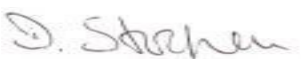
Information Security Policy

Caledonia are in continual pursuit of innovative measures to ensure the ongoing security of our information. This Policy is our commitment to information security as part of our established Information Security Management System (ISMS) which ensures a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity and availability of information through the following commitments:

- Establish and maintain an Information Security Management System (ISMS) in accordance with ISO 27001 as well as complying with all applicable statutory, regulatory and other requirements related to the ISMS
- Incorporating the ISMS into all business functions whilst ensuring it is appropriate to our purpose and strategic direction
- Set objectives and targets to measure our performance and identify opportunities for improvement, thus ensuring continual improvement of our ISMS
- Establishment of an Information Security Committee or equivalent who shall be the governing body for the ISMS, ensuring the following:
    - Proper information security systems are established, maintained, monitored, improved and achieving its objectives
    - Information assets are adequately protected using a risk-based approach
    - Performance of the ISMS is identified, analysed, evaluated, tracked, managed and reported
    - Manage the relationship between Caledonia and external IT Providers
    - Conduct compliance monitoring activities
    - Facilitate the ISMS management reviews
- Provision of training, familiarity and awareness programs to help employees and external IT Providers using Caledonia information assets better understand policies, responsibilities, consequences of non-compliance, potential security threats and how to prevent them
- All information assets will be identified, classified, labelled and recorded in a centralised inventory; be subject to periodic reviews to confirm their existence, adequacy of implemented controls and defined classifications
- Access controls shall be established according to our CP031 Access Control Policy
- Networks will be designed, configured and operated in a secure manner to prevent cyber-attacks and minimise disruptions
- Mobile devices and communication technologies will be controlled, secured and monitored
- All cyber and information security incidents, such as unauthorised disclosure, access or deletion/destruction of information assets (including applications or network credentials), will be reported to the Information Security Committee and promptly investigated
- Non-compliances to Policy will be identified, analysed, evaluated, tracked, managed and reported.

This policy is applicable to Caledonia in all its operations and functions including those situations where employees are required to work on specific sites. The Policy Statement will be reviewed on an annual basis and is available to all interested parties via the Caledonia website.

Jim Cunningham – Managing Director



David Stephen – Managing Director