



## **FUTURELINK TECHNOLOGIES (FLT) LTD**

### **INFORMATION SECURITY POLICY**

FutureLink Technologies Ltd (FLT) has established a documented Information Security Policy based on the requirements of ISO/IEC 27001:2022, which is appropriate for the purpose of the company. This policy includes information security objectives necessary to protect the confidentiality, integrity and availability of information assets from threats, whether internal or external, deliberate or accidental in relation to the processing, transmission and storing of sensitive financial and customer information.

The advancement of technology has brought provided a competitive advantage of the company in providing trusted efficient and effective services to our customers. As such, this emphasises the need for a strong information security management system to maintain the security and trust in the use of our technology enabled services. The company is therefore committed to consistently undertake the following measures:

- a) Implement the appropriate risk-based technology, administrative, security and organisational controls for protection of all critical information assets
- b) Undertake periodic security awareness training for all its staff and contractors annually
- c) Comply with statutory requirements and contractual security obligations
- d) Manage and control access to all business applications
- e) Implement business continuity plans that address information security continuity
- f) Conduct periodic independent security assessments of critical services

FLT is committed to satisfying applicable requirements related to information security, and to the continual improvement of the information security management system.

To support this policy FLT shall establish an information security management system which incorporates a systematic approach to information security risk management and fully comply with the ISO/IEC 27001 standard.

This policy must be communicated to internal parties through our internal document sharing platform, induction training, ISMS awareness sessions and a signed ISMS policy must be displayed at all prominent places within the company.

The policy must further be communicated to external parties through publishing on the company official website, communicated through official email, or during contract signing.


Any changes to this policy must be communicated to internal and external parties.

This policy shall be reviewed at regular executive meetings annually or when there is a major change within the company.

### Document Control

No	Type of Information	Document Data
1.	Document Title	Information Security Policy
2.	Date of release	126/2025
3.	Document number	
4.	Document version no.	2.0
5.	Document owner	Chief Executive Officer
6.	Document author	Sentinel Africa Consulting Ltd

### Document Approvers

Approver	Approver Designation	Signature	Approval Date
Mr. Vincent Tumwijukye	Chief Executive Officer		2 <sup>nd</sup> Feb 2025

### Change Log

Version No.	Revision date	Nature of Change	Date Approved