Exabytes Information Security Statement

Exabytes Group of Companies (hereinafter referred to as 'Exabytes' or 'our' or 'us') is committed to establishing and proactively managing an Information Security Management System ("ISMS"), which recognizes that Confidentiality, Integrity, and Availability ("CIA") of information are integral to its management function. Exabytes' ISMS is designed to protect information assets, prevent security incidents, and continually improve security practices in line with evolving technologies and regulatory requirements.

Our Objective

The objective of Exabytes' ISMS is to ensure comprehensive protection of its information assets against potential breaches of confidentiality, compromises to integrity, and/or interruptions to availability. The ISMS is designed to minimize the risk of damage to information assets by preventing security incidents and mitigating their potential impact.

Our Commitments

We are committed to maintaining a robust ISMS and ensuring that:

1. **Protection Against Unauthorised Access:** All information assets, including personal data and sensitive business information, will be protected against unauthorized access, disclosure, alteration, or destruction through appropriate technical, administrative, and physical controls.
2. **Confidentiality Assurance**: Confidentiality of information will be preserved in accordance with contractual obligations, company policies, and applicable laws, including the Personal Data Protection Act 2010 (PDPA) in Malaysia.
3. **Integrity Maintenance:** The integrity of information will be maintained to ensure that data is accurate, complete, and reliable for decision-making and operational purposes.
4. **Availability Assurance:** Information required for business processes will be available when needed, with minimal disruption, ensuring continuity of critical services.
5. **Compliance with Legal and Regulatory Requirements:** All applicable Malaysian laws, regulations, and industry standards relating to information security and data protection will be met.
6. **Business Continuity Planning**: A Business Continuity Plan (BCP) is developed, maintained, and periodically tested to mitigate the impact of disruptions and ensure recovery of critical business functions in a timely manner.
7. **Incident Management and Reporting**: All actual or suspected information security incidents or breaches will be promptly reported to the Incident Response Team, investigated thoroughly, and documented in accordance with ISMS procedures.
8. **Continual Improvement**: Our ISMS and associated policies, procedures, and controls will be regularly reviewed and updated to enhance effectiveness, adapt to technological changes, and address emerging threats and regulatory requirements.

Changes to this Information Security Statement

Exabytes may update this Information Security Statement from time to time to ensure compliance with applicable laws and regulatory requirements in Malaysia. Any changes will take effect upon publication on our website. You are encouraged to review this Statement periodically to stay informed about our information security practices.

Enquiries

If you have any questions or concerns regarding our information security practices, please contact us at enquiry@exabytes.com.