
# Information Security Policy

## Introduction

As a company Dakar is committed to satisfying applicable requirements relating to information security and the continual improvement of its Information Security Management System (ISMS).

Information security is the responsibility of all Dakar staff members, and all staff members have been made aware of this policy, so that they may demonstrate the practical application of the key objectives, where appropriate, in their daily duties.

Verification of compliance with this policy will be by a continuous programme of internal and external audits.

## Scope

This policy applies to all employees, contractors and third parties working for or supplying a service to the company.

# Information Security Policy

## Information Security Roles and Responsibilities

Senior management are responsible for the overall effectiveness of the Information Security Management System (ISMS) and for providing the resources necessary to implement and improve it. Where necessary, the company will provide specific training on information security according to an employee's role.

The COO and Compliance Manager (CM) are responsible for business continuity planning and the CEO is responsible for providing the resources to implement all business continuity plans (BCPs).

Technical measures to mitigate threats to Information Security (InfoSec) are the responsibility of the CTO.

The CM is responsible for maintaining, communicating, and monitoring the ISMS, and reports regularly to the CEO and COO on its status and effectiveness.

All staff are responsible for Information Security in the execution of their work.

## Information Security Objectives

1) Maintain and adhere to the Statement of Applicability.
2) Continue to provide our services in a secure environment.
3) Ensure the availability of critical hardware and software applications.
4) Continually improve the ISMS.
5) Undertake annual risk assessments to ensure that data under our care is safe.
6) Ensure that information related to business processes conforms to the ISO27001 standard.
7) Establish quantified information security goals annually through management and review meetings.

## Legal and Regulatory Obligations

Dakar understands its legal, regulatory, contractual, requirements and adopts applicable controls to meet them.

The key areas of compliance are:

- Enforcement of Intellectual Property Rights (Regulation) Act.
- General Data Protection Regulation (GDPR) 2016/679.
- Companies Act, Chapter 386 of the laws of Malta.
- Convention on Cybercrime, ETS 185 of 23.XI.2001.
- Occupational Health & Safety (OHS) Legislation, Chapter 424 of the laws of Malta.
- NIS2 Directive.
- The Employment and Industrial Relations Act, Chapter 452 of the Laws of Malta.

Compliance is achieved by:

- Monitoring the legal, regulatory, contractual, and standards required.
- Implementing controls where necessary.
- Communication with the relevant bodies and agencies.
- Obtaining Expert advice where necessary.

## Information Security Statement

It is Dakar's policy that:

1. Senior management will champion information security and provide the resources necessary to implement, improve and maintain the ISMS as part of our Integrated Management System (IMS).
2. Information is only accessible to authorised persons from within or outside the Company.
3. Confidentiality of information is maintained.
4. The Integrity of information is maintained throughout all processes.
5. Controls will be established to maintain the availability of all systems and data to authorised users. Including business continuity plans that are maintained and tested.
6. All personnel are trained in information security and are informed that compliance with the InfoSec policy is mandatory.
7. All breaches of information security and suspected weaknesses are reported and investigated.
8. A formal disciplinary process will take place for serious information incidents.
9. Procedures exist to support the policy, including virus control measures, a password policy, and continuity plans.
10. Business requirements for availability of information and systems will be met.