



ISMS Corporate Policy

Classification: Public

This document may be viewed, distributed or printed by authorized personnel only. Distribution table below should always show the distribution of this document.

Document Details

DOCUMENT VERSION CONTROL

Item	Description
Project Name:	ISO 27001:2022 Implementation and Certification
Document Name:	ISMS Corporate Policy
Document Code:	
Document Version:	1.0
Status:	Final
Authors:	Kayan HR Solution
Approved By:	ISMS-Steering Committee (ISMS-SC)
Data Classification:	Internal
Issue Date for this version:	28.02.2026

REVISION HISTORY

Revision Date	List of Changes	Author	Approval
22.12.2025	Initial Release	Kayan HR Solution	
28.02.2026	Reviewed and updated	Kayan HR Solution	ISMS-Steering Committee (ISMS-SC)

DISTRIBUTION LIST:

Name	Title / Department	Signature

TABLE OF CONTENTS

1. Scope	4
2. Policy Statement	4
3. Compliance Statement	5

1. Scope

- ✓ The policy applies to all information created or received in **KAYAN HR SOLUTION**.
- ✓ This policy forms the basis of **KAYAN HR SOLUTION** Information Security Management System (ISMS) related policies and procedures, based on the International Standard 27001, taking a risk-based approach to embed appropriate levels of information security controls and countermeasures.

2. Policy Statement

It is the policy of **KAYAN HR SOLUTION** to ensure that appropriate controls and countermeasures are put in place to protect corporate and client data, as well as the information technology systems, and services and equipment of **KAYAN HR SOLUTION**. The purpose of the policy is to protect **KAYAN HR SOLUTION's** information assets from all threats, whether internal or external, deliberate, or accidental.

- ✓ **KAYAN HR SOLUTION** is committed to protect its information assets, personnel, privacy and intellectual property, computer systems, data, and equipment from all threats, whether internal or external, deliberate, or accidental, in a cost-effective manner. This should be achieved with minimum inconvenience to authorized users and against threats to the level of service required by the **KAYAN HR SOLUTION** to conduct its business.
- ✓ **KAYAN HR SOLUTION** shall adopt ISO 27001 Information Security Management System (ISMS) as a tool to implement a formal system for protecting confidentiality, integrity, and availability of information.
- ✓ **KAYAN HR SOLUTION** is committed to comply with regulatory and legislative requirements.
- ✓ **KAYAN HR SOLUTION** is committed to satisfying the expectations and requirements of interested parties, and to provide the necessary resources to achieve this.
- ✓ **KAYAN HR SOLUTION** is committed to encouraging information security improvements by engaging with its personnel, providing them with information security training and awareness, and enhancing their competences.
- ✓ Information security should be aligned with **KAYAN HR SOLUTION's** strategic direction and business objectives.
- ✓ Information security risks shall be managed based on **KAYAN HR SOLUTION's** Risk Management Methodology.
- ✓ **KAYAN HR SOLUTION** is committed to continually improving its ISMS and information security posture.
- ✓ **KAYAN HR SOLUTION** is committed to treat and resolve security incidents and suspected vulnerabilities per their respective nature.
- ✓ Objectives relating to information security performance will be set then monitored and reviewed by the **ISMS Steering Committee (ISMS-SC)**.
- ✓ **KAYAN HR SOLUTION** will continually review this policy and its information security performance to ensure it improves over time.
- ✓ All **Managers** are directly responsible for implementing this **ISMS Policy**, and for ensuring staff compliance in their respective departments.

- ✓ This policy is available to all **KAYAN HR SOLUTION** personnel and relevant interested parties. All **KAYAN HR SOLUTION** personnel are made aware of their commitment and the contents of this policy.

3. Compliance Statement

Compliance with this policy and all other supporting policies, standards, and procedures is mandatory for all staff and third parties. Violation of this policy or any other IS policies, standards, or procedures will result in corrective action by management. Disciplinary action will be consistent with the severity of the violation, as determined by an investigation, and as deemed appropriate by management.



28.02.2026