CYBER SECURITY POLICY

OF

STOVE KRAFT LIMITED

STOVEKRAFT®

Table of Contents:

Objective:

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

General Guidelines

1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.
2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.
3. Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security.

Scope and Applicability

This policy is applicable to all employees, staff members, vendors, interns, allies, customers, and business partners who may access confidential information that has been gathered or handled or who provide information to the organization.

All employees of Stove Kraft are expected to support the privacy policy and principles when they collect and / or handle personal information or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization’s commitment towards data privacy.

All partner firms and any Third-Party working with or for Stove Kraft, and who have or may have access to personal information, will be expected to have read, understand, and comply with this policy. No Third Party may access personal information held by the organization.

Responsibilities

The owner for the Data Privacy Policy shall be the Data Privacy Officer i.e., Chief Financial Officer. The Data Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the Data Privacy Officer.

This policy shall be reviewed for updates by Data Privacy Officer on periodical basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization’s operating environment or on recommendations provided by internal/ external auditors.

Data Classification

1. The organization classifies data into three categories:

a. High Risk:

It includes information which have legal requirements for non-disclosure and financial penalties imposed for disclosure.

E.g. Payroll, personnel, financial, biometric data

b. Medium Risk:

It includes confidential data which would not impose losses on the organization if disclosed but is also not publicly available.

E.g. Agreement documents, unpublished reports, etc.

c. Low Risk:

It includes information that can be freely disseminated.

E.g. brochures, published reports, other printed material etc.

2. Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.

3. High risk data must be encrypted when transmitted over insecure channels.

4- All data must be backed up on a regular basis as per the rules defined by the IT Dept. at that time.

Access Control

Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication. Authentication includes the use of passwords, biometrics or other recognized forms of authentication.

All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.

Default passwords on all systems must be changed after installation,

Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

Virus Prevention

Virus prevention for personal computers and email usage has been described previously.

Apart from that, all servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up to date.

Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

Intrusion Detection

1. Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.

Operating system and application software logging process must be enabled on all systems. Server, firewall and critical system logs must be reviewed frequently.

Conclusion

This cyber security policy is designed to protect the company's information technology systems and data from cyber threats. All employees are expected to follow this policy and report any suspicious activity to the IT department immediately. The company will review and update this policy regularly to ensure that it remains effective in protecting the company's data and systems.

The Board had adopted this Policy at its meeting held on 29th March 2023.