

Cyber Security Policy

Protecting client information is an important part of the services provided by Cranage Private Wealth Pty Ltd ABN 97 007 009 903, Corporate Authorised Representative No. 260866 of CFG Advice Pty Ltd ABN 62 621 016 055, Australian Financial Services Licence No. 501857. Cyber security is an ongoing process. No system can be guaranteed to prevent every incident, but we use risk-based controls and regularly review our practices to reduce the risk of unauthorised access, loss, misuse or disclosure.

Purpose and scope

This public policy summarises our approach to protecting information and technology used to provide financial services. Detailed operational controls, incident procedures and system configurations are maintained separately and are not published for security reasons.

Our approach

Our security arrangements are designed with reference to recognised cybersecurity guidance, including the Australian Signals Directorate Essential Eight. The Essential Eight is a baseline and does not address every cyber risk. Any statement about a specific maturity level should only be made where supported by a current, documented assessment across all eight mitigation strategies.

Security measures

Depending on the system and risk, measures may include:

- Multi-factor authentication and role-based access controls.
- Approved and managed devices, device encryption and endpoint protection.
- Security updates, vulnerability management and restrictions on administrative access.
- Encryption and secure transfer methods where appropriate.
- Email and web filtering, monitoring, logging and alerting.
- Secure backups and recovery arrangements.
- Staff training on phishing, fraud, privacy and secure information handling.
- Due diligence and contractual controls for technology and service providers.
- Cyber incident response and data breach response procedures.

Approved systems and providers

Client information must only be stored, accessed or shared through approved business systems and authorised service providers. Providers may include cloud, software, administration, paraplanning and information technology services. Our administration and paraplanning providers may access information from the Philippines. Our other approved technology and service providers are located in Australia. Further information is available in our Privacy Policy.

Incident response

Suspected cyber or privacy incidents are assessed, contained and investigated under our incident response and data breach response procedures. We take steps appropriate to the circumstances to preserve evidence, reduce harm, restore services and meet applicable notification or reporting obligations. Where we suspect an eligible data breach may have occurred, we will conduct a reasonable and expeditious assessment and take reasonable steps to complete the assessment within 30 days. If an eligible data breach is established, we will notify affected individuals and the Office of the Australian Information Commissioner as soon as practicable, unless an exception applies.

How clients can help

- Use strong, unique passwords and enable multi-factor authentication where available.
- Do not send Tax File Numbers, identity documents, bank details or other sensitive information by ordinary email unless specifically instructed and an approved secure method is unavailable.
- Use our approved secure portal or document-sharing method when requested.
- Treat unexpected links, attachments, login prompts and payment requests with caution.
- Verify any request to change bank details or redirect a payment using a trusted telephone number already known to you.
- Keep devices and software updated and protected by a screen lock.
- Contact us promptly if you believe information or communications connected with us may have been compromised.

Payment and impersonation warning

Email accounts can be impersonated or compromised. Do not rely solely on an email requesting a payment, transfer, change of bank account or disclosure of sensitive information. Confirm the request using a trusted contact method before acting. We will not ask you to disclose your password or multi-factor authentication code.

No security guarantee

This policy does not guarantee that a cyber incident cannot occur and does not represent that every system has achieved a particular Essential Eight maturity level. Security controls and technology change over time. Public descriptions are kept general so they do not disclose information that could weaken security.

Contact

To report a suspicious email, unauthorised disclosure or possible security incident, contact us immediately on 03 9097 6000 or at info@cfgadvice.com.au. If the matter concerns a payment or change of bank details, telephone us using a number you have independently verified.

Phone	03 9097 6000
Email	info@cfgadvice.com.au
Mail	PO Box 534, Flinders Lane VIC 8009
Website	www.cranagegroup.com.au