Cyber Security Statement

Our cybersecurity and whom we share data with is built upon the Australian Cyber Security Council's Essential Eight guidelines and the National Institute of Standards and Technology (NIST) Cybersecurity Frameworks.

At Finkey Capital, cyber security is a fundamental aspect of our strategy, deeply integrated into the everyday operations of our Australian-based business. Our approach revolves around proactive measures to safeguard our systems and customer data, encompassing the detection, analysis, and swift response to potential cyber threats and incidents.

We adhere to the highest security standards and implement cutting-edge controls to protect customer data. To achieve this, we collaborate and store data with partners and third-party platform providers renowned for their excellence in Australian cyber security practices.

A robust set of cyber security controls is meticulously maintained to shield our services and customer data. These controls are subject to regular testing and updates, encompassing essential elements such as firewalls, virtual private networks, multi-factor authentication, encryption, access control, email security, malware detection, application control, and endpoint detection.

We regularly ensure our systems and those of our partners and third parties are consistently audited, with immediate attention to addressing critical security vulnerabilities. Our partners and third parties employ dedicated security teams to ensure round-the-clock cyber security monitoring, providing comprehensive protection.

Every staff member undergoes routine cyber training and testing, fostering a strong culture of cyber awareness throughout our organisation.

For more detailed information regarding Finkey's commitment to cyber security, please don't hesitate to contact us via email at privacy@finkey.co