Information Security Policy

Purpose

The goal of this Policy is to establish a framework for all employees to understand their legal and ethical obligations regarding information, as well as to permit them to gather, utilise, keep, and disseminate data in responsible ways.

This Policy provides relevant and defining information about the objectives and functions of K2 Bitumen Sdn. Bhd. (K2B)'s Information Security Program, which is implemented to minimise malicious or unintended risks to the confidentiality, integrity, and availability of IT assets such as people, facilities, equipment, and information in all forms. It applies equally to client assets under K2B's control.

Objective

The objective is to create a framework for creating appropriate levels of information security for all K2B's information systems, which include, but are not limited to, all computers, storage (physical and cloud-based), mobile devices, networking equipment, software, and data.

K2B's goal is to reduce the risks associated with the theft, loss, misuse, damage, or abuse of these systems, as well as to ensure that users are aware of and comply with the relevant legislation and requirements of interested parties on information security, in order to protect the Company from liability or damage caused by the misuse of IT facilities and information technology.

Principles of Information Security

K2B adheres to the following information security and management standards.

1. Information is classified according to the level of secrecy, integrity, and availability that is suitable.

2. Employees must handle information in accordance with its classification level, as well as follow any contractual obligations, rules, processes, or systems in place to satisfy those duties.

4. Information should be both safe and accessible to people who have a valid need for access based on its categorization level.

5. Information shall be safeguarded against unauthorised access and processing based on its categorization level.

6. Policy violations must be reported. Employees and counterparts of K2B who fail to comply with Information Security Policies and Standards may face disciplinary action.

Information Classification

The table below summarizes the information classification levels that K2B has implemented.

1. Confidential Information

- Very essential and highly sensitive information that is generally available exclusively to certain members of K2B's team.

- Personnel information, key financial information, proprietary information of product and manufacturing designs, system access passwords, and information file encryption keys are examples.

- Unauthorized disclosure of this information to people without the need for access may violate laws and regulations, or may cause substantial problems for K2B, our customers, or our business partners.

2. Internal Information

- Intended for unlimited usage inside K2B and, in some situations, within related organizations such as sister companies or approved sub-contractors.

- Examples are personnel directories, internal policies and procedures, and internal electronic mail and communications.

- Unauthorized release of this information to outsiders is absolutely prohibited and may result in prosecution by K2B or any other authority.

- This information may be transmitted **within** the organization without prior authorization from the information owner.

3. Public Information

- Information specifically approved for public release by K2B's designated authority, such as marketing brochures and material posted to K2B's internet web pages or other approved means of publication, company policy and procedures (as applicable to the subject matter).

4. Policy Understanding, Compliance, and Disciplinary Action

All employees, contractors, and suppliers shall receive information security training using a variety of media to notify them of the presence of this policy and the availability of supporting policies, codes of practise, and guidelines.

Any security breach of K2B's information systems that results in the potential loss of confidentiality, integrity, and availability of personal or other private data held on these information systems will be dealt with appropriate disciplinary measures and processes.

Mohamed Nasser Bin Ahmad
Managing Director
05/05/2025
Rev. No. : 01