Ebenezer Commercial Works Ltd. Innovation. Integrity. Performance						
	Created	01/01/2019	Review	25/09/2026	Next Review	05/01/2027
	Revision	01		Doc Ref No:	ECWL/WBM/LV1/001/PST02	
	Author	HR Manager				
	Reviewer	Quality Manager		Operations Manager		
	Approver	Managing Director				

Information Security Management System (ISMS) Policy Statement

Ebenezer Commercial Works Limited (ECWL) is committed to establishing, implementing, maintaining and continually improving an **Information Security Management System (ISMS)** in accordance with **ISO/IEC 27001:2022 and applicable information security requirements of ISO/IEC 17020**, to protect the confidentiality, integrity and availability of information and information-processing assets under its control.

The organization shall achieve this commitment by:

1. **Protecting Information Assets:** Ensuring the confidentiality, integrity and availability of information through appropriate safeguards against unauthorized access, disclosure, modification, loss, destruction and disruption.
2. **Managing Information Security Risks:** Identifying, assessing and treating information security risks and implementing appropriate controls to address identified risks and opportunities.
3. **Satisfying Applicable Requirements**: Committing to identify, understand and satisfy all applicable legal, regulatory, statutory, contractual and other information security requirements relevant to the organization's operations and interested parties.
4. **Establishing Information Security Objectives:** Establishing measurable information security objectives consistent with this policy, monitoring their achievement and reviewing them periodically to ensure continued relevance and effectiveness.
5. **Maintaining Business Continuity:** Establishing and maintaining appropriate backup, information recovery and business continuity arrangements to ensure the availability and resilience of critical information and information-processing systems.
6. **Managing Information Security Incidents:** Ensuring information security incidents and weaknesses are promptly reported, assessed, investigated and addressed through appropriate corrective actions.
7. **Continual Improvement:** Regularly evaluating ISMS performance through risk assessments, internal audits, management reviews and monitoring of information security objectives, and implementing necessary improvements to enhance the suitability, adequacy and effectiveness of the ISMS.

Top management shall provide the necessary leadership, commitment and resources to implement this policy and achieve the established information security objectives.

This policy shall be communicated to all relevant personnel, made available to relevant interested parties where appropriate, and reviewed periodically to ensure its continued suitability and alignment with the organization's purpose and strategic direction.

NAOMI KAIRU
CHIEF EXECUTIVE OFFICE

Dated: **25th September 2026**

Ebenezer CW Ltd