CYBER SECURITY POLICY

A. OBJECTIVE

The higher the degree of our reliance on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions in addition to causing great financial damage may also jeopardize company's reputation.

In this background, our cyber security policy outlines the guidelines and provisions for preserving the security of its data and technology infrastructure.

B. SCOPE

This policy applies to all our employees, vendors, customers, other third parties and anyone who has permanent or temporary access to Company's systems and hardware.

Policy Elements

Confidential data

Any confidential data is secret and valuable. Common examples include:

- Data of customers/partners/vendors
- Customer lists (existing and prospective)
- Patents, formulas or new technologies
- Unpublished financial information

All employees are obliged to protect this data. Some of the safeguards to avoid security breaches include-

Protecting personal and company devices

Use of digital devices (company-issued computer, tablets and cell phones etc.,) to access company emails or accounts introduces security risk to Company's data. Ensuring the security of digital devices is of paramount importance. Some of the measures that can be practiced include:

- Keeping all devices password protected
- Ensuring that the devices are not left exposed or unattended
- Logging into company accounts and systems through secure and private networks only.
- Installing and upgrading a corporate antivirus software
- Installing security updates of browsers and systems periodically

Kesoram Industries Limited
Cement Division
Unit : Vasavadatta Cement Works : Post. Sedam - 585 222.
Tq. Sedam, Dist. Kalaburagi, Karnataka
P + 08441 - 276005 / 276391
Corporate Office :
E : corporate@kesoram.net
Registered Office : Birla Building, 8th Floor, 9/1, R.N. Mukherjee Road, Kolkata-700 001,
CIN - L17119WB1919PLC003429

Employees are advised to strictly avoid accessing internal systems and accounts from others' devices and lending their own devices to others.

Keeping emails safe

Emails often carry and host scams and malware. To avoid virus infection or data theft, employees are instructed to:

- Check email and senders' names to ensure they appear legitimate
- Avoid opening attachments and clicking on links when the content cannot be understood from the face of it (e.g. "watch this video, it's amazing." and the likes)
- To remain vigilant and suspicious of clickbait titles (e.g. offering prizes, advice etc.,)
- Look for inconsistencies or give-aways (e.g. grammatical mistakes, Use of all capital letters, use of excessive number of exclamation marks)

If not sure and in case of doubt, as to whether an email received is safe, employees are advised to refer to Company's IT Support.

Manage passwords properly

Password leaks are dangerous as they can potentially compromise the entire IT infrastructure of the Company. Passwords should be strong so that they cannot be easily hacked and secrecy of the passwords should be maintained at all times. In this regard, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid passwords that can be easily guessed (e.g. birth dates of self and family, anniversary date etc.,)
- Change their passwords every month
- Remember passwords and avoid writing them down
- Exchange credentials only when absolutely necessary. Even then if in-person exchange is not possible, exchange over phone should be preferred instead of email and only after recognising the identity of the person they are talking to.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary
- Ensure that confidential data is only shared over the company's network/ systems and not over public network/Wi-Fi connection
- Use Microsoft Sharepoint/Onedrive for transfer of bulk data
- Limit use of external storage drives, only company's authorised device must be used
- Ensure that the addressees of the data are properly authorized people or organizations and have adequate security policies
- Report scams, privacy breaches and hacking attempts

IT Department needs to have information about scams, breaches and malware so that they can better protect the Company's IT infrastructure. For this reason, all employees are advised to report perceived attacks, suspicious emails or phishing attempts as soon as possible. IT department on its part must investigate promptly, resolve the issue and send a companywide alert as necessary.

IT teams are knowledgeable and responsible for advising employees on how to detect scam emails. Employees are encouraged to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks
- Report a perceived threat or possible security weakness in company systems
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment
- Avoid accessing suspicious websites
- Report stolen or damaged equipment as soon as possible to HR/ IT Department
- Change all account passwords at once when a device is stolen

We also expect our employees to comply with our internet usage policy-

IT support/team should:

- Arrange for security training to all employees
- Inform employees regularly about new scam emails or viruses and ways to combat them
- Install firewalls, anti-malware software and access authentication systems
- Investigate security breaches thoroughly
- Strictly follow these policies and provisions as other employees do

Remote employees

Remote employees must also follow these policies and instructions. Since they will be accessing the company's accounts and systems remotely, they are obliged to follow all data encryption, protection standards and settings and ensure their private network is secure. Remote employees are encouraged to seek advice from IT Department.

Abhay Dadhich
Chief Operating Officer