THE DATA CREW

ISMS INFORMATION SECURITY POLICY

ISO 27001 ISMS Polices & Procedures

Abstract

This standard ensures that The Data Crew complies with the ISO 27001:2013 security principles

THE DATA CREW

Didsbury Business Centre
137 Barlow Moor Road
Didsbury
Manchester
M20 2PW

ISMS Information Security Policy

Policy Overview

This policy is based on ISO 27001:2013 the recognised international standard for information security. This standard ensures that the organisation complies with the following security principles:

- **Confidentiality**: all sensitive information will be protected from unauthorised access or disclosure;
- **Integrity**: all information will be protected from accidental, malicious and fraudulent alteration or destruction; and,
- **Availability**: Information services will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

The Data Crew is committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions.

Compliance with The Data Crew security policies and procedures is mandatory for all personnel.

The Chief Executive Officer (CEO) approves this policy. The Information Security Forum (ISF) has the responsibility for ensuring that the policy is implemented and adhered to.

The security policy confirms The Data Crew commitment to continuous improvement and highlights the key areas to effectively secure its information.

Policy Detail

Senior Management Team Responsibilities' and commitment

The Senior Management Team are committed to satisfy all applicable requirements within this policy and to the continual improvement of the ISMS, and therefore have established this information security policy so that:

- it is appropriate to the purpose of the organisation;
- it includes information security objectives and provides the framework for setting continual information security objectives;

This information security policy shall be available as documented information; be communicated within the organisation; and be available to interested parties, as appropriate.

Leadership and commitment

Top management will continue to demonstrate leadership and commitment with respect to the information security management system by:

- ensuring the information security policy and information security objectives are established and are compatible with the strategic business direction of the organisation;
- ensuring the integration of the information security management system requirements into the organisation's processes;
- ensuring that the resources needed for the information security management system are available;
- communicating the importance of effective information security management and of conforming to the information security management system requirements;
- ensuring that the information security management system achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the information security management system;
- Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Information Security Objectives

Information security objectives have been established and are compatible with the strategic direction of the organisation, the key objective is to work in line with the sections of the best practice standard ISO 27001:2013 detailed below.

Furthermore security objectives will be set by management as an ongoing task and at ISMS Management Review Meetings and an Information Security Objectives Policy will be produced and implemented as part of the ISMS.

Management Objectives for Information Security will be continually set and monitored to ensure they are achieved.

The Data Crew will seek to continually improve the information security management system in line with a PLAN-DO-CHECK-ACT to improve process embedded within its ISMS.

Organisation of Information Security.

The importance attached to information security within The Data Crew is demonstrated by the existence of the Information Security Forum; the function of the Information Security Forum is outlined below;

- reviewing and progressing strategic security issues;
- establishing relationships outside of The Data Crew with other security advisers;
- assessing the impact of new statutory or regulatory requirements imposed on The Data Crew;

- monitoring the effectiveness of the Information Security Management System ("ISMS") (e.g. from the results of Internal Audit reports and Security Incident Reports);
- recommending & endorsing changes to the ISMS;

The Information Security Forum meets regularly to address the above activities in order to assure the continuing effectiveness of The Data Crew ISMS. The review process is defined in the **ISMS Information Security Forum Management Review Policy**.

Human Resource Security

All employees must sign up to the Staff Handbook which requires them to work in accordance with all policies and procedures which includes information security specific requirements. Furthermore an 'Acceptable Use Policy' ensures that employees are made aware that they are required to follow best practices regarding information security established by The Data Crew. There is also a procedure for all employees that leave The Data Crew (including temporary and contract employees) to disable their network account and recover all items of property.

All new employees (permanent, temporary and contractors) must be trained on procedures in the areas described above as part of their induction programme. Ongoing training must be provided in the form of a programme of regular updates and training sessions by the Information Security Forum.

Asset Management

The Data Crew information must be classified according to its sensitivity and an information owner assigned. The IT Team will maintain an information asset inventory which is also updated periodically, according to its risk profile and protected accordingly.

Access Control

Employees must be aware of and must follow a number of controls and procedures, which exist to limit access to confidential information. The IT Team are responsible for both establishing and maintaining robust logical access controls. An **ISMS Physical & Environmental Security Policy** for the Office and Data Centre's must be in place and complied with by all employees and third parties.

Cryptography

Where cryptographic controls are employed by The Data Crew a policy on the use of cryptographic controls for protection of information must be developed and implemented. Please refer to the **ISMS Cryptographic Use and Control Policy.**

Physical and Environmental Security

Staff must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include;

- building and individual alarm systems

- restricted access to the building and further restricted access within it
- secure lockers, drawers, safes and storage, fireproof storage
- secure offsite backups and archiving
- clear desk policy
- clear screen policy

Operations Security

The Data Crew will ensure correct and secure operations of information processing facilities.

Communications Security

Staff must be aware that the use of technology and communications are established, controlled and managed by the IT Team. The department is responsible for ensuring that the appropriate security measures and processes are in place. The Data Crew will ensure that security around the network, mobile and remote working are adequately protected.

System Acquisition, Development and Maintenance

The Development Team must ensure that the appropriate information security processes are included in all projects. Please refer to the **ISMS Secure Development & System Engineering Policy**.

Supplier Relationships

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets must be agreed with the supplier and documented.

Information Security Incident Management

Security incident management records must be centrally maintained, updated and monitored via the Case Management System. All employees must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to.

The responsibility for the oversight of breaches of technical and physical security rests with the Chief Information Security Officer (CISO).

Information Security Aspects of Business Continuity Management

The organisation must ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

Compliance

The Data Crew must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

The Data Crew must take technical and organisational measures to protect personal data against accidental or unlawful destruction, or accidental loss or alteration, and unauthorised disclosure or access. In particular The Data Crew takes measures that are intended to ensure that:

- Anyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained to do so; and
- Everyone managing and handling personal data is appropriately supervised.

Review

This document must be reviewed at least annually by its 'Document Owner'. The Document Owner must ensure the correct version number is applied to the document once the review has taken place.

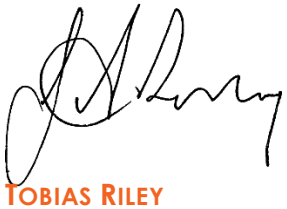
Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Compliance

The document owner or a nominated proxy will conduct regular compliance reviews of this document using the following template to record evidence of the review, along with any corrective or preventative actions that have been agreed as a result of non-compliance occurrences.

Signed



TOBIAS RILEY
CEO AME FUTURES LIMITED (THE DATA CREW)

Version Control

Version	Date	Author	Reviewed By	Approved By	Summary of Change
1.0	01/06/2016	Toby Riley	ISF	CISO	Initial Version.