CANTABIL RETAIL INDIA LIMITED
CYBER SECURITY POLICY

Policy's brief & objective

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage, Workhours damage and may jeopardize our company's reputation.

For this reason, we have implemented several security measures. We have also prepared. instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, who have permanent access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors/sales

All employees are required to protect this data. In this policy, we will give our employees instructions. On how to avoid security breaches.

Protect personal and company devices.

When employees use their digital devices to access company emails or software, they introduce. security risk to company's data. We advise our employees to keep both their personal and company issued. Computer, tablet, and cell phone secure.

They can do this if they:

- Always keep all their devices password protected. Never share their respective passwords with ANYONE. Keep changing their password on frequent time intervals. The policy is in force to update their password in 45 days. If in case, they fail to do so. They are not even allowed to access the company's vulnerable data.
- Keep their Antivirus software updated with new definition. We at the backend make sure all the devices are updated & Install antivirus security updates as soon as updates are available.
- Never leave their device unattended & exposed to anyone unknow.
- Access to any device is not allowed without company accounts.Log in systems through secure and company's private networks only.

- All the ports available in the device are blocked. We don't allow employees to use any unauthorized media.

Keep emails safe.

Emails often host scams and malicious software to avoid virus infection or data theft,

we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Check email and names of people they received a message from to ensure they are legitimate.
- However strong SPAM FILTER is also deployed. Which itself chunk out the spam mails.
- If an employee isn't sure that theemail, they received is safe, they can refer to our IT Department.

Manage passwords properly.

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret.

For this reason, we advise our employees to:

- Password combination policy is there. Choose passwords with at least 7 characters (numbers and symbols) and avoid information that can be easily guessed.
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroyit when their work is done.
- Exchange credentials only when necessary. When exchanging them in-personisn't possible, employees should prefer the phone instead of email, and only if theypersonally recognize the person they are talking to.
- Change their passwords every 45Days. Password change policy is also there on active directory.

Transfer data securely

- Avoid transferring sensitive data (customer information, employee records, Sales data) to other devices or accounts unless necessary. When mass transfer of such data isneeded, we request employees to contact IT department.
- Share confidential data over the company network/ system and not over public Wi-Fi orprivate connection.
- Ensure that the recipients of the data are properly authorized people or organizations andhave adequate security policies.

- Report scams, privacy breaches and hacking attempts to IT department at once.

The ITdepartment needs to know about scams, breaches, and malware so theycan better protect the company's infrastructure.
For this reason, we advise our employees to report perceivedattacks, suspicious emails, or phishing attempts as soon as possible to the IT department. The IT Department must investigate promptly, resolve the issue, and send acompanywide alert when necessary.

****