



Information Security Management System Manual

DOCUMENT CLASSIFICATION	Protected
DOCUMENT REF	ISMS-DOC-05-1
VERSION	1
DATED	25 June 2024
DOCUMENT AUTHOR	Adrian Harte
DOCUMENT OWNER	IT Manager – Adrian Harte


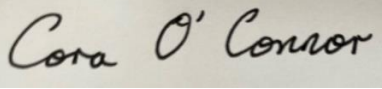
Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	26/05/2024	Adrian Harte	Initial draft
1.1	03/06/2024	Steering group	Review and update
1.2	05/06/2024	Steering group	Pre-final review
V1	25/06/2024	Adrian Harte	Final Approval – Adrian Harte
V1	25/06/2024	Cora O'Connor	Final Approval - Cora O'Connor

Distribution

NAME	TITLE
Kirby Group Employees	

Approval

NAME	POSITION	SIGNATURE	DATE
Adrian Harte	IT Manager		25 th June 2024
Cora O'Connor	Compliance Lead		25 th June 2024

Contents

1	Introduction.....	4
2	ISMS manual.....	5
2.1	Top management leadership and commitment.....	5
2.2	Framework for setting objectives.....	5
2.3	Roles and responsibilities.....	5
2.4	Continual improvement of the ISMS.....	5
2.5	Approach to managing risk.....	5
2.6	Human resources.....	6
2.7	Auditing and review.....	6
2.8	Documentation structure and policy.....	6
2.9	Control of records.....	6

1 Introduction

This manual defines how an Information Security Management System (ISMS) will be set up, managed, measured, reported on and developed within Kirby Group.

While it does not give any absolute guarantees of security, an ISMS can contribute significantly towards keeping our information safe and delivering many of the following benefits to Kirby Group:

- Significantly reduced risk of reputational damage, legal penalties or business revenue due to loss of sensitive or Personally Identifiable Information (PII)
- Peace of mind assurance to our customers, staff, board members, suppliers and other interested parties that their data is secure
- An ability to bid for and respond to tenders for business where ISO/IEC 27001 certification is a requirement
- A public demonstration that Kirby Group takes information security seriously
- Internal and external recognition of the quality of the information security controls in place
- Year-on-year improvement in the security of our (and our customers) information assets as a result of the continuous improvement aspects of the standard
- A strong move away from reactive fire-fighting towards proactive security incident reduction
- Better alignment of information security controls with the needs of the business and our customers through regular review meetings with interested parties
- Better perception and awareness of information security issues within the business, our customers and the internal IT user population
- An improved ability to manage information security breaches if they do occur, so reducing reputational damage and limiting business impact to us and our customers

The International Standard for Information Security, ISO/IEC 27001, is a development of the earlier British Standard, BS 7799 and was first published in 2005. This standard defines the requirements for an ISMS based on internationally recognized best practice.

Kirby Group has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

2 ISMS manual

2.1 Top management leadership and commitment

Commitment to information security extends to senior levels of the organization and will be demonstrated through this *ISMS Manual* and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and relevant issues are identified through the audit programme and management processes. Management review can take several forms including departmental and other management meetings.

The [Information Security Manager] shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation and fulfilment of information security requirements
- Implementation, management and improvement of risk management processes
- Integration of operational processes, procedures and controls
- Compliance with statutory, regulatory and contractual requirements
- Reporting to top management on performance and improvement

2.2 Framework for setting objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This framework is documented in the *Information Security Policy*.

2.3 Roles and responsibilities

Within the field of information security, there are several management roles that correspond to the areas defined within the scope set out above. In a larger organization, these roles will often be filled by an individual in each area. In a smaller organization these roles and responsibilities must be allocated between the members of the team.

Full details of the responsibilities associated with each of the roles and how they are allocated within Kirby Group are given in a separate document *Information Security Roles, Responsibilities and Authorities*.

It is the responsibility of the [Information Security Manager] to ensure that employees and contractors understand the roles they are fulfilling and that they have appropriate skills and competence to do so.

2.4 Continual improvement of the ISMS

Kirby Group policy regarding continual improvement of the ISMS is described in the *Information Security Policy*.

2.5 Approach to managing risk

Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of information security objectives will be assessed and reviewed on a regular basis
- Information security and IT service continuity risk assessments
- Assessment of the risk of changes via the change management process

- As part of major projects to achieve business change e.g. new computer systems and services

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

A risk assessment process will be used which is line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security. This is documented in *Risk Assessment and Treatment Process*.

From this analysis, a risk assessment report will be generated followed by a risk treatment plan in which appropriate controls will be selected from the reference list in Annex A of the ISO/IEC 27001 standard.

2.6 Human resources

Kirby Group will ensure that all staff involved in information security are competent based on appropriate education, training, skills and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within Kirby Group. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records will be kept by the HR Department to document individual skill levels attained.

2.7 Auditing and review

Once in place, it is vital that regular reviews take place of how well information security processes and procedures are being adhered to. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures
2. Internal audit reviews against the ISO/IEC 27001 standard (and accompanying codes of practice) by the Kirby Group Internal Audit Team
3. External audit against the standard by a Registered Certification Body (RCB) in order to gain and maintain certification

Details of how internal audits will be carried out can be found in *Procedure for Internal Audits*.

2.8 Documentation structure and policy

All information security policies and plans must be documented. Details of documentation conventions and standards are given in the *Procedure for the Control of Documented Information*.

Several core documents will be maintained as part of the ISMS. They are uniquely numbered, and the current versions are tracked in the ISMS Documentation Log.

2.9 Control of records

The keeping of records is a fundamental part of the ISMS. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are defined in the document *Procedure for the Control of Documented Information*.