PROCESS&SMITH
WWW.PROCESSANDSMITH.COM

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.

PROCESS&SMITH WWW.PROCESSANDSMITH.COM CarrotCut

Document Details

DOCUMENT VERSION CONTROL

Item	Description
Project Name:	ISO 27001 Implementation and Certification
Document Name:	ISMS Corporate Policy
Document Code:	ISMS-CP-01
Document Issue No:	1.0
Status:	Final
Authors:	PROCESS&SMITH
Approved By:	ISMS-Steering Committee (ISMS-SC)
Data Classification:	Public
Date:	05.12.2023

REVISION HISTORY

Revision Date	List of Changes	Author	Review
05.12.2023	Initial Release	PROCESS&SMITH	ISMS Information Security Steering Committee
10.01.2024	Reviewed Document	PROCESS&SMITH	ISMS Information Security Steering Committee
29.01.2024	Approved Version	PROCESS&SMITH	ISMS Information Security Steering Committee

DISTRIBUTION LIST:

Name	Title / Department	Signature

PROCESS&SMITH WWW.PROCESSANDSMITH.COM CarrotCut

TABLE OF CONTENTS

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

PROCESS&SMITH WWW.PROCESSANDSMITH.COM CarrotCut

1. Scope

- The policy applies to all information created or received in **PROCESS&SMITH**.
- This policy forms the basis of **PROCESS&SMITH** Information Security Management System (ISMS) of 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 **PROCESS&SMITH** 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 **PROCESS&SMITH**. The purpose of the policy is to protect **PROCESS&SMITH's** information assets from all threats, whether internal or external, deliberate, or accidental.

- **PROCESS&SMITH** is committed to protect its information assets, personnel, 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 **PROCESS&SMITH** to conduct its business.
- **PROCESS&SMITH** shall adopt ISO 27001 Information Security Management System (ISMS) as a tool to implement a formal system for protecting the confidentiality, integrity, and availability of information.
- **PROCESS&SMITH** is committed to comply with regulatory and legislative requirements.
- **PROCESS&SMITH** is committed to satisfy the expectations and requirements of interested parties, and to provide the necessary resources to achieve this.
- **PROCESS&SMITH** 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 **PROCESS&SMITH**'s strategic direction and business objectives.

PROCESS&SMITH WWW.PROCESSANDSMITH.COM CarrotCut

- Information security risks shall be managed based on **PROCESS&SMITH's** Risk Management Methodology.
- **PROCESS&SMITH** is committed to continually improve its ISMS and information security posture.
- **PROCESS&SMITH** 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)**.
- **PROCESS&SMITH** 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 **PROCESS&SMITH** personnel and relevant interested parties. All **PROCESS&SMITH** personnel are made aware of its 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.

Name: Shadi Al Hasan

Position: CEO