IMS POL/0029

Information Security Reviews

Approved by:	Adebola Badmus
Role:	COO
Date:	20 June 2024

Revision history

Revision	Date	Description of Changes	Prepared By	Approved By
0.1	10-11-2023	Version 0.1	Project Team	
0.1	05-03-2024	Version 0.1		

Distribution history

Revision	Date	Stakeholders

Control of hardcopy versions

The digital version of this document is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the **Document Controller** and provided with a document reference number and revision in the fields below:

Document Ref.		Rev.		Uncontrolled Copy	X	Controlled Copy	

Table of Contents

1 Introduction

1.1 Scope

This policy sets out Intelfort's arrangements for ensuring that information security is implemented and operated in accordance with our organizational policies and procedures.

1.2 References

Standard	Title	Description
ISO 27000:2014	Information security management systems	Overview and vocabulary
ISO 27001:2013	Information security management systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls
ISO 27001:2013	Information security management systems	Clause A.7 Human resources security

1.3 Terms and Definitions

- "Staff" and "Users" means all of those who work under our control, including employees, contractors, interns etc.
- "We" and "Our" refer to Intelfort.

1.4 Responsibilities

The ISMS Manager is responsible for all aspects of the implementation and management of this policy, unless noted otherwise.
The ISMS Manager is authorized to appoint independent information security experts to conduct reviews.

Departmental heads and supervisors are responsible for the implementation of this policy, within the scope of their responsibilities, and must ensure that all staff under their control understand and undertake their responsibilities accordingly.

2 Policy

We ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

1.1 Independent review of information security

Our approach to managing information security, its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) and its potential for improvement is independently reviewed at planned intervals, or when significant changes occur.

Independent information security reviews are carried out at intervals not exceeding **12 months** or when significant changes occur.

Independent reviews are carried out either by independent internal auditors or third party specialist individuals / organizations having the appropriate skills and experience.

Reports are addressed to both the ISMS Manager and the Intelfort Manager who are responsible for promptly implementing any necessary corrective and/or preventative actions and for considering proposed improvements.

Reports are also discussed, and progress monitored, at the next available information security management review.

Our arrangements for internal audits are set out in our Control of Internal Auditing Procedure.

1.2 Compliance with security policies and standards

Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

Where any noncompliance is identified, the responsible manager, in consultation with the ISMS Manager:

- Determines the causes of the non-compliance.
- Evaluates the need for actions to ensure that non-compliance does not reoccur.
- Determines and implements appropriate corrective action.
- Reviews the corrective action taken to ensure outcomes are as expected.

1.3 Technical compliance reviews

Information systems are regularly reviewed for compliance with our information security policies and standards.

Technical compliance reviews are supervised/ undertaken, and reports prepared by an experienced systems engineer using suitable tools.

Where penetration tests or vulnerability assessments are used, they are carefully planned, exercised with due caution, are designed to be repeatable and the approach and results are documented.

3 Records

Records retained in support of this procedure are listed in the **IMS Controlled Records Register** and controlled according to the **Control of Management System Records Procedure.**