Client Confidentiality and Data Security Policy

1. Introduction

Jeff Wong is committed to upholding the highest standards of client confidentiality and data security. This policy outlines my commitment to safeguarding client data, including personal data, in compliance with the industry best practices.

2. Compliance with the Singapore PDPA

2.1. Personal Data

We acknowledge and adhere to the Singapore PDPA, which governs the collection, use, and disclosure of personal data. Personal data refers to any data that can be used to identify an individual.

2.2. Consent

We obtain explicit consent from clients when collecting, using, or disclosing their personal data for project-related purposes.

2.3. Purpose Limitation

We collect and process personal data only for specified purposes that are relevant to the project and that the client has consented to.

2.4. Data Protection Officer

Jeff Wong is the Data Protection Officer (DPO) responsible for ensuring compliance with the PDPA and addressing data protection queries or concerns.

3. Confidentiality

3.1. Non-Disclosure Agreements (NDAs)

We are prepared to sign Non-Disclosure Agreements (NDAs) with clients upon request. NDAs reinforce our commitment to maintaining client confidentiality.

3.2. Access Control

Access to client environments, is strictly controlled and granted on a need-to-know basis. Unauthorized access is prohibited.

3.3. Data Handling

Client data is handled with the utmost care and confidentiality. We do not share, disclose, or use client data for any purpose other than what is explicitly agreed upon with the client.

3.4. Remote Work

When working remotely, alll team members are required to use secure and encrypted communication and collaboration tools to protect client data from unauthorized access.

4. Data Security

4.1. Secure Data Storage

We maintain secure data storage practices, including encryption, access controls, and regular data backups, to protect client data from loss or unauthorized access.

4.2. Infrastructure Security

We follow industry best practices for securing infrastructure and cloud-based services used in our projects. Regular updates are conducted.

4.3. Incident Response

In case of a security breach or data leak, I will promptly inform the affected client and take all necessary steps to mitigate the issue and prevent recurrence.

5. Data Retention

I retain client data, including personal data, only for the duration of the project and as required by law or contractual obligations. Data is securely deleted when it is no longer needed.

6. Compliance

I adhere to all relevant data protection and privacy laws, including the Singapore PDPA, as applicable to our operations.

7. Third-Party Services

When using third-party services for project work, we ensure that these services also adhere to high standards of security and confidentiality.

8. Client Communication

I maintain transparent communication with clients regarding the handling and security of their data, especially personal data. Clients are encouraged to reach out with any questions or concerns about data security.

9. Review and Update

This policy is reviewed periodically and updated as needed to reflect changes in technology, best practices, and regulatory requirements.

Last updated 2021-05-07