Cyber Security at First Samuel

First Samuel places great importance on information security, including cyber security, to protect against external threats and malicious insiders. Our cyber security strategy prioritises detection, analysis and effective management of cyber risks, and resilience against cyber incidents.

We regularly benchmark our cyber security practices against the Essential Eight Maturity Model and the recommendations of the Australian Cyber Security Centre.

This document provides an overview of our approach to information security and our practices to secure data, systems and services.

OUR APPROACH

I] IDENTIFY

- **Risk Governance and Oversight**

  Risk governance and risk management are a function of our management culture and embedded practices. The governance model is designed and implemented by the CEO, the Risk Compliance & Governance Manager and the Technology Support Officer and our external IT support company, Emerging IT. The Board's Audit and Risk Committee provide governance and oversight.

- **Information Security and Cybersecurity Policies and Standards**

  We maintain information security policies and standards to document our approach to compliance with internal policies and regulations.

- **Asset Management**

  The firm maintains an asset management program to appropriately inventory, classify, and protect applications, data, and hardware.

II] PROTECT

- **Training and Awareness**

  We provide Associates with cyber security awareness training. Additional, targeted training is delivered periodically to ensure Associates maintain awareness of evolving cyber threats.

- **Identity and Access Management**

  We have controls to identify, authorise, authenticate and manage Associates' and clients' access to our systems and information.

- **Application and Software Security**

  We manage application and software security through our software management process. These include multifactor authentication, control monitoring and logging.

- **End User Device Security**

  Our mobile solutions allow Associates to conduct business activities on their dedicated devices while protecting our systems and client data.

- **Data Protection and Data Privacy**

  We have controls designed to safeguard company and client information. This includes secure storage, handling, transmission, and destruction.

- **Physical Security**

  We have physical access controls in our office space.

- **Vendor Security**

  Information security risk management is built into our vendor management process. This includes vendor selection, onboarding, and risk management.

III] DETECT

- **Continuous Monitoring**

  Through use of its partners, First Samuel maintains detection controls at the network and application levels. These are to detect anomalous activity that might indicate threat activity.

- **Anomaly Detection**

  We ensure that security anomalies and events are detected quickly.

IV] RECOVER

- **Business Continuity and Technology Resilience**

  The firm has a mature and comprehensive Business Continuity Program for Disaster Recovery (BCP/DR). The program covers both business and technology resilience. The main features of the program include recovery and restoration of services.