INFORMATION SECURITY & PERSONAL DATA PROTECTION STATEMENT

1. Information Security Commitment

We are committed to protecting the confidentiality, integrity and availability of information entrusted to us in the course of providing sustainability and environmental consulting services. Information security forms an integral part of our governance framework and risk management approach.

Our practices are aligned with internationally recognised information security principles, including those reflected in ISO/IEC 27001, without representing formal certification.

2. Governance and Accountability

Information security responsibilities are clearly defined within the organisation. Oversight mechanisms are in place to ensure that information security risks are identified, assessed and managed in a structured and proportionate manner, consistent with the nature and scale of our operations.

Policies and procedures are periodically reviewed to maintain their relevance and effectiveness.

3. Personal Data Protection and Legal Compliance

We comply with the Personal Data Protection Act 2010 (“PDPA”) and applicable data protection requirements in Malaysia.

Personal data is:

- Collected and processed lawfully and fairly
- Used only for legitimate and defined business purposes
- Protected against unauthorised or unlawful access, disclosure, alteration or loss

Access to personal data is limited to authorised personnel on a need-to-know basis.

4. Risk-Based Information Security Controls

We adopt a risk-based approach to information security. Appropriate administrative, technical and organisational controls are implemented to safeguard information assets, including but not limited to:

- Access control mechanisms
- Logical and physical security measures
- Secure handling, storage and transmission of information
- Segregation of duties where appropriate

Controls are proportionate to identified risks and the sensitivity of the information involved.

5. Confidentiality of Client Information

All client information, whether commercial, technical, financial or personal in nature, is treated as confidential. Such information is used solely for the purpose of delivering agreed services and is not disclosed to unauthorised parties without lawful basis or client consent.

Confidentiality obligations apply throughout and beyond the duration of client engagements.

6. Third-Party and Supplier Management

Where third-party service providers are engaged to support business operations, reasonable steps are taken to ensure that they are subject to appropriate confidentiality, data protection and information security obligations.

Third-party access to information is restricted to what is necessary for the performance of contracted services.

7. Incident and Breach Management

Procedures are in place to identify, assess and respond to information security incidents, including potential data breaches.

Where applicable, incidents are managed in accordance with legal and regulatory requirements, including notification obligations under the PDPA.

8. Data Retention and Disposal

Information is retained only for as long as necessary to fulfil contractual, legal, regulatory or operational requirements. Secure disposal methods are applied when information is no longer required, to prevent unauthorised access or recovery.

9. Awareness and Continuous Improvement

Personnel handling information are expected to adhere to established information security and data protection requirements. Information security practices are subject to periodic review as part of our commitment to continuous improvement.

10. Statement Review

This statement may be updated from time to time to reflect changes in legal requirements, risk considerations or business operations. The most current version is made available upon request or via our official communication channels.

Alignment with ISO/IEC 27001 reflects adherence to recognised information security principles and does not constitute a claim of certification.