Appmart

...creating a world of money without borders

Cyber-Security Manual

Document Classification:	Internal
Document Ref.	APPMART-IMS-Cyber Security Manual
Version:	1.0
Dated:	31 October 2024
Document Owner:	Executive Management

Revision History

Version	Date	Revision Author	Summary of Changes	Next Date Review
1.0	31 October 2024	Executive Management	Initial Documentation	31 October 2025

Distribution

Title	Date
ALL STAFF	31 OCTOBER 2024

Approval

Name	Position	Signature	Date
EMEJIOFOR ANTHONY CHINEDU	CHIEF TECHNICAL OFFICER		31-10-2024
MAKO SYLVESTER	MD/CEO		31-10-2024

Contents

Introduction

This Cyber-Security Manual outlines the policies, procedures, and best practices to safeguard Appmart Limited's digital assets, including its data, systems, and infrastructure, against potential cyber threats. This document is intended for all employees, contractors, and third-party partners of Appmart Limited.

Purpose

The purpose of this manual is to:

- Protect the confidentiality, integrity, and availability of Appmart Limited's digital resources.
- Ensure compliance with relevant legal and regulatory requirements.
- Minimize the risk of cyber threats, including data breaches, malware attacks, and unauthorized access.
- Promote a culture of cyber awareness among employees and stakeholders.

Scope

This manual applies to:

- All employees, contractors, and third-party partners.
- All company-owned or managed devices, including laptops, smartphones, and servers.
- All software, cloud services, and internal applications.
- Any data processed, stored, or transmitted by Appmart Limited.

Key Policies

1. Access Control

- Employees must use unique, complex passwords and enable multi-factor authentication (MFA) wherever available.
- Access to sensitive systems and data is granted on a need-to-know basis.
- Regular audits (annual but will be biannual in the future) will be conducted to review access permissions.

2. Data Protection

- All sensitive data must be encrypted during transmission and storage.
- Employees must adhere to data classification policies and handle information accordingly (e.g., public, internal, confidential).
- Regular backups of critical data must be performed and stored securely.

3. Incident Response

- Any suspected or confirmed security incidents must be reported immediately to the IT Security Team.
- An incident response plan (IRP) outlines procedures for containment, investigation, and remediation.
- Post-incident reviews will be conducted to improve future responses.

4. Network Security

- Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) must be deployed and monitored.
- Remote access must be secured using Virtual Private Networks (VPNs) and MFA.
- All devices connected to the company network must comply with security standards.

5. Software and Patch Management

- Only authorized software is allowed on company devices.
- Software updates and security patches must be applied promptly.
- Employees are prohibited from using unlicensed or pirated software.

Employee Responsibilities

1. Awareness and Training

- All employees must complete annual cybersecurity training/Awareness.
- Phishing simulations and other exercises will be conducted periodically to raise awareness.

2. Device Security

- Employees must ensure devices are locked when unattended.
- Lost or stolen devices must be reported immediately to the IT Security Team.

3. Email and Internet Use

- Avoid clicking on links or opening attachments from unknown sources.
- Use company-provided email for official communication only.
- Do not download files or software from untrusted websites.

4. Vendor and Third-Party Risk Management

- **Objective:** Mitigate risks arising from third-party relationships.
- **Key Actions:**
  - Perform due diligence before onboarding vendors.
  - Require vendors to comply with company security policies.
  - Regularly review vendor security practices.

Compliance and Enforcement

- Non-compliance with the policies outlined in this manual may result in disciplinary action, up to and including termination of employment.
- Regular audits and assessments will ensure adherence to the cybersecurity framework.
- External audits may be conducted to verify compliance with legal and regulatory requirements.