Cyber Security POLICY

JTH Asset Management Pty Ltd is committed to ensuring our business information and data is appropriately managed, stored and protected. Our Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. JTH understands that more of our business is conducted online, and this area continues to grow. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to security breaches. Not only does a cyber-attack threaten our company's confidential data, but it could also negatively impact the relationships with our customers and our damage the company's reputation, so it is vital to our interests and business operations, that the Company addresses cyber security threats by engaging an IT specialist to assist us with protecting our information assets.

This policy applies to all our employees and contractors, in the office or onsite, and anyone who has permanent or temporary access to our systems and hardware.

JTH aims to achieve our Policy objectives by engaging with an IT specialist that provides:

- Workstation protection which is actively monitored by a dedicated help desk team.
- Network protection delivered via Next-Gen 7-layer firewall and content filtering.
- Advanced malware protection, intrusion detections and protection (IDS/IPS).
- DNS protection that blocks traffic to malicious domains before connection is made.
- Microsoft 365 protection that analysis risk and enforces multi-factor authentication.
- Consolidated user management and authentication with single sign on (SSO).
- Full audit logs of user activity across Microsoft 365 platform.
- Email protection with advanced spam filter for all inbound and outbound emails.
- Machine learning to detect and remove phishing emails, malicious websites and malware.
- Staff training on cyber security awareness, passwords, email use and phishing attacks.
- Monthly simulated phishing attacks sent to all staff via email tailored specifically to JTH.
- Hardware and software support, software update and installation managed by IT provider.
- Backup and recovery managed via off-site cloud back up and VSS shadow copy.

This policy statement shall be displayed at our JTH office in Mackay and is accessible to employees and the public via our Company website. We will review this policy periodically to ensure it remains relevant to the needs of the Company and our clients.

The directors of JTH Asset Management endorse this cyber security policy which helps our employees to understand the processes we have in place to protect our company, data and assets.

JTH IS COMMITTED TO PROTECTING OUR INFORMATION ASSETS AND DATA AGAINST CYBER ATTACKS AND THREATS THORUGH RESPONSIBLE MANAGEMENT.

Jason Trannore | Director

Dan Hollis | Director