MK Clairvoyants (includes Healing the Soul Training)

Information Protection Policy

Policy Statement

MK Clairvoyants will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will always be maintained.

Purpose

Information is a major asset that MK Clairvoyants has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow, and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality, and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at MK Clairvoyants. The policy specifies the means of information handling and transfer within the Business.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for MK Clairvoyants purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

MK Clairvoyant recognises that there are risks associated with users accessing and handling information to conduct official business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents
- inadequate destruction of data,

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Policy compliance

If any user is found to have breached this policy, they may be subject to MK Clairvoyants disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Matt or Kirsty

Policy Governance

The following table identifies who within MK Clairvoyants is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Matt Grogan
Accountable	Matt and Kirsty Grogan
Consulted	Matt and Kirsty Grogan
Informed	All members, owners and trainees.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Matt and Kirsty

References

The following MK Clairvoyants policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Remote Working Policy.
-

The following MK Clairvoyants policy documents are indirectly relevant to this policy

- Privacy Notice
- Data Protection Policy

Key Business

- The Business must draw up and maintain inventories of all-important information assets.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until Matt and Kirsty are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- PROTECT and RESTRICTED information must not be disclosed to any other person or organisation via any insecure methods including paper-based methods, fax and telephone.
- All information of a sensitive nature should not be sent via email unless it is a guaranteed encrypted site such as GCSX

Applying the Policy

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

MK Clairvoyants must draw up and maintain inventories of all-important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management, and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

Personal information

This is any information about any living, identifiable individual. The business is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998.

PROTECT or RESTRICTED information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with the persons permission

Any sharing or transfer of information with other organisations must comply with all Legal, Regulatory and Policy requirements. This must be compliant with the Data Protection Act 2018, The Human Rights Act 2000, and the Common Law of Confidentiality.

Signed: M. GROGAN / K. GROGAN Date: 1/5/2020