Red Snapper Group

Information Security Policy

Title	Information Security Policy
Department	Security – Data Protection
Sector	RSG
Document Owner	Stuart Traynor – Chief Technology Officer
Data Classification	Public
Type	Controlled
Date Adopted:	November 2021
Date of Next Review:	November 2022

Version Control – Controlled Document

Issue Date	Version No.	Saved As	Owner	Changes Made
April 2017	1.0	Information_Security_Policy	Martin Jerrold	Draft version
June 2018	1.0	Information_Security_Policy	Jane Salmon	Document reviewed
August 2019	2.0	Information Security Policy v2	Jane Salmon	Document reviewed, Coversheet added, MD signature added
May 2020	3.0	Information Security Policy	Ryan Farmer	Document reviewed and realigned to strategic objectives
September 2021	3.1	Information Security Policy	Stuart Traynor	Revisions per ISO audit observations
November 2021	3.2	Information Security Policy Final v3.2	Stuart Traynor	Inserted watermark Took out Introduction paragraph
November 2021	3.3	Information Security Policy Final v3.3	Stuart Traynor	Inserted formal sign off subtitle 14.

Contents

1. Related Documents

All documents which constitute the information security management system (ISMS) may be accessed via shared drive, and are located at G:\Red Snapper Group\Compliance\1.2. ISO 27001 2013.

Additionally, policies and procedures within the ISMS that require staff review or understanding are made available through the employee document library within the Breathe HR system – https://www.redsnappergroup.breathehr.com. Here all staff receive bulletins informing them which documents they are required to read, and may confirm both their receipt and understanding of the documents.

2. Applicable Legislation

The information security management system is subject to statutory and regulatory requirements. One of its primary purposes is to satisfy the Group's obligations against this legislation:

- Computer Misuse Act 1990
- Copyright, Designs and Patent Act 1998
- Criminal Finances Act 2017
- Cyber Security Essentials Plus
- General Data Protection Regulation (EU) 2016/679
- ISO 27001: 2013
- ISO 9001: 2015
- Payment Card Industry Data Security Standard (PCI DSS) 3.2.1
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Telecommunications Regulations: Lawful Business Practice and Interception of Communications, 2000; and Data Protection & Privacy, Direct Marketing 1999
- UK Data Protection Act 2018
- UK Electronic Communications Act 2000
- The Human Rights Act 1998

3. Information Security Policy

The Red Snapper Group recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, The Red Snapper Group will facilitate the secure and uninterrupted flow of information, both within The Red Snapper Group and in external communications. The Red Snapper Group believes that security is an integral part of the information sharing which is essential to its commercial and operational endeavours and the policies outlined above are intended to support information security measures throughout The Red Snapper Group.

This policy is based on recommendations contained in ISO/IEC 27001:2013.

4. Definition

For the purposes of this document, information security is defined as the preservation of: confidentiality: protecting information from unauthorised access and disclosure; integrity: safeguarding the accuracy and completeness of information and processing methods; and availability: ensuring that information and associated services are available to authorised users when required.

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.

Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations

5. Objectives

In order to measure the success of the Group's ISMS and information security policies, a number of objectives have been set, and are located as per page 4 of this policy. These objectives are intended to be measurable on an ongoing basis so as to provide the opportunity to continually monitor the ISMS for effectiveness and suitability. These objectives shall be reviewed on a 6 monthly basis as part of Management Review Meetings to review their ongoing relevance and the Group's performance against them.

6. Protection of Personal Data

The Red Snapper Group holds and processes information about employees, job seeker, client information and other data subjects for administrative and commercial purposes. When handling such information, The Red Snapper Group, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the 2018 Act) and General Data Protection Regulation (EU GDPR 2016/679). Responsibilities under the data protection legislation are set out in the Data Protection Policy.
The Group recognize the importance of encryption in minimizing the risk of data loss, and utilise it through outsourced services to protect data in transit and at rest. This is facilitated through email security services from Mimecast and the cloud provider HTL UK. The minimum standard of encryption used is 256-bit AES. Encryption procedures and key management are handled by these third party suppliers.

7. Information Security Responsibilities

The Red Snapper Group believes that information security is the responsibility of all staff members. Every person handling information or using the business information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at The Red Snapper Group.

This Policy is the responsibility of the policy owner but will be formally reviewed and signed off by the Senior Management Team. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Information Security Management Representative and other designated personnel with security responsibilities in specified areas of The Red Snapper Group.

8. Information Security Education and Training

The Red Snapper Group recognises the need for all staff and other users of the businesses' systems to be aware of information security threats and concerns, and to be equipped to support. The business security policy in the course of their normal work. The ISMR shall implement a training program for each class of users and, at the behest of The Red Snapper Group's divisions and shall provide information and further training in information security matters to answer particular requirements.

9. Compliance with Legal and Contractual Requirements:

9.1 Authorised Use

The business IT facilities must only be used for authorised purposes. The Red Snapper Group may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

9,2 Monitoring of Operational Logs

The Red Snapper Group shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur (i) when required by and consistent with law; (ii) when there is reason to believe that a violation of law or of a business policy has taken place; or (iii) when there are compelling circumstances.

9.3 Access to The Business Records

In general, the privacy of users' files will be respected but The Red Snapper Group reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with the business policies and regulations, and to determine which records are essential for The Red Snapper Group to function administratively or to meet its legal obligations. Except in emergency circumstances, authorisation for access must be obtained from the Managing Director or their nominee, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation

9.4 Protection of Software

To ensure that all software and licensed products used within The Red Snapper Group comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts.

The Red Snapper Group will carry out audits from time to time to ensure that only authorised products are being used, and will keep a record of the results of those audits. Unauthorised copying of software or use of unauthorised products by staff or students may be grounds for disciplinary, and where appropriate, legal proceedings.

9.5 Virus Control

The Red Snapper Group will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of Group computers, including laptops, shall comply with best practice. All antivirus updates and scans are scheduled to occur automatically, although staff are expected to contact the IT Service Desk or compliance department in the event of notifications relating to infections or errors in the operation of the control.

9.6 Retention and Disposal of Information

All staff have a responsibility to consider security and data protection when disposing of information in the course of their work. Each division has established procedures and retention periods appropriate to the information held and processed by them, and the Group shall ensure that all staff are aware of these and their responsibilities for processing personal data.

Retention periods for the processing of personal data across the Group are as follows:

Brand	Personal data set	Type of Data Subject	Retention period	Onset event
Recruitment	CV file	Jobseeker	5 years	Registration
Recruitment	Financial data	Contractor	2 full tax years	End of employment
Recruitment	Compliance documentation	Contractor	2 years	End of employment
Learning	CV file	Trainer - jobseeker	5 years	Registration
Learning	Financial data	Trainer - contracted	2 full tax years	Commencement of employment
Learning	Compliance documentation	Trainer - contracted	2 years	Commencement of employment
Media	Contact information	Subscriber	3 years	Registration
Media	Contact information	Advertiser	3 years	Registration
Media	CV file	Job board user	5 years	Registration
Managed Services	Contact information	Jobseeker	5 years	Registration
Managed Services	CV file	Jobseeker	5 years	Registration
Managed Services	Compliance documentation	Contractor	2 years	End of employment
Managed Services	Financial data	Contractor	2 full tax years	End of employment
Managed Services	Evidence files	Suspects, witnesses	Duration of investigation	Commencement of investigation

After the above conditions are met, personal data is deleted where possible, or archived so as to be inaccessible to users. The latter of these occurs where a record that the data has been at some point processed is required, for example to provide an employment reference for a contractor. Deletions are conducted by the Data Protection Officer, utilising a proprietary tool which removes or archives personal data from all information systems (including RDB ProNet, websites, and mailing platform). En masse deletions are handled via SQL transaction statements. After each deletion type, sample records are tested to verify that the deletion or archiving has been successful.

10. Reporting

All staff, job seekers and other users should report immediately by email to itsupport@rsg.ltd or by telephone to the Computer Help Desk, any observed or suspected security incidents where a breach of The Red Snapper Group's security policies has occurred, any security weaknesses in, or threats to, systems or services.

Software malfunctions should be reported to the IT support team.

11. Business Continuity

The Red Snapper Group will implement, and regularly update, a business continuity management process to counteract interruptions to normal the business activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

12. Continual Improvement

The Group is committed to information security and its ISO 27001 accreditation as business-critical concerns. Utilising the ISMS objectives, risk management and opportunities for improvement, the Group intends to continually review the effectiveness of its ISMS and make improvements based on these. The Group is aware of the legislative requirement for continuous improvement of its ISMS and approach to information security management, and will conduct such reviews regularly in order to identify areas where this can be achieved. Strategically the Group has identified that it can broaden the scope of its ISO 27001 accreditation to include its offices outside of the currently in scope London HQ, and to roll this out across other brands, namely 3GS and Police Revision.

13. Review

This policy will be reviewed annually by the policy owner. Revisions, however, may be made throughout the year.

14. Formal Sign Off

This Policy has been formally reviewed and signed off by top management:

Martin Jerrold
Managing Director
Red Snapper Group

The End.