Information Security Policy

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of Moore Insight (the Company). Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for the Company to recover.

This information security policy outlines the Company's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Company's information systems and should be read in conjunction with all IT and Company Policies, codes of practice, procedures and guidelines provide further details.

The Company is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data.

The Company is committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of information security standard ISO 27001. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Company is responsible.

2. Objectives

The objectives of this policy are to:

- Provide a framework for establishing suitable levels of information security for all the Company's information systems.
- Provide a safe and secure information systems working environment for staff, contractors and any other authorised users.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle, including satisfying the information security requirements of third-party data providers and comply with all current and relevant UK and EU legislation.
- Protect the Company from liability or damage through the misuse of its IT facilities.
- Maintain data and other confidential information provided by clients at a level of security commensurate with its classification (see Data Classification policy), including upholding any legal and contractual requirements around information security.
- Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

3. Scope

This policy is applicable to, and will be communicated to, all staff, contractors, other members of the business and other third parties who interact with information held by the Company and the information systems used to store and process it.

4. Definitions

- Data Protection - The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.
- Data - The Company's Data, for the purposes of this policy, is data owned, processed or held by The Company, whether primary or secondary.

- Least Privileged - The principle of Least Privilege (POLP) is the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs.
- Personal Data - (which is classified as 'Confidential') means any information relating to an identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. An example of Personal Data would be someone's address which we hold.

5. Policy

Information Security Principles

The following information security principles provide overarching governance for the security and management of information at the Company.

Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements and the Companys Data Classification Policy (see Legal and Regulatory Obligations).

Staff with particular responsibilities for information (see Responsibilities) must:

- Ensure the classification of that information.
- Handle that information in accordance with its classification level.
- Abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.

All users covered by the scope of this policy (see Scope) must handle information appropriately and in accordance with its classification level.

Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on the basis of need to know and least privilege (see Definitions).

Information will be protected against unauthorised access and processing in accordance with its classification level.

Breaches of this policy must be reported (see Incident Handling).

Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits.

Any explicit Information Security Management Systems (ISMSs) run within the Company will be appraised and adjusted through the principles of continuous improvement, as laid out in ISO27001.

6. Legal and Regulatory Obligations

The Company has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

- A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided (see Appendix).

7. Information Classification

The Company has adopted a Data Classification Policy. The following list provides a summary of the information classification levels that have been adopted by the Company and which underpin the 8 principles of information security defined in this policy.

- Personal
- Public
- General
- Confidential
- Highly Confidential

8. Suppliers

All the Company's suppliers will abide by this Information Security Policy. This includes when accessing or processing the Companys assets, whether on site or remotely when subcontracting to other suppliers.

9. Compliance, Policy Awareness and Disciplinary Procedures

The loss or breach of confidentiality of personal data is an infringement of the Data Protection Act (1998) and the EU General Data Protection Regulation (2018), contravenes The Company's Data Protection Policy, and may result in the loss of business, financial penalties, criminal or civil action against the Company.

10. Incident Handling

If a staff member, contractor or third party is aware of an information security incident then they must report it to the IT Security Team at Security@moore-insight.co.uk or telephone 020 7952 4691. Any information will then be passed to the Incident Response Team for investigation and action.

If appropriate, employees of the business may also use the Companys Whistle Blowing Policy.

11. Supporting Policies, Codes of Practice, Procedures and Guidelines

Supporting policies have been developed to strengthen and reinforce this policy. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on the Company's Intranet.

Supporting Policies Include:

- Incident Response Policy & Plan
- IT Policy
- Control of Documents and Records
- Privacy Policy & Notice
- Data Protection Policy

12. Review and Development

This policy, and its subsidiaries, shall be reviewed by the Operations Team and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional policies may be created to cover specific areas.

The Operations Director will determine the appropriate levels of security measures applied to all new information systems.

13. Responsibilities

All members of staff, contractors and third-party suppliers on Company projects will be users of the Company's information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. Breaching this policy could result in disciplinary or legal action.

To report policy contraventions, please see Incident Handling.

14. Data Owners / Guardians

Users of the Company's systems will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

Heads of Departments

Responsible for the security of information produced, provided or held in the course of carrying out fee earning work. This includes:

- Ensuring that data is appropriately stored.
- That the risks to data are appropriately understood and either mitigated or explicitly accepted.
- That the correct access rights have been put in place, with data only accessible to the right people.
- Ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

Support Team Managers

Responsible for the information systems (e.g. HR/ Finance) both manual and electronic that support The Company's work.

Departmental Managers / Line Managers

Responsible for specific areas of The Company's work, including all the supporting information and documentation that may include professional documents / working papers / contracts.

Operations Director

Responsible for:

- Physical aspects of security and will provide specialist advice throughout the Company on physical security issues.
- This and subsequent information security policies.
- Providing specialist advice throughout the business on information security issues.
- Advising on and recommending information security policies across the business, assessing information security risks and identifying and implementing controls to risks.

A. Appendix

The Computer Misuse Act 1990

https://www.legislation.gov.uk/ukpga/1990/18/contents

Data Protection Act 1998

https://www.legislation.gov.uk/ukpga/1998/29/contents

General Data Protection Regulation

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Contacts

If there are any questions regarding this policy or if you would like to contact us, please send an email to Info@moore-insight.com.

Moore Insight
St. James House, Vicar Lane, Sheffield, S1 2EX
T +44 (0)20 7952 4690
www.moore-insight.com