Rundles.

Information Security

The Board and management of Rundle & Co are committed to preserving the confidentiality and integrity of all physical and electronic information assets throughout the organisation.

As a trusted supplier to clients in the public sector, Rundles understand the importance of information security and take this area extremely seriously. Rundles ensure effective information security measures by maintaining detailed risk and recovery plans and implementing effective mitigation strategies. This level of planning and focus on security has enabled our ISO27001 accreditation (international standard for information security management) and ensures Rundles deliver on its promise to maintain data and information security at all times.

The Board will invest all resources required to protect our information and that of clients and debtors from any security threats.

The purpose of the Policy is to protect all Rundles information assets and that of its stakeholders from all threats, whether internal or external, deliberate or accidental.

Policy Statement & Summary

Rundles maintain electronic and hardcopy information assets which are essential to delivering services for our clients. These resources are to be viewed as valuable assets over which the company has both rights and obligations to manage, protect, secure and control. Rundles employees, contractors, and other affiliates are expected to utilise these information assets for only legitimate business purposes while assuring the confidentiality, integrity and availability of the assets.

Information and information security requirements will continue to be aligned with Rundles goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels.

Rundles risk management framework provides the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The risk assessment and risk management plan identify how information-related risks are controlled. Additional risk assessments will be carried out as required to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the ISMS manual and are supported by specific, documented policies and procedures.

The ISMS is subject to continuous, systematic review and improvement by the Information Steering Committee, chaired by the Managing Director and including Director Information Systems, Information Security Manager and other management representatives to support the ISMS framework and to periodically review the security policy.

Our policy will be reviewed to respond to changes in risk assessment or risk treatment plan at 6 month intervals.

Chris Rundle

Managing Director