Data Security Policy

Introduction:

At Vendekin Technologies Pvt. Ltd. and its subsidiaries and affiliates (hereinafter collectively referred to as “Vendekin”, “We”, “Us” or “Our”) we understand the care you assign towards usage and sharing of your information and we appreciate your unwavering trust that we will do so carefully. This notice describes our Data Security policy.

This Data Security Policy describes how we collect, use, and disclose personal information that you provide to us when you visit or use our website https://www.vendekin.com/ (the “Site”) and our mobile application the name of Payekin in UK and US and Vendekin in India (the “Application”), collectively “**Services**”.

This Data Security Policy explains the objective, applicability of this policy and security measures adopted by us to ensure protection of your information. For more details on how we collect, use, and disclose information when you use our services please refer to our privacy policy.

Please review this Data security policy carefully. By using our Services, you consent to the processing of your personal information as described in this Data security policy. IF YOU DO NOT AGREE WITH THESE PRACTICES, PLEASE DO NOT USE THE SERVICES.

Some Key terms:

In our Data security policy are:

- **“User(s)”** (hereinafter collectively referred to as “You”, “Your”, “User”), mean our user(s) who use our Services, including, without limitation, any companies, organizations, or other legal entities that register accounts or otherwise access or use the Services through their respective employees, agents, or representatives.
- **“User Content”** means all electronic data, text, messages or other materials, including personal data of Users, submitted to the Service(s) by You in connection with Your use of the Service(s).
- “**Applicable Data Protection Law”** means the General Data Protection Law, Data Protection Act and Personal Data Protection Bill.

Objective

The main objective of The Data Security Policy (hereinafter referred to as “the policy”) is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy has been drafted to achieve the following objectives:

i. Founding Vendekin data security stance and classification scheme.
ii. To inform the users of Vendekin their responsibility to protect all data assets.
iii. To guarantee integrity and security of all user data.

Applicability

Our data security policy applies to all users, agents, contractors or any other party accessing the Mobile Application and the Vendekin Official Website. This policy also applies to all of our and all consumer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our agents.
If the user fails to comply with the terms mentioned in this policy, it would result in termination of user account and potential legal action by Vendekin.

Authority

This policy authorises Vendekin to develop, review and implement data security policies to ensure the protection of proprietary information of its users, agents, contractors or any other party accessing its services.

Policy Review

Due to the dynamic nature of the internet, this policy will be subjected to regular reviews, you are advised to regularly review this Agreement, as your continued use of the services after any such changes constitute your agreement to such changes.

Data Access

Access to our technology resources is only permitted through secure connectivity (for e. SSL) and requires authentication. Our password policy requires complexity, expiration, lockout and disallows reuse. We here at Vendekin, take your data security very seriously and adhere to the principle of “least access” i.e. users are allowed access only to the information they require in order to perform their task. No user shall be granted access to sensitive information stored on Vendekin’s database. The access is revoked immediately after employee termination.

Safety measures

We are committed to ensuring the highest level of protection to your personal data. We have opted for all reasonable and appropriate technical measures like, pseudonymization, encryption such as SSL, access, and retention policies to guard against unauthorised access

and unnecessary retention of personal data in our systems. We also ensure that your personal data stored in our systems are secured via physical security measures.
If you feel that the security of your account has been compromised, you are advised to change your password immediately or immediately report to Vendekin.

Third party

You may access third party websites via links on our website/application with or without warning. Vendekin is not responsible for protecting the data provided by you to those third-party websites.

Security Policies

We review and update our security policies at least annually. Our employees are obligated to acknowledge policies on an annual basis and are provided training and job-specific security and skill development for key job functions.

Personnel Screening

We conduct background research at the time of hire (to the extent permitted or facilitated by applicable laws and countries). In addition, we communicate our data security policies to all personnel (who must acknowledge this) and require new employees to sign non-disclosure agreements and provide ongoing privacy and security training.

Dedicated Security Personnel

We have a dedicated Security personnel department focusing on network and system security. This team is responsible for security compliance and response in case of any incident.

System Vulnerability Assessments

We have a vulnerability assessment program which includes periodic scans, identification, and remediation of security vulnerabilities on servers, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third-party vendors.

Notification of Breach

Despite all the best efforts, no method of transmission over the Internet, or method of electronic storage, is perfectly secure. Therefore, we cannot guarantee absolute security. However, if we learn of a security breach, we will notify affected users so that they can take appropriate protective steps. We are committed to keeping our consumers and customers fully informed of any matters relevant to the security of their account and to providing

customers with all information necessary for them to meet their own regulatory reporting obligations

Business Continuity

Our databases are backed up on a regular basis and are verified regularly. Backups are encrypted and stored within the production environment to preserve their confidentiality and integrity and are tested regularly to ensure availability.

Customer Responsibilities

Keeping your data secure also requires that user maintains the security of his account Apart from above-mentioned measures, you are yourself expected to protect your own account by using a unique and strong password, not sharing the password with anyone, logging out after having used the services and limiting access to your computer and browser. You should also ensure that you have sufficient security on your own devices.

We respect your valuable comments

In case of any queries that you may have please reach to our Data Protection Officer at dpo@vendekin.com

This Data Security Policy was last updated on 12 July 2019