Data Security Policy for Kein Sheldrake IT Help

Effective Date: 04/07/2023

At Kein Sheldrake IT Help, we are committed to maintaining the security and confidentiality of the data we handle. This Data Security Policy outlines the measures we take to protect data from unauthorized access, disclosure, alteration, and destruction. By using our website or services, you agree to adhere to the terms of this policy.

1. Data Classification: a. We classify data into different categories based on its sensitivity and criticality. This includes personal information of customers, employees, and any other data entrusted to us.

2. Data Handling: a. We ensure that data is handled only by authorized personnel who have a legitimate need to access it for business purposes. b. Data is collected and processed in a lawful and transparent manner, and only for specified purposes outlined in our Privacy Policy. c. We take reasonable steps to ensure the accuracy and completeness of data collected, and promptly update or correct any inaccuracies.

3. Data Access and Authorization: a. Access to data is granted on a need-to-know basis, and only authorized individuals are given appropriate access rights. b. User accounts are secured with strong passwords and are periodically reviewed and updated. c. Employees are trained on data protection and confidentiality, and are required to sign confidentiality agreements.

4. Data Storage and Transmission: a. Data is stored in secure systems with appropriate access controls, encryption, and other technical safeguards to protect against unauthorized access. b. Confidential and sensitive data is transmitted over secure channels, such as encrypted connections or secure file transfer protocols.

5. Data Retention: a. We retain data only for as long as necessary to fulfill the purposes outlined in our Privacy Policy, or as required by applicable laws and regulations. b. Once data is no longer required, we securely delete or anonymize it to prevent unauthorized access.

6. Incident Response: a. We have procedures in place to promptly detect, investigate, and respond to any data security incidents or breaches. b. In the event of a data breach, we will notify affected individuals and regulatory authorities as required by applicable laws and regulations.

7. Third-Party Service Providers: a. When engaging third-party service providers, we ensure that they maintain an adequate level of data security and comply with applicable data protection laws. b. We conduct due diligence to assess their security practices and review their privacy and security policies.

8. Employee Responsibilities: a. All employees are responsible for adhering to this Data Security Policy and protecting the data they handle in the course of their duties. b. Employees are required to report any suspected or actual data security incidents or breaches to the designated authority.

9. Policy Review: This Data Security Policy will be reviewed periodically and updated as necessary to reflect changes in technology, legal requirements, and business practices.

10. Contact Us: If you have any questions, concerns, or requests regarding this Data Security Policy or our data security practices, please contact us at info@sheldraketech.com.

By using our website or services, you acknowledge that you have read and understood this Data Security Policy and agree to comply with the measures outlined herein to ensure the security and protection of data.