Our commitment to safeguarding your wealth

CYBER SECURITY

RICHARDSON GMP

At Richardson GMP Limited, we believe in being accountable to you. As such, we would like to take this opportunity to reassure you of the cyber security measures consistently used to protect your assets.

Threat management

Richardson GMP takes many steps to protect our systems from any data compromise, some of those steps include:

- **Next generation firewalls:** We use next generation firewalls that inspect data passing the firewall to ensure data is what it claims to be and is classified correctly.
- **Advanced endpoint security:** Our workstation all have advanced malware protection that is updated in real time, multiple times per day. We also use heuristic protection which protects workstations against zero day threats before they are known to most anti-virus solutions.
- **Structured patch management:** Emerging threats heard on the news are often attacks based on vulnerabilities already known and that have patches available. At Richardson GMP, we adhere to a strict patch cycle which ensures our server and workstation environments are patched well ahead of outbreaks to ensure we stay ahead of any vulnerabilities.
- **Protected networks:** At Richardson GMP we've separated our corporate and guest Wi-Fi to ensure we can provide guests access to required resources without allowing unknown devices or guest access to the corporate network.

Security Analytics

Richardson GMP collects analytics from our key systems to ensure that anomalies in the system are tracked and our information technology experts can review and action any perceived issues.

Information Protection & Access Management

- **Role-based access control:** With many systems in place, Richardson GMP has applied role based access control to ensure that the individuals who can access sensitive data are in an appropriate role and access to such data is provided on a 'need to know' basis.
- **Application security:** Applications are built using a centralized authentication method, this allows us to simplify security and have enhanced logging for easy auditing of information.

- **Device encryption:** Richardson GMP encrypts all mobile computers to ensure a lost or stolen device does not mean data is at risk. With this practice the data on mobile computers is protected.
- **Single sign on:** Richardson GMP utilizes a single sign on solution that allows our staff to minimize the amount of passwords that are required to be tracked, and this practice allows us to leverage a strong password policy.

Application & Infrastructure Protection

- **Penetration testing:** Richardson GMP hires external ethical hackers to test the strength of our applications and infrastructure. These tests allow us to identify any changes in our infrastructure which can reduce risk and increase our systems strength.
- **Software development standards:** At Richardson GMP we follow industry standards to ensure any internally developed software is secure. There is a defined software development life cycle (SDLC) which is followed along with adherence to the Open Web Application Security Project (OWASP) standards.
- **Secured data center:** Richardson GMP keeps all production data housed in a System and Organization Control (SOC) 1 & 2 compliant data center. The data center is staffed 24/7 with security and video surveillance and biometric physical access.
- **Third party physical security audits:** Richardson GMP conducts physical premise audits to ensure that our offices are secure and that staff are following policy and protecting client sensitive information.
- **Automated patch management:** Richardson GMP has automated patch management to ensure that all security patches are delivered to our server and workstation platform with minimal intervention from IT Staff. This minimizes risk of exposure to malware.

Cyber Security Management

- **Code of conduct:** Richardson GMP uses a corporate code of conduct and business ethics to reinforce with staff the importance of cyber security.
- **Incident response plan(s):** Richardson GMP has an incident response plan that ensures impacted parties can be notified promptly in the event that confidential information was compromised.
- **Business continuity planning testing:** As part of our commitment to ensure minimal disruptions, Richardson GMP holds a contract with a third party facility where critical business functions can be supported in the event that staff cannot gain access to one or more of our office buildings or if such buildings have lost power or connectivity.

We appreciate the trust that you've placed in Richardson GMP and we take the responsibility of securing your assets with the utmost importance. If you should have any questions, do not hesitate to reach out to your Advisor for more information.

Our strength. Your security.

The strength of the Richardson GMP network is our belief in defense in depth. This principle ensures that we have many safeguards in place so no single vulnerability or attack can compromise the network.