection.
- Consent must be obtained through written agreements, online consent forms, or recorded verbal consent where applicable.
- Stakeholders will have the opportunity to review and agree to the terms before data processing begins.

5. Handling and Sharing Confidential Information

- Confidential information will only be used for the stated purpose agreed upon at the time of consent.
- Information will not be shared with third parties without explicit consent unless required by law or necessary for contractual obligations.
- All third-party recipients of confidential information must adhere to data protection agreements.

6. Data Storage and Security Measures

- Confidential information will be stored securely using encryption, password protection, and restricted access controls.
- Only authorized personnel with a legitimate need will have access to stored information.
- Regular security audits will be conducted to ensure compliance with data protection policies.

7. Withdrawal of Consent

- Stakeholders have the right to withdraw their consent at any time by submitting a written request to KSH Automotive Pvt Ltd.

- Upon withdrawal, KSH Automotive Pvt Ltd will cease processing and delete the information unless legally required to retain it.

8. Data Access and Management Rights

- Stakeholders may request access, correction, or deletion of their personal data by contacting [Data Protection Officer/Designated Contact].
- Requests will be processed in accordance with applicable laws and within a reasonable timeframe.

9. Compliance and Review

- This policy will be reviewed periodically to ensure alignment with legal and regulatory changes.
- Non-compliance with this policy may result in disciplinary action or legal consequences.

For KSH Automotive Pvt. Ltd.

Mr. Yongsung Kim
Managing Director