INFORMATION SECURITY POLICY

VERSION 1.10 JULY 2018

REED & MACKAY

CONTENTS

POLICY STATEMENT

The Board of Reed & Mackay recognises the significance of Information Security, and maintaining the highest standards of confidentiality, integrity and availability of internal, customer and supplier information is fundamental to its brand promise of *"Extraordinary Travel Management"*. Continuity of operations, provisions of facilities and levels of service is paramount and focuses on the "brand pillars" of *"Extraordinary Service"*, *"Considered Confidence"* and *"Deeper Understanding"*, while being underpinned by the remaining pillars of *Inspired Intelligence"* and *"Sharper Efficiency"*.

Reed & Mackay have created an Information Security Policy to set a clear direction for information security and demonstrate support for, and commitment to the management of information security throughout the company.

The aims of the policy are:

- To manage the risks to service, financial performance, client confidence, rights and freedoms of individuals, or other areas of the business which may result from a failure in information security
- To identify and support improvements to the Information Security Management System
- To comply with all relevant regulatory, contractual and legislative information security requirements and obligations

Information Security Policy awareness is incorporated in our induction process and our annual mandatory compliance training for all employees, and more detailed Information Security objectives are documented by the Governance, Risk Management and Compliance department.

Information Security is managed through a stringent set of controls, including policies, processes, procedures, software and hardware functions that constitute our Information Security Management System (ISMS). These controls are monitored, reviewed and, where necessary, improved to ensure that specific security and business objectives are met. The ISMS is managed in conjunction with Quality, Business Continuity and Environmental Management Systems and incorporates the applicable statutory, regulatory and contractual requirements. Reed & Mackay is committed to continually improving of the Information Security Management System across all areas of the business. Like all responsible companies Reed & Mackay recognises the importance of protecting its stakeholders from disruption caused by information security incidents.

POLICY SCOPE & COMPLIANCE

This policy applies to all Reed & Mackay locations and staff and to all information and information systems, on which Reed & Mackay depends. All staff are responsible for complying with this policy. Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

The prevailing version of the Statement of Applicability (SOA), referenced in the Information Security Management System, identifies the ISO/IEC 27001 controls applicable to Reed & Mackay. At present no controls are excluded.

The Resilience Working Group is responsible for identifying relevant statutory, regulatory and contractual requirements that the company must adhere to.

Through compliance to the standard for Information Security Management ISO/ IEC 27001, Reed & Mackay will demonstrate confidence, integrity and credibility both internally and externally.

DEFINITIONS

ISO/IEC 27001 defines Information Security as including:
"…three main dimensions: confidentiality, availability and integrity"

and as involving:

"…the application and management of appropriate security measures that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimising impacts of information security incidents"

Confidentiality
Ensuring that information is accessible only to those authorised to have access.

Integrity
Safeguarding the accuracy and completeness of information and processing methods.

Availability
Ensuring that authorised users have access to information and associated assets when required.

ISO/IEC 27001 defines an Information Security Management Systems (ISMS) as:
"… policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets"

The information security management system seeks to preserve the confidentiality, integrity and availability of information by applying a risk management process; giving confidence to interested parties that risks are adequately managed.

POLICY GOVERNANCE, REVIEW & REVISION

The following table identifies who within Reed & Mackay is Accountable, Responsible, Informed or Consulted with regard to this policy.

RESPONSIBLE	Head of Governance, Risk Management & Compliance, Information Security Lead
ACCOUNTABLE	Group Chief Financial Officer
CONSULTED	Group Chief Financial Officer, Group Chief Technology Officer
INFORMED	All employees, all contractors, all other 3rd party organisations with any form of access to Reed & Mackay's information and information systems.

This policy will be reviewed as it is deemed appropriate, but no less frequently than annually. Policy review will be undertaken by the Group Chief Financial Officer, Group Chief Technology Officer, Head of Governance, Risk Management & Compliance and Information Security Lead.

ROLES & RESPONSIBILITIES

Information security is a responsibility of all staff. The ultimate responsibility for information security lies with the Group Chief Financial Officer but this responsibility is discharged through the designated roles of Head of Governance, Risk Management & Compliance and Information Security lead.

The Head of Governance, Risk Management & Compliance is responsible for information risk within Reed & Mackay and advises the Board on the effectiveness of information risk management across the organisation.

Information Security Lead has primary responsibility for information security management within Reed & Mackay and acts as the central point of contact on information security for both staff and external organisations. The Information Security Lead holds relevant qualification/certifications in Information Security.

Directors and Heads of Department are directly responsible for implementing the Security Policy within their business areas and for adherence by their staff.

It is the responsibility of each employee to adhere to the Security Policy. Failure to do so may result in disciplinary action.

All staff have a responsibility for Information Security; ensuring that they follow relevant company policies, processes and procedures and have a general awareness of importance of Information Security and the potential risks; reporting any potential ISMS weaknesses to the appropriate Head/Director of Department, and then with the Governance, Risk Management & Compliance department.

All staff also have a responsibility for reporting any Information Security related events or incidents to SecurityIncident@reedmackay.com as soon as they become aware of, or suspect, their occurrence, identifying when the incident took place, providing enough information for an investigation to start.

AWARENESS, TRAINING & QUERIES

The Information Security policy is readily accessible internally via the company intranet, and can be provided upon request to external parties.

Information Security awareness is incorporated in the induction process and delivered on an on-going basis through a number of communication methods, including:

- On-line training (FUSE), including mandatory annual compliance training
- Intranet awareness page
- Meetings and Conferences
- Emails

To discuss any matter relating to the Information Security Policy, contact your Head/Director of Department, a member of the Resilience Working Group or the Governance, Risk Management & Compliance department.