SECURE DEVELOPMENT POLICY

The objective of SDM Holdings Limited is to provide a storage, retrieval and management service for the documentation and products of its customers.

To achieve this objective, the organisation will maintain effective and efficient secure development practices based upon the requirements of ISO 27001:2013.

As such, the Managing Director (Marc Chauveau) of SDM Holdings is committed to the following:

- Our company is committed to maintaining a strict separation of development, testing, and operational environments to ensure the secure and efficient development and deployment of web applications. This includes implementing different hardware and software configurations and implementing robust testing procedures before pushing any code to production. By adhering to this policy, we aim to minimise the risk of security breaches and ensure the highest level of quality for our software-based products.

- Strict access controls are implemented to minimise the risk of security breaches and ensure the highest level of quality for software-based products.

- Secure IT Engineering procedures based on security principles are established, documented, and applied for in-house IT Engineering. Data security and accessibility must be balanced in all architecture layers and new technology for security threats must be evaluated.

- Security engineering principles are applied to outsourced systems through agreements with suppliers to ensure comparable standards.

- Thorough testing and verification are necessary for new and updated systems, including detailed testing plans, input and expected outputs under various conditions. Conducted by the development team and subject to specific approval assessments to ensure proper function.

- External cyber security scanning and risk assessments are conducted to ensure the security of our software during development, along with regular periodic penetration testing to further validate security.

- Regular review of established engineering processes and principles to ensure they remain relevant and effective in protecting against new potential threats.

- Code analysis tools, vulnerability scanners, A/B testing, and best practices are used to test and verify systems in a realistic environment as acceptance testing methods and ensuring adequate security for new and upgraded web applications.

- To ensure the integrity of live system data, a separate test environment is used for test data, with distinct host servers and credentials. Data used during testing is promptly purged upon completion to mitigate potential security vulnerabilities.

Signature/Realise Confirmation

26.07.23

Marc Chauveau

Managing Director

26.07.23

Nicola Peters

Quality & Compliance Manager