Information Security Policy

Why is this policy important?

This Information Security Policy sets out requirements for the proper and secure use of information technology services and IT assets (computers and any other devices we use in our business, along with the applications they use).

Its objective is to protect our business, clients and employees to the maximum extent possible against security threats that could jeopardise their integrity, privacy, reputation and business outcomes.

The policy applies to all employees, including temporary employees, visitors with temporary access to our premises, and to any third parties we interact with.

Our policy

We do this:

- Only use software applications which meet recognised, international security standards.
- Ensure our IT assets are well maintained, and software is up to date.
- Ensure only IT assets approved by us can access company email accounts.
- Maintain strong password protection, appropriate encryption mechanisms and antivirus software, to keep our IT assets secure at all times (including where that access is via remote access).
- Manage access to IT assets and any applications used for business purposes centrally via an established approval process.
- Regularly review our cyber risks and threats, and review the appropriateness of our risk mitigation approach.
- Initiate six-monthly testing of our cyber vulnerabilities by service providers (e.g. website, other external interaction points).
- Maintain appropriate cyber risk monitoring, threat detection and protection systems.
- Report any material cyber security breaches promptly.
- Maintain appropriate levels of access to our physical premises.

We don't do this:

- Access internet resources for non-authorised advertising, external business, spam, political campaigns and other uses unrelated to our business.
- Access illegal sites, hacking sites and other risky sites.
- Use devices for work purposes that have not been approved.
- Use software applications that are sourced from vendors or independent developers that do not meet robust security standards.

Implementation

All brokers and FAP employees receive induction and annual retraining on the contents of this policy and complete cyber security training modules.

IT asset access is controlled, approved and reviewed centrally with application access reviewed six-monthly.

All applications are reviewed annually to ensure they are current and up to date, particularly as regards security patches.

An Employee Exit Checklist is used to ensure all security access is revoked when an employee leaves the brokerage.

External cyber security penetration testing is undertaken by an independent specialist annually.

Maintain a level of cyber insurance cover commensurate with the risks faced in our business.

Ensuring compliance

Annual third-party review and security assessment, third-party security monitoring service reporting.

Employee training attendance and test results.

Date

01/03/2021