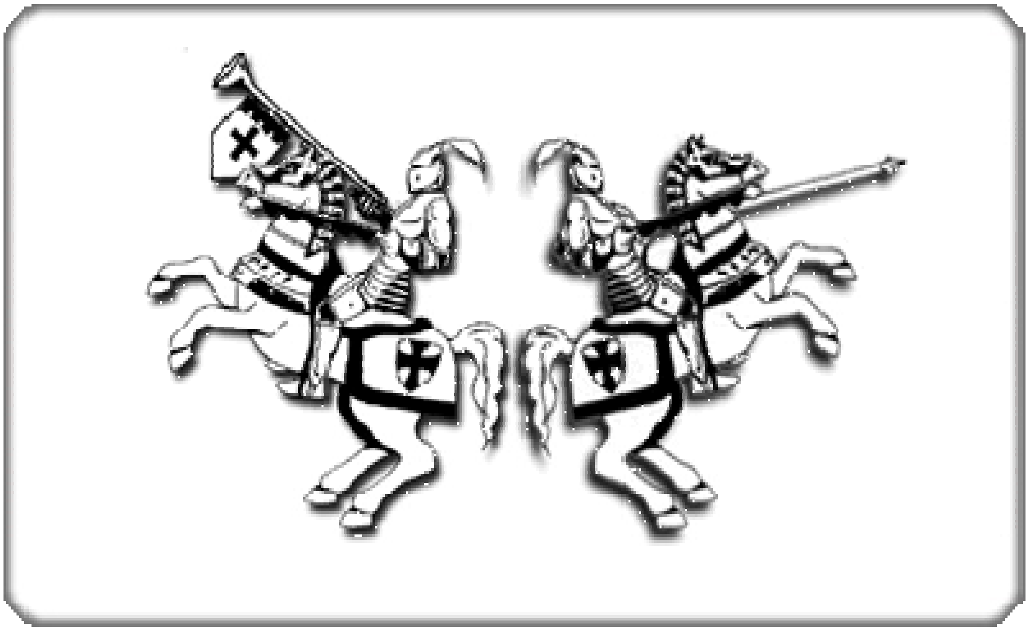
INFORMATION SECURITY MANUAL

THE KNIGHTS Inc.



NOTES:

The manual is intended to conform to the minimum requirement of ISO 27001:2013 with some minor additions.

More work required to finalise

Contents:

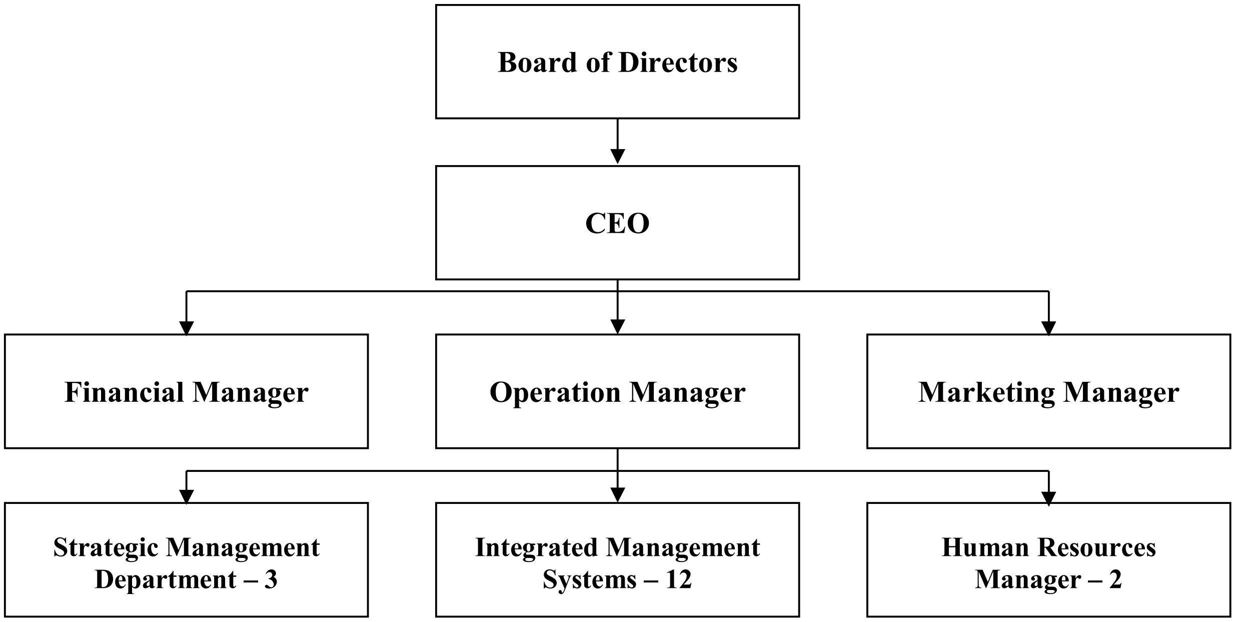
CONTENTS

1 - Profile

The Knights Inc. is a consultancy company providing consultancy services in strategic management, change management, human resources management and development of integrated management systems.

The Head Quarters of the Company are located in an administrative building in the center of town X. The Head Quarters comprise the offices of the CEO, those of the respective managers and the Strategic Management Department. The company has a branch office in the town of Z. The branch office hosts the Integrated Management Systems and the Human Resources Management Department. It is located in an administrative building. The company located in the neighboring offices has an operating ISMS.

2 - Organization Chart


Board of Directors
CEO
Financial Manager
Operation Manager
Marketing Manager
Strategic Management Department – 3
Integrated Management Systems – 12
Human Resources Manager – 2

CEO – He/She is responsible for the overall management and planning of the activities of *The Knights Inc.;* resource planning, holding of ISMS Management Reviews. The CEO, occupying the position at present, has been promoted to this position by the Board of Directors after 7 years in the company as an Operation Manager.

- **Financial Manager –** evaluation of investment projects, management of assets, management of the accounting system, participates in the ISMS Management Reviews.
- **Marketing Manager –** plans and implements the marketing strategy of the company, public relations; participates in the ISMS Management Reviews.
- **Operation Manager –** responsible for the day-to-day planning and management of the company's activities, general administration, human resources; participates in the ISMS Management Reviews; responsible for the supply, installation and maintenance of the equipment; application of security procedures.

The Operation Manager is responsible for the provision of information security and the operation, control and improvement of the Information Security Management System (ISMS)

3 – Reference

The following terms and definitions have been used in the Manual:

- **Availability –** ensuring that authorized users have access to information and associated assets when required.
- **Confidentiality –** ensuring that information is accessible only to those authorized to have access.
- **Integrity –** safeguarding the accuracy and completeness of information and processing methods.

- **Information Security –** security preservation of the confidentiality, integrity and availability of information.

- **Statement of Applicability –** document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment process.

4. - Information Security System

General

The Knights Inc., has established, implemented, operates and continually improves a documented ISMS in the context of its overall business activities and risks. In compliance with the requirements of ISO 27001:2005 and ISO 27002:2005, the process for the establishment and implementation of the system is based on the PDCA cycle.

Establishment and Management of the ISMS

Scope

The ISMS of *The Knights Inc*. covers all the activities of the company related to the reception, creation, processing, retention, archiving and transmitting of information. The ISMS covers the activities of the company within the limits of the company's office, as well as the relations with external organization. Through the establishment and the management of the system the management aims at the preserving of all the information assets of the organization and the business continuity processes.

The ISMS is established in compliance with ISO 27001:2013 and ISO 27002:2013, as well as with all applicable legal requirements.

Policy

The top management of *The Knights Inc*., is committed to the preserving of the confidentiality, integrity and availability of all the information assets of the organization in order to maintain and improve the competitive edge, cash flow, profitability, legal compliance and positive commercial image of the organization. The ISMS of the organization has been developed on the basis of the risk assessment performed, in which the best practices and methodologies known, as well as the experience of the company in the sphere of information security, have been employed.

The management of The Knights Inc. is committed to adopt and implement the following guiding principles with respect to information security:

- Incorporation of the company to best global principles in information security;
- Providing the resources necessary for technical innovation, improve technology and quality in the performance of ISMS;
- Ensure effective organization and management of the enterprise;
- Management of significant risks, threats and vulnerabilities in a manner consistent with applicable legal and other requirements;
- Ensure information security compliant working conditions in accordance with applicable regulatory requirements to the staff, service facility and persons residing within the organization in connection with their duties;
- Update applicable regulatory requirements for information security management;
- Achieve and maintain information security education, training, and motivation of staff and persons associated with identified information security internal and external issues;
- Provision of high discipline and personal responsibility of personnel of the enterprise for performance, information security controls and compliance with legal and other requirements for achieving information security;
- Implementation of effective and compliant links and relationships with suppliers and subcontractors.

Management of The Knights Inc. is confident that the implementation of information security policy, is possible only by maintaining and improving an ISMS, and in accordance with ISO 27001:2013. We are committed to satisfy all applicable requirements, and work towards improvement of the ISMS. To implement the policy, management will work to achieve the following GENERAL OBJECTIVES:

1. Continuously increase the market share of executed consultancy work;
2. Increasing the efficiency of business processes in the organization;
3. Providing conditions for process management in the organization in accordance with the requirements for information security management, regulatory and other requirements;
4. Increasing the competence and professionalism of staff in the work;
6. Continuously increase the satisfaction of investors / customers.

All the employees of the company are expected to understand and follow this policy and the ISMS procedures.

The management has approved the information security policy and is committed to review its adequacy at planned intervals or at least annually.

Approach to Risk Assessment

The organization has established and used an approach for risk assessment, which estimates the risks on the basis of probable loss incurred by a certain event and the probability of its occurrence. A three level categorization of the probable losses has been established. After the risk assessment actions are undertaken for the elimination, reduction or transfer of risks to other organizations. **(See IS Doc 05)**

Risk Identification

A methodology for the classification of all the information has been used, which was approved by the management, the "owners" of the assets have been identified. The threats to the assets and the vulnerabilities, as well as the impacts that losses of confidentiality, integrity and availability may have on the assets have also been identified. **(See IS Doc 05)**

Risk Assessment

The organization has assessed the business harm that might result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability to the assets. The realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented have been assessed.

The levels of the risks identified have been estimated, the acceptable risks have been determined as well as those requiring treatment. The results have been documented in a Risk Assessment Report **(IS Doc 05)**. A plan for regular review and re-assessment has been developed. **(See IS Doc 05)**

Risk Treatment

The organization has developed a Risk Treatment Plan **(IS Doc 06)**. Possible actions depending on the risk assessment have been identified for the purposes of risk treatment. The actions undertaken include (See IS Doc 05) :

- Applying appropriate controls
- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance
- Avoiding risks
- Transferring risks to external organizations

Control Objectives, Controls and Risk Treatment

Based on the results of the risk assessment the following control objectives and controls have been selected from Annex A of the standard – **see IS Doc 06**

Statement of Applicability

This Statement of Applicability has been adopted by the Top Management at a IS Forum held on XXX, 2004 and it will be reviewed for adequacy at least annually. The statement takes into account the risk assessment held on XXX, 2004. The identification of the controls selected follows that of Annex A of the standard. The controls implemented are defined in 4.2.1g of the company's IS Manual.

The management is committed to implement the selected controls according to the requirements of the standard, active legislation and contractual obligations of the company.

Documented information

The Knights's information security management system includes:
a) documented information required by ISO 27001:2013; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:
1) the size of organization and its type of activities, processes, products and services;
2) the complexity of processes and their interactions; and
3) the competence of persons.

Creating and updating

When creating and updating documented information the organization shall ensure appropriate:
a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

Control of documented information

Documented information required by the information security management system and by ISO 27001:2013 shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
For the control of documented information, the Knights shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.
NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

5. - Management Responsibility

Management Commitment and Leadership

The management is fully committed to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. The management has developed and adopted an Information Security Policy; it has ensured that information security objectives and plans are established. It has established roles and responsibilities for information security. The importance of meeting the IS objectives has been communicated in the organization as well as the conforming to the information security policy; their responsibilities under the law and the need for continual improvement. The management provides sufficient resources for the development, implementation, operation and maintenance of the ISMS. The levels of acceptable risks have been defined. ISMS Management reviews are held at planned intervals.

Resource Management

Provision of Resources

The organization has determined and provided the resources needed to:

- Establish, implement, operate and maintain the ISMS
- Ensure that information security procedures support the business requirements
- Identify and address legal and regulatory requirements and contractual security obligations.
- Maintain adequate security by correct application of all implemented controls
- Carry out reviews when necessary, and react appropriately to the results of these reviews
- Where required, improve the effectiveness of the ISMS.

Training, Awareness and Competency

The organization ensures that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

- Determining the necessary competencies for personnel performing work effecting the ISMS
- Providing competent training and, if necessary, employing competent personnel to satisfy these needs
- Evaluating the effectiveness of the training provided and actions taken.

The company also ensures that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6. - Management Review of the ISMS

General

The management reviews the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the ISMS, including the security policy and security objectives. The results of the reviews are documented and records are maintained.

Review Input

The inputs to the management review include information on:

- Results of ISMS audits and reviews
- Feedback from interested parties
- Techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness
- Status of preventive and corrective actions
- Vulnerabilities or threats not adequately addressed in the previous risk assessment
- Follow-up actions from previous management reviews
- Any changes that could affect the ISMS
- Recommendations for improvement

Review Output

The outputs from the management review include decisions and actions related to the following:

- Improvement of the effectiveness of the ISMS
- Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
  - Business requirements
  - Security requirements
  - Business processes effecting the existing business requirements
  - Regulatory or legal environment
  - Levels of risk and/or levels of risk acceptance
- Resource needs

Internal ISMS audits

The organization conducts internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of the ISMS:

- Conform to the requirements of the standard and the relevant legislation
- Conform to the identified information security requirements
- Are effectively implemented and maintained
- Perform as expected

An audit programme is planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audits criteria, scope, frequency and methods are defined. Selection of auditors and conduct of audits ensures objectivity and impartiality of the audit process. Auditors do not audit their own work.

The management responsible for the area being audited ensures that actions are taken without undue delay to eliminate detected nonconformities and their causes. Improvement activities include verification of the actions taken and the reporting of verification results.

ISMS Improvement

Improvement

The organization is committed to continually improve the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management reviews.

Corrective Actions

A documented procedure has been developed for the management and control of Corrective actions. (Procedure 3)

Annexes

Procedure 1. – Control of Documented Information

Procedure 2. - Corrective actions

Risk Assessment Report - IS Doc 06

Risk Treatment Plan – IS Doc 06

Procedure 1- *Control of Documented Information*

A1 - RESPONSIBILITIES

The security Manager is responsible for the co-ordination of all ISMS documentation, which includes:

Establishment and maintenance of - this of the IS manual, procedures, Process descriptions (diagrammatic and text) Work instructions and forms.

Control of changes to procedures.

- Revision & distribution of procedures/process maps
- Maintaining a history of all changes
- Maintaining a master set of Company forms

The Management is responsible for the authorisation of process descriptions applicable to their scope of responsibility.

A1.2 - REQUIREMENTS

It is a requirement of the company's ISMS and that of ISO/IEC 27002:2005 that certain 'mandatory' procedures are established, documented and maintained. Any further procedures identified within the manual are grouped together with the mandatory procedures and incorporated within this manual as appendices.

The organization has developed the following documents required by the standard:

- Security Policy
- Scope, procedures and controls in support of the ISMS
- Risk Assessment Report
- Risk Treatment Plan
- Documented procedures
- Statement of Applicability

A1.3. - PROCEDURE CONTROL

A1.3.1 - Generating Process descriptions or Procedures

Any employee identifying the need for a new procedure, process description or work instruction shall first obtain approval to proceed from the Manager of the respective Department.

Written Procedures shall where practical adopt the following headings:

- Responsibilities
- Requirements
- Procedure
- Records

These requirements may be curtailed if procedures/process descriptions are located & presented graphically within the software based ISMS that provides purpose, scope etc., by virtue of the software package structure.

A1.3.2 - Authorisation

The authorisation for IS documentation is as follows:

Document Type	Authority
IS Manual	CEO
Procedures/Flow diagrams	Security Manager
Work Instructions	Security Manager

A1.3.3 - Numbering

The Security Manager is responsible for the allocation and logging of numbers for all documents within the ISMS - software based numbering is automatically preset by the software package used.

A1.3.4 - Issue Status Control

All documents (this includes each individual diagram within the total 'MAP' contained in the ISMS] within the ISMS shall be controlled by a revision number.

Whenever a procedure (or diagram) is updated the ‘footer’ will carry the latest revision number and operative date. The software ISMS shall maintain a record of current status and copies of all previous status levels for a period of at least 10 years subsequent to any changes being implemented.

The revision status of forms shall be denoted by a number following the form number, i.e. [x]FXX- Rev 3. Whenever a “Form” is updated the “Forms Register (Form F0)” shall be revised manually to maintain a record of revision level current status. The Forms Register (Form F0) shall also contain the following information relating to copies of completed forms (IS Records).

- Authoriser for changes/updated Form master
- Location stored
- Time period of retention
- Authority to scrap/destroy old records

A1.3.5 - New or Revised Forms

The FORMS REGISTER (Form F0) is maintained and changes reviewed/authorised by the Security Manager.

The Knights Inc Security Manager will advise on the appropriate reproduction method for forms based on complexity, application, usage rate, quality of presentation etc.

The ISMS shall be the source of all blank forms that require manual or electronic storage when completed.

Photocopying is only to be used if the ISMS is temporarily unavailable to access the required form.

Forms/Records originating from software packages [other than via the ISMS] shall have a copy of the current revision level maintained & accessible via the ISMS for reference and training purposes.

A1.3.6 - Change Control

Change requests relating to any element of the ISMS are made in writing to the Security Manager.

These requests are produced in hard copy form and filed in the ISMS Management Review folder for inclusion at the next Review.

Changes that require more urgent action are to be photo-copied and used as the working document to execute changes – this copy shall be annotated with the actual actions taken and filed along with the original filed in the management review folder.

When changes are made to the IS Manual (except appendices thereto) the whole document is raised to the next issue.

When process maps [& procedures] forms or work instructions are updated the document is replaced and its 'Version Number' updated.

The procedure (or diagram) or other document is then re-authorised as per paragraph A1.3.2 and made available by promoting the newly authorised copy into general use, showing the Revised Version Number.

The Management is responsible for bringing to the attention of the staff any changes that affect work operations, this will be communicated via e-mail.

A1.4. – CONTROL OF THIRD PARTY ACCESS

The access of third parties to ISMS documentation is defined through the controls implemented.

A1.5. - RECORDS

Evidence of change-requests and resulting actions shall be retained on the Documentation Change Log for a minimum of 3 years.

Records shall be retained in a manner so as to prevent damage, deterioration or loss and that procedures are in place for the identification, collection, indexing, access, filing, retrieval, storage, maintenance and disposal. Where practical electronic media is preferred for the retention of data.

Unless otherwise stated in process descriptions, records will be retained for a period of 6 months.

The Security Manager is responsible for ensuring that all manually entered records are legible, any records falling below a reasonable standard of legibility shall be rewritten before storage.

Controls for Identification, retention, storage, protection, retrieval and disposition are the responsibility of the directors to which the documents belong.

Procedure 2 - ***Corrective actions***

A6.1 - RESPONSIBILITIES

All staff are responsible for the correct and accurate recording of data for non-conformities at any stage.

The Security Manager is responsible for the analysis of non-conformity data reported, the various quality records and preparing a summary of the main problems for the ISMS Management Review.

A6.2 - PROCEDURE

Nonconformity data shall be analysed on a regular bi-monthly basis and presented as a Key Performance indicator in order to monitor trends and identify corrective actions taken.

Data analysis shall include, but not be restricted to:

- ISMS Management Review reports
- Security Incidents records
- Internal Audit Reports
- Others

In general corrective activities shall be processed on a day to day basis whereas preventative action may be a longer term activity to eliminate future problems.

All staff are responsible for the timely progress of corrective actions allocated to their area of responsibility.

Changes to procedures as a result of corrective/preventative action shall be in accordance with IS Manual Section ??

A6.4. - RECORDS

Records of corrective actions shall be retained as Records for a minimum of 3 years.

End of Procedure 2