



STELTH SMC LTD INFORMATION SECURITY STATEMENT

1.0 Introduction

This information security policy outlines Stelth's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the confidentiality, integrity and availability of all its physical and operational information assets that are critical to the provision of its services, in accordance with contractual requirements.

2.0 Purpose

The Information Security Policy is aligned to the ISO 27001:2022 Standard and is meant to set out Stelth's approach to managing its information security objectives

- 2.1 The purpose of the information security policy is to provide a framework for establishing suitable levels of information security for all of Stelth's information assets and to mitigate the information security risks associated with the theft, loss, misuse, damage or abuse of these information assets.
- 2.2 This policy is an integral part of other organizational policies that are in force.
- 2.3 This information security policy is further supported by topic-specific information security policies and to guide Stelth's implementation of security controls. These policies, procedures etc. have been approved by Management and made available to relevant target groups within Stelth and relevant parties.

3.0 Scope

This policy governs all information that is created, transmitted, processed, stored or disposed during the course of Stelth business and information assets and the systems used to create and maintain that information.

- 3.1 It applies to:
 - 3.1.1 All Stelth staff, partners, suppliers and contractors with access to Stelth's information assets
 - 3.1.2 Employees, representatives and agents from other organizations who directly or indirectly support Stelth's information systems, including auditors and other external consultants
 - 3.1.3 This policy applies to all physical and electronic information assets for which Stelth is responsible.
 - 3.1.4 The procurement, development, implementation, operation and support and any other activities involving the use of Stelth's information assets.

4.0 Definitions

- 4.1 Information: Facts or processed data that relates to Stelth whether in physical or digital format
- 4.2 Information Security: This refers to the protection of critical assets to ensure their confidentiality, integrity and availability
- 4.3 Risk: is the probability that a threat, an unwanted event or action will adversely affect Stelth's ability to achieve its strategic objectives
- 4.4 Information Asset: A collection of information, and facilities used to capture, record, transmit, process and display it.

5.0 Stelth's Information Security Statement

Information assets underpin Stelth's operations and are essential to the achievement of its strategic goals and objectives. It is therefore important that we ensure that the information we are responsible for is safeguarded and conforms to the principles of confidentiality, integrity and availability in accordance with our business requirements, information security objectives and legal, regulatory and contractual requirements.

To this end, the Stelth Management Team is committed to the implementation and continual improvement of a robust Information Security Management System aligned to ISO 27001:2022 Standard for Information Security Management. The Company aims to ensure the appropriate confidentiality, integrity and availability of its data and data entrusted to its care. The requirements of interested parties (including regulatory, contractual and legal requirements) with respect to information security will be met.

Stelth's Top Management is further committed to maintaining and improving the company's information security posture and minimizing exposure to risk, to ensure secure and resilient services that enrich customer experience and supports the achievement of its strategic goals.



Clere Atuhaire
Chief Executive Officer