Process Document

PD-19f
Information Security Policy

Table of Contents:

1. Overview/Purpose 3
2. Scope 3
3. Definitions 3
4. Responsibilities 5
5. Policy 5
5.1. ISMS benefits 6
5.2. Non-compliance with ISMS requirements 7
6. References 7

1. Overview/Purpose

The purpose of this document is to demonstrate the Security Management Team's commitment to information security and to provide the over-arching policy statements to which all subordinate policies and control must adhere.

The Management Team at Generis operates primarily in the business of creating and supporting document management systems.

Generis is committed to preserving the confidentiality, integrity, and availability ("CIA") of all the physical and electronic information and information-related assets to meet the purpose and goals of the organisation as summarised in **SOP-19 Information Security Management System.**

Information and information security requirements must continue to be aligned with the organisation's business goals and must consider the internal and external issues affecting the organisation and the requirements of interested parties. Generis' ISMS Objectives are outlined and measured in accordance with the requirements of the ISO/IEC standard 27001:2013 as per Cl.6.2.

2. Scope

All staff must comply with this policy.

3. Definitions

ISMS – Information Security Management System

In this policy and the related set of policies contained within the online environment that incorporate our ISMS, '**information security**' is defined as:

preserving

This means that all Generis' staff have, and will be made aware of, their responsibilities that are defined in their job descriptions or contracts to act in accordance with the requirements of the ISMS. The consequences of not doing so are described in **PD-11b Staff Management**. All relevant Interested Parties will receive information security awareness training and more specialised resources will receive appropriately specialised information security training.

the confidentiality

This involves ensuring that information is only accessible to those authorised to access it and preventing both deliberate and accidental unauthorised access to the organisation's, and relevant Interested Parties information, proprietary knowledge, assets and other systems in scope.

integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial, or complete, destruction or unauthorised modification, of either physical assets or electronic data.

and availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The environment must be resilient, and the organisation must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems, and information.

of information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the organisation or those of relevant Interested Parties and BYOD in scope that are processing organisation related information.

of our organisation

The organisation and relevant Interested Parties that are within the scope of the ISMS.

4. Responsibilities

Role	Responsibility
HR Manager	• Ensure that all staff are familiar with this document
CEO	• Review and approve the guidelines
Security Management Team	• Update the guidelines as required
Staff	• Understand the content of the policy, importance of ISO 27001 controls Participate in all the activities to maintain and improve Generis' ISMS

5. Policy

All staff must comply with all the policies that are related to ISO 27001:2013 controls (**Generis Documents Management Plan**) and are required as per **Generis Job Description Document**. Appropriate training is assigned through a special 'Read and Understood' task in **eProf** system and mandatory for completing. ISMS communications as per Cl.7 (Leadership) are available in #isms_maintenance channel in Slack on an ongoing basis.

The ISMS is intended as a mechanism for managing information security related risks (**SOP-20 Risk Assessment and Treatment Methodology**) and improving the organisation to help deliver its overall purpose and goals.

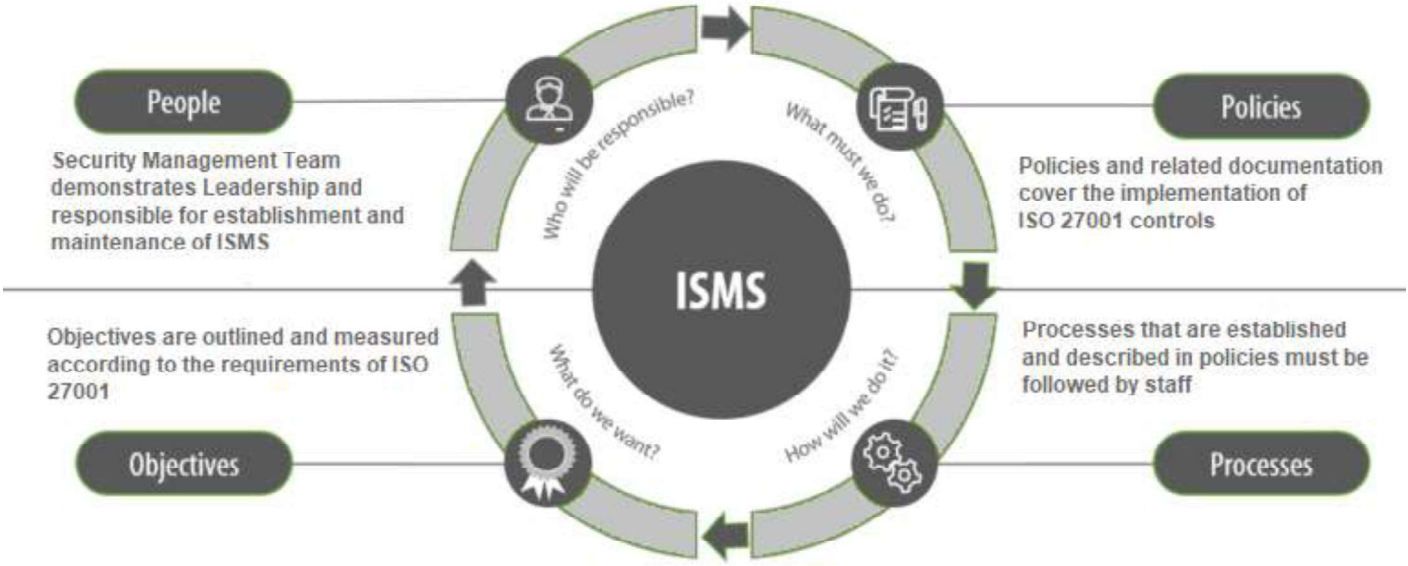
The **ISMS.online** platform allows tracking compliance with ISO/IEC standard 27001:2013, maintain it and manage the related risks and assets.

The approach taken towards Risk Assessment and Management, the Statement of Applicability and the wider requirements set out for meeting ISO 27001:2013 identify how information security and related risks are addressed.

The SMT is responsible for the overall management and maintenance of the Risk Treatment Plan with specific risk management activity tasked to the appropriate owner within the organisation. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.

Control objectives for each of these areas are supported by specific documented policies and procedures **eProf** (internal document management system) and they align with the comprehensive controls listed in Annex A of the ISO 27001:2013 standard.

The ISMS is subject to review and improvement by the Security Management Team with participation of Security Support Team (**SOP-06 Review Process, SOP-17 Internal Audit**).



5.1. ISMS benefits

Generis' staff must contribute to effectiveness of ISMS by following the related policies, participating in ongoing activities and discussions. Activity owners (for controls, risks, assets) are assigned in **ISMS.online.** All the ISMS roles, their responsibilities and authorities are described in **SOP-19.**

Active support of effective ISMS allows Generis to achieve the following benefits:

- **Assurance –** customer is assured of the quality of a system, business unit, or other entity if a recognized framework or approach is followed
- **Interoperability –** systems from diverse parties are more likely to fit together if they follow a common guideline
- **Awareness –** implementation and maintenance of a standard such as ISO 27001 results in greater security awareness within Generis

- **Alignment –** meeting of ISO 27001 controls tends to involve both business management and technical staff, greater IT and Business alignment is a result
- **Lowering the expenses –** risk management helps to lower expenses caused by incidents.

5.2. Non-compliance with ISMS requirements

All staff must be aware of all their responsibilities according to ISMS requirements. The consequences of non-compliance are described in **PD-11b Staff Management** (see definition of **information security** in section 4).

Compliance with ISMS requirements are checked during internal audits and management reviews **– SOP-06 Review Process, SOP-17 Internal Audit**. All the nonconformities and corrective actions must be logged, analysed and processed as per **PD-05a Change Management and CAPAs Processing**.

6. References

- SOP-20 Risk Assessment and Treatment Methodology
- SOP-19 Information Security Management System.
- Generis Documents Management Plan
- Generis Job Description Document
- SOP-06 Review Process
- SOP-17 Internal Audit
- PD-05a Change Management and CAPAs Processing