Streamline Security Commitment

Sublime Streamline Limited, (Streamline), takes the Privacy and Security of our clients' business data very seriously.

We use and follow industry best practices, including:

- risk management standards based on the globally recognised ISO 31000
- security controls based on the ISO 27001 Information Security Management Standard;
- internal security team responsible for management and monitoring of all products and related services;
- use of a secured encrypted channel, for all communication, ensuring that the transmission of data between the computer/browser and the streamline products are not compromised;
- compliance with Payment Card Industry Data Security Standard (PCI DSS) for the handling of credit card data; and
- compliance with the Australian and New Zealand privacy laws, including the Australian Privacy Principles (for more details, please visit Streamline's Privacy Policy).

Independent testing

Streamline engages external security vendors to test our products both during and post-development.

Open Web Application Security Project Application Security Verification Standard, is used as the basis for this testing which provides:

- application developers and application owners with a yardstick to assess the degree of trust that can be placed in our online products; and
- guidance to our product engineers about building security controls to satisfy application security requirements.

Banking security standards

Streamline uses the same security measures required of banks and other financial institutions when transmitting data. A streamline client authorises their data supplier (typically a bank or other financial institution) to provide streamline with transaction data relating to the client's nominated account through a secure, integrated software linkage, direct between the supplier and streamline. Streamline complies with PCI DSS which is a security standard set by the major credit card companies, in relation to financial data transmission.

World class partner

Streamline's cloud partner of choice is Amazon Web Services who provide key infrastructure and services, such as monitoring for suspicious activity, physical security, server and power redundancy, and built-in firewalls:

- Amazon Web Services production platform hosted in Australia
  - For details about Security, Privacy, and Compliance in Amazon Web Services, please visit here.
  - Amazon Web Services audits are performed as per https://aws.amazon.com/compliance/

To report a security vulnerability, please email security.officer@sublimegroup.net