Rundles.

Information Security Policy

Resolve Together.

As One Team

Rundles.

INFORMATION SECURITY POLICY

Rundle & Co Limited maintains electronic and hardcopy information assets which are essential to performing services for our clients. Like any other capital resources owned by the company, 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, sub processors and other affiliates are expected to utilise these information assets only for legitimate business purposes while assuring the confidentiality, integrity and availability of the assets.

The Board and management of Rundle & Co Limited, located at Office 102, Harborough Enterprise Centre, 34 Compass Point Business Park, Northampton Road, Market Harborough, Leicestershire, LE16 9HW, which operates in the provision of debt recovery services, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

Information and information security requirements will continue to be aligned with Rundles goals and the 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.

Rundle's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The risk assessment and risk treatment plan identify how information-related risks are controlled. The Managing Director is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

The purpose of the Policy is to protect the Company's information assets from all threats, whether internal or external, deliberate or accidental.
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.

All employees of Rundles and certain external parties identified in the ISMS scope document are expected to comply with this policy and with the ISMS that implement this policy. All staff, and certain external parties, will receive and be required to provide appropriate training to individuals supporting Rundles. Violations of the security

policy will be investigated in accordance with the company's disciplinary procedures and will incur disciplinary measures the same as violations of other company policies.

The ISMS is subject to continuous, systematic review and improvement.

Rundles has established an Information Steering Committee, chaired by the Managing Director, and including the IT Manager, Information Security Manager and other management representatives to support the ISMS framework and to periodically review the security policy.

Rundles has achieved certification of its ISMS to ISO/IEC 27001:2017 standard.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, "information security" is defined as:

PRESERVING

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Rundles disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialised information security training.

CONFIDENTIALITY

This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to Rundle's information and proprietary knowledge and its systems [including its network(s), website(s), extranet(s), and e-commerce systems].

INTEGRITY

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency [including for network(s), e-commerce system(s), web site(s), extranet(s)] and data back-up plans,

and security incident reporting. Rundles must comply with all relevant data-related legislation (GDPR) in those jurisdictions within which it operates.

AVAILABILITY

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network [identified as part of the scope in section 1 of the ISMS Manual] must be resilient and Rundles must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

PHYSICAL ASSETS - NON-IT

The physical non-IT related assets of Rundles including but not limited to headquarters office, telephone systems, filing systems, APS and copiers.

PHYSICAL ASSETS - IT

The physical IT related assets of Rundles including but not limited to computer hardware, data cabling, firewall appliance, laptops, printers, and T-1 line.

INFORMATION ASSETS

The information assets of Rundles include information printed or written on paper, transmitted by mail or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD Roms, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means.

SOFTWARE ASSETS

The software assets of Rundles include the sets of instructions that tell the system(s) how to manipulate information (i.e., the software: operating systems, applications, utilities, custom programs, etc.).
Amendment or changes to Anti-Viral software is not permitted by any unauthorised personnel, this should only be carried out under the authority of the IT Management Team.

SUPPORTING DOCUMENTS

Rundles.

The supporting document assets of Rundles include policies, information security procedures and work instructions, SLAs, disaster recovery plans, HR Procedures and business plans.

THE SERVICES

The service assets of Rundles include HVAC, ISP, electric power, firewall monitoring, and telecommunication services.

INTANGIBLE ASSETS

The intangible assets of Rundles include the company reputation, public image, client relationship, and company intellectual property.
All managers are directly responsible for implementing the Policy within their business areas, and for adherence by their staff.

It is the responsibility of each employee to do everything reasonable and within their power to ensure that the Policy is adhered to.

Changes to this Policy in response to changing operational, legislative, regulatory and contractual requirements will be made as necessary by the Information Security Manager.

The ISMS is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation is a part, and which has been designed in accordance with the requirements contained in ISO/IEC 27001:2017.

A SECURITY BREACH is any incident or activity that causes or may cause a breakdown in the availability, confidentiality or integrity of the physical or electronic information assets of the organisation. All information security incidents, actual or suspected, will be reported to and investigated by the Information Security Manager.

Signed: Amy Collins

Position: Managing Director
Date: 05th March 2023