Risk Assurance Management Ltd

Information Security Policy

Revision 2.0
May 2018

Chancery House, Leas Road,
Guildford, Surrey GU1 4QW
Tel: 0370 7200 780 Fax: 0370 7200 781
Email: group.risk@ram-ltd.co.uk Web: www.ram-ltd.co.uk

Contents

1. Introduction

Risk Assurance Management (RAM) is a registered Data Controller with the Information Commissioner's Office (ICO). The continued confidentiality, integrity and availability of information systems underpin the operations of RAM. This document outlines the guiding principles and responsibilities followed by RAM to ensure the security of information. Supporting policies, codes of practice and guidelines provide further details (see 4. Supporting Polices and Guidelines).

1.1. Objectives

The objectives of this policy are to:

- Ensure that the information systems that RAM manages are protected from security threats and to mitigate risks that cannot be directly countered.
- Ensure that all RAM employees are aware of and able to comply with relevant UK and EU legislation.
- Ensure that all employees are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.
- Ensure that all employees are aware of and are able to comply with this policy and other supporting policies.
- Safeguard the reputation and business of RAM by ensuring its ability to meet its legal obligations and to protect it from liability or damage through the misuse of its IT facilities.
- Ensure timely review of policy and procedure in response to legislation, changing security threats and other factors to improve ongoing security.

1.2. Scope

The Information Security Policy applies to, and will be communicated to all employees of RAM, and where applicable any third party contractors working on the company's behalf.

The policy covers any information held by RAM in either electronic or paper form.

2. Policy

2.1. Awareness and Communication

- All employees will be informed of the policy and all supporting policies when they join the company.
- All employees will receive annual training on information security and the protection of data.
- All employees will be required to read and confirm their understanding of the policy on an annual basis, or in the event of changes to the underlying policies.

2.2. Principles

The following principles provide a framework for the security and management of RAM's information and information systems.

1. Information should be classified in line with RAM's data protection framework, and in accordance with any legislative, regulatory or contractual requirements that might increase the sensitivity, handling or security requirements.
2. All employees must handle information appropriately in accordance with its classification level.
3. Information should only be available to those with a legitimate need for access.
4. Information will be protected against unauthorised access and processing.
5. Information will be protected against loss and corruption.
6. Information will be disposed of securely and in a timely manner with measures appropriate for its classification.
7. Breaches of policy must be reported by anyone aware of the breach in a timely manner to RAM's Data Controller.

2.3. Legal and Regulatory Obligations

RAM staff must adhere to all current UK and EU legislation as well as regulatory and contractual requirements.

2.4. Third Parties

RAM will ensure that data held by a third party is held within the European Economic Area (EEA), and that appropriate security, procedures, controls and notification processes are in place to protect that data.

2.5. Information Classification

The following table provides a summary of the information classification levels which are part of RAM's Data Protection Policy. Some data assets may appear in multiple categories. The strongest levels of control/restrictions will apply where this is the case. Individuals should think carefully before disclosing any 'sensitive' information to third parties or external agencies.

Category	Definition
Sensitive Individual	Information that is linked to or could be used to identify an individual.
Internal Financial Sensitive	Information of a financial nature that is deemed internally sensitive.
External Financial Sensitive	Information of a financial nature that is deemed externally sensitive.
Commercial Sensitive	Information that is commercially sensitive.
Non Sensitive	Information that may or may not be generally available through our website or general publications but is not deemed confidential.

2.6. Incident Handling and Notification

If a member of staff is aware of an information security incident they must report it to RAM's Data Controller as soon as is practicably possible.

2.7. Review

The Information Security policy and associated internal policies shall be reviewed on a quarterly basis and updated to ensure they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

3. Responsibilities

3.1. All Members of Staff

All members of staff must comply with IT policies and procedures, and should only access systems and information which they have a genuine business need to view or process.

Members of staff should;

- Always use a strong password and change it regularly, and immediately if they believe it has been compromised. Report any such incident to the Data Controller.
- Always report any loss or suspected loss of data.
- Never record or share logon credentials and passwords.
- Never open suspicious email attachments or click on suspicious links.
- Always reports suspicious emails or suspicious activity to the IT department.
- Always encrypt sensitive (individual, financial or commercial) information if sent via email or removed from RAMs premises.
- Always verify the authenticity of any external requests for information before making that information available.

3.2. Data Controller

The Data Controller is responsible for collating, evaluating and reporting any information security breaches internally and to the relevant regulatory bodies and/or affected individuals.

3.3. IT Department

The IT department is responsible for securing, maintaining, backing up, auditing, proactively monitoring and recovering RAMs computer systems in accordance with company policy.

3.4. Data Protection Committee

The committee is responsible for evaluating and updating policy in the event of any changing security threats, technical requirements, and legal or regulatory changes. The committee will review policy on a quarterly basis and will meet on an ad hoc basis in response to any specific requirements for review or change.

4. Supporting Polices and Guidelines

The following **internal only** policy and guideline documents support and reinforce this policy. All staff are required to read, understand and acknowledge these polices and guidelines.

4.1. Data Protection Policy

The company's internal data protection policy gives details on;

- Information classification, storage, handling and retention.
- Security of premises, computer systems and the acceptable use of company equipment and services such as email and internet, together with restrictions on computer use, web sites, services and personal devices.
- Compliance monitoring and auditing.
- Verification and protection of data shared with third parties.
- The use of company laptops, telephones and mobile devices.
- Secure disposal of hardware, software and data assets.
- Password and Account management.
- Protection of systems through regular updates, antivirus and firewalls.
- What may constitute a data or policy breach, who this should be reported to, the relevant escalation procedures and how RAM notifies those affected.

4.2. Acceptable Use Policy

What constitutes acceptable use of company equipment and related services.

4.3. Password Policy

Best practice for password creation, usage and management.

4.4. Disaster Recovery Plan

The documented process to follow to recover services in the event of a disaster.

4.5. Financial Conduct Authority (FCA)

RAM is regulated by the FCA and follows all FCA guidelines and recommendations in relation to data protection.