SECURE SYSTEM ENGINEERING PRINCIPLES POLICY

Background

The background for these principles is the increasing threat of cyber-attacks and data breaches. With the proliferation of sensitive data in today's digital world, it is essential for companies like SDM Holdings Ltd to have robust security measures in place to protect our client's data.

These principles are developed to address security at all levels of the technology stack, from the business layer to the technology layer, ensuring that client data is protected at all times and that we are compliant with relevant regulations and industry standards.

Scope

The scope of these secure system engineering principles for Secure Data Management covers the overall design, development, and maintenance of our systems.

These principles aim to ensure the security of our systems at every layer of the technology stack, including the business layer, data layer, application layer, and technology layer.

These principles are intended to be implemented and followed by all employees involved in the design, development, and maintenance of our systems to ensure the security and integrity of our client's sensitive data.

Principles

Business Layer:

1. Implement strict access controls to ensure that only authorised personnel have access to sensitive client data.

2. Regularly review and update our security policies and procedures to ensure they are in line with industry best practices.

3. Adhere to all relevant regulations and compliance standards related to data protection and privacy.

4. Establish an incident response plan and conduct regular incident response drills.

Data Layer:

5. Use encryption to protect sensitive data at rest and in transit.

6. Implement regular backups to ensure that data can be recovered in the event of a disaster.

7. Use multi-factor authentication for access to sensitive data.

8. Implement data access control and auditing mechanisms.

Application Layer:

9. Implement input validation and sanitisation to protect against injection attacks.

10. Use secure communication protocols to protect data in transit.

11. Implement role-based access controls for the application.

12. Perform regular vulnerability scans and penetration testing.

Technology Layer:

13. Keep all software and hardware up to date with the latest security patches.

14. Use firewalls and intrusion detection/prevention systems to protect against network-based attacks.

By adhering to these principles, we aim to provide the highest level of security for our client's data and maintain the trust of our clients. It's important for all employees developing software to understand and implement these principles in their daily work.

Signature/Realise Confirmation

26.07.24

Marc Chauveau

Managing Director

26.07.24

Nicola Peters

Quality & Compliance Manager