CYBER SECURITY AND DATA PRIVACY POLICY

Background:

Sunteck Realty Limited (hereinafter referred to as "**Sunteck**" or "**The Company**") is one of the fastest growing Maharashtra-based luxury real estate company engaged in construction, development, and management of commercial and residential properties.

The Company is dedicated to ensuring data privacy and Cybersecurity by putting in place a solid framework that enables well-organized information management and incorporates all security protocols to safeguard the integrity of data that is stored within the company's infrastructure. The protection of your privacy and personal data is an important concern to which the Company pays special attention in its business processes. The Company processes the personal data provided by the third party voluntarily during visits to its website, in accordance with the applicable law of the country where the Company's website is maintained.

Definitions:

"Personal Information (PI)": is information that is about, or can be related to, a natural person/entity, which either directly & indirectly, can identify such person/entity or reveal one's identity.

Purpose:

The policy seeks:

- To cultivate organization-wide privacy culture to protect the rights and privacy of individuals / data of the Company.
- To comply with applicable privacy and data protection legislations by implementing privacy principles and controls within the company
- To ensure that Sunteck is adequately prepared to mitigate Privacy and Cybersecurity related risks.

Scope:

The Policy applies to the contractor of the Company and data collected, received, possessed, owned, controlled, stored, dealt with or handled by anyone.

Cyber Security

Access Control Mechanisms:

The mechanism addresses all the aspects involved in prevention of unauthorized access (including physical), fraud, theft, damage and interference to information and IT systems / assets, which lead to interruption of business activities of the Company.

Control mechanism will seek to:

- Minimize the need for special access privileges (e.g., User IDs that have additional capabilities, such as 'Administrator', or special capabilities, such as User IDs that can be used to authorize payments).
- Require approval/s of business application/system/network/computing device from appropriate authority to provide access privileges for both business users and staff.

Use of Email:

Emails often host phishing attacks, scams, or malicious software (e.g., trojans and worms). The mechanism ensures that strict and appropriate controls are established for a secure email system and the access to email is controlled as per business requirements. To avoid virus infection or data theft, the company instructs its employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait titles (e.g., offering prizes, advice) and do not try to open restricted domains.
- Check email and names of people they received a message from, to ensure they are legitimate.
- If an employee isn't sure that an email, they received is safe, they should forthwith contact their IT Team.

Password Management:

Password leaks are dangerous since they can compromise company's entire infrastructure. For this reason, the company instruct employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols)
- Exchange credentials only when absolutely necessary.
- Change their passwords regularly, but at a minimum every three months.

Transfer Data Securely:

Transferring data introduces security risk. Employees must:

- Log into company accounts and systems through secure and private networks only and avoid accessing internal systems and accounts from other people's devices.
- Avoid transferring sensitive data to other devices or accounts unless necessary.
- Share confidential data over the company network/system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.

Data Privacy

Sunteck shall strive for the preservation of the Confidentiality, integrity and availability of the company's information assets pertaining to customer's data. All employees are required to follow

the established policies and standards regarding the protection and use of personal information. The employees sign a “Confidentiality Acknowledgement” which abides to the components of the policy and are expected to honor at all times.

Collection of Information:

The Company shall collect, use, retain, and disseminate personally identifiable information (PII) only that is permitted by law of land and would also describe the purpose(s) for which personally identifiable information (PII) is collected, used, retained, and disseminated. The Company may collect the following information:

- Name, gender, residential / correspondence address, telephone number, date of birth, marital status, email address or other contact information.
- PAN, Aadhaar, KYC Status, Signature and Photograph and frequency of visits to the Company’s Office

Please be aware that third-party websites linked to the company’s website are not covered by this policy.

Training and Awareness:

The Company strives to conduct training and educational sessions for employees to make them aware on building cybersecurity and basic system hygiene awareness, to enhance knowledge of this Policy. The employees are required to complete relevant trainings that varies according to job function and their performance on routine evaluations.

Disciplinary Action:

- Sunteck expects all its employees to follow this policy and those who voluntarily/involuntarily cause security breaches may face disciplinary action from temporary suspension to permanent termination to civil / criminal action as per the applicable law/s.
- The Company shall examine each incident on a case-by-case basis.

Policy monitoring and review:

The Company shall review the implementation of the Cyber Security and Data privacy policy on a yearly basis. The review shall be placed before the Board of directors for taking appropriate action(s), if required.