

INTEGRATED MANAGEMENT SYSTEM POLICY STATEMENT

Purpose

This policy statement defines the organizations commitment to Information Security, Privacy and Business Continuity in order to protect information from loss of confidentiality, integrity, and availability, to protect user privacy as well as improve the organization's preparedness, resilience, and ability to continue delivering its mandate in the event of a disruption.

To fulfil this commitment, the management has established, an Integrated Management System (IMS) aligned with the requirements of ISO/IEC 27001:2022, ISO/IEC 27701:2019, and ISO 22301:2019.

Scope

This policy is applicable to all Smart Applications personnel, contractors, vendors, and other parties, and covers all information entrusted to or owned by Smart Applications and stored, processed, or transmitted on the organization's information systems and operated by the organization.

Integrated Management System Objectives

- 1. Fostering a culture of Security, Privacy, and Continuity awareness**
Promote organization-wide understanding and ownership of key principles through ongoing education and engagement.
- 2. Strengthen Resilience Against Phishing and Enhance Incident Response Readiness**
Reduce exposure to phishing threats and improve detection, reporting, and containment capabilities.
- 3. Achieve Full Compliance with Legal, Regulatory, and Contractual Obligations**
Maintain 100% adherence to applicable requirements through proactive monitoring and governance.
- 4. Ensure Timely Recovery of Critical Business Processes and IT Systems**
Meet defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for essential operations.
- 5. Safeguard the Organization across the Supply Chain**
Implement controls to manage third-party risks and ensure supplier alignment with security and privacy standards.
- 6. Maintain High System Availability and Uptime**
Ensure infrastructure reliability to support uninterrupted business operations.

7. Remediate Critical Vulnerabilities identified in Assessments

Address high-risk findings promptly to reduce exposure and strengthen the security posture.

8. Formalize Data Processing Agreements with Controllers and Processors

Ensure all relevant parties have signed DPAs that reflect the organization's privacy and security commitments.

9. Promote Sustainable and Resilient Operations

Reduce reliance on physical infrastructure by enabling secure, flexible, and remote-friendly work environments.

Integrated Management System Policy

Smart Applications is committed to implementing, maintaining, and improving comprehensive Information Security, Privacy and Business Continuity Management Systems appropriate to its context.

This will enable the organization to protect information, privacy as well as to protect people, brand, assets and enable timely recovery of critical operations in the event of a disruption so far as is reasonably practical.

Smart Applications is also committed to complying with all applicable legal, regulatory and contractual requirements related to information security, privacy and business continuity in its services and operations.

All staff and third parties shall comply with this policy and guidelines, or procedures derived from it.

For and on behalf of Smart Applications International Ltd; -



Harrison Muiru
Group Managing Director