CENTREPOINT ALLIANCE

How we manage data and security

Centrepoint Alliance Limited places paramount importance on both data management, privacy and data security. Safeguarding both your information and ours is essential in today's digital environment.

Our commitment to Cybersecurity at Centrepoint consists of comprehensive policies supported by a suite technical of measures. The implementation of these measures serves to fortify not only our Centrepoint Infrastructure but also our Advisers and their clients against the persistent threats of cybercrime, identity theft, and fraudulent activities. Centrepoint's Cyber Program encompasses both technical and non-technical aspects.

Technical Cybersecurity measures

- Web Content Filtering.
- Email Content Filtering.
- Targeted Threat Protection (Safe Links) to minimise phishing links in emails.
- Next Generation Firewalls with 24/7 with 3rd party monitoring.
- Next Generation Antivirus and Antimalware Endpoint Protection.
- Cyber Security and Privacy Training to all Staff.
- Data Encryption at Rest and in Transit.
- Compulsory Multi-Factor Authentication and Password Management Policies, as well as single sign-on for supported applications.
- Advanced Conditional Access Policies to block access to Centrepoint environment from outside Australia.
- Device compliance, configuration management and hardware-based security mobile device management for all corporate devices including corporate mobile devices.
- Device encryption across all devices including corporate mobile devices.
- Mature implementation of the Australian Cyber Security Centre Essential 8.
- 24/7 Security monitoring by industry leading international vendor.
- Corporate domain management including domain multi-lock.
- Use of dedicated networks between our offices using a tier 1 carrier in Australia.
- On-going vulnerability management processes.
- Public Key Infrastructure (Certificate Management) from industry leading PKI provider.
- Advanced auditing capabilities across our Office 365 landscape including SharePoint, Exchange, and OneDrive.
- Microsoft 365 E5 licensed tenancy including the Advanced Identity Management and Governance including in Azure Active Directory P2 license such as identifying risky users, sign-ins and workload identities.
- Daily backups across major data landscapes including flat files, Salesforce and Office 365.

Non-technical measures

- Cybersecurity Committee which meets on a bimonthly basis. The Committee actively monitors Cyber Trends/threats, Data and Cyber governance as well as any corporate or adviser incidents.
- A Cybersecurity Policy and a Cyber Incident Response Plan.
- A Data Breach Response Plan.
- Business Continuity Management Plan.
- Membership of the Joint Cybersecurity Centre program.
- A Licensee Cybersecurity Standard.
- Annual Third-Party Cybersecurity Review process.

Centrepoint will continue to monitor and improve the Cybersecurity Program to ensure the highest level of Cybersecurity resilience within the business. Please refer to our Privacy Policy for additional information on how we collect, use, hold and disclose your personal information.