

PRESTIGE TECHNOLOGY LTD

ISMS Policy

Document Title	ISMS Policy
Document Reference	PTG-ISMS-POL-001
Document Owner	Chief Technology Officer (CTO)
Version	1.0
Classification	Internal Use
Publication Date	May 2026
Next Review Date	May 2028

Document Information

Date	Ver. No	Modified By	Action	Pages
January 2026	1.0	ISC	Initial Draft	All

Approval

Name	Position	Approval	Date
Mr. Attah Mensah	CTO	Approved	25 May 2026

Contents

Document Information 2

Approval 2

1. Purpose 4

2. Scope/Audience 4

3. Notice of Compliance 4

I. Information Security Objectives..... 5

II. Leadership Commitment 5

III. Information Security Principles 5

IV. Risk Management Approach..... 6

V. Roles and Responsibilities 6

VI. Policy Statements 6

VII. Continuous Improvement..... 7

VIII. Policy Review and Approval 7

IX. Policy Enforcement..... 7

X. ISO 27001:2022 References..... 7

1. Purpose

The purpose of this Information Security Management System (ISMS) Policy is to establish Prestige commitment to preserving the confidentiality, integrity, and availability (CIA) of information assets, in line with the requirements of ISO/IEC 27001:2022 and relevant regulatory standards (including the Cyber Security Authority guidelines, and local data protection laws).

This policy defines the framework within which Prestige Technology manages security risks, ensures compliance, protects customer trust, and continuously improves the ISMS.

2. Scope/Audience

This ISMS policy applies to:

- All business functions, subsidiaries, and operations of Prestige.
- All employees, contractors, consultants, and third parties with access to Prestige's systems and data.
- All information assets, including but not limited to customer data, payment transaction data, intellectual property, financial records, and operational systems.
- All physical and digital environments, including cloud services, mobile platforms, data centres, and third-party integrations.

3. Notice of Compliance

Prestige Technology reserves the right to modify (add or remove) portions of this document at any time. Notification of changes to any document (policies, procedures, or manuals) shall be by email or publication via Prestige Technology's internally approved communication channels and shall be deemed fully enforceable thereon. Failure to comply with this document could result in consequences, including, but not limited to, the summary termination of the contract or employment.

1. Information Security Objectives

Prestige will:

- a. ensure that the organisation's regulatory, contractual and legislative requirements are met.
- b. ensure that policies, procedures and other relevant documentation are in place to establish appropriate information security practices within Prestige Technology's environment.
- c. provide assurance that Prestige Technology is committed to creating and sustaining a culture of security awareness that ensures the protection of the organisation's, clients' and partners' information assets.
- d. ensure that all suspected breaches or incidents of information security are reported, investigated and adequately managed.
- e. ensure information is maintained and protected from unauthorised access (Confidentiality).
- f. ensure information is protected from unauthorised modification (Integrity).
- g. ensure information and information processing facilities are available to authorised personnel (Availability).
- h. preserve the organisation's reputation and enhance business.

2. Leadership Commitment

Top management at Prestige is committed to ensuring Prestige Technology adheres to all application information security requirements. Top Management is committed to:

- a. Providing adequate resources, technology, and expertise to support the ISMS.
- b. Ensuring information security objectives are aligned with business strategy and risk appetite.
- c. Demonstrating visible leadership and accountability in promoting a strong security culture.
- d. Regularly reviewing ISMS performance and approving corrective/improvement actions.
- e. Supporting risk-based decision-making for managing threats and vulnerabilities.
- f. Capacity changes, as a result of increasing network usage or changes in the network architecture, shall be reflected in the Business Continuity Management Plans to ensure the continued recovery of systems and processes.
- g. Stress tests should be performed before the installation of newly acquired systems. Determine if the current system infrastructure can support the new equipment/service and update the capacity plan appropriately.

3. Information Security Principles

Prestige's ISMS is built on the following principles:

- a. **Confidentiality:** Protect sensitive financial and personal information from unauthorized access.
- b. **Integrity:** Safeguard information from unauthorized modification to maintain accuracy and trustworthiness.

- c. **Availability:** Ensure services and information remain accessible to authorized users when needed.
- d. **Accountability:** Assign clear ownership of information assets and security responsibilities.
- e. **Compliance:** Adhere to legal, regulatory, and contractual obligations.
- f. **Continuous Improvement:** Regularly update practices to address evolving risks and business needs.

4. Risk Management Approach

- a. Risks to Prestige's information assets will be systematically identified, assessed, treated, and monitored using a risk-based methodology aligned with ISO 27005.
- b. A Risk Register will be maintained, and mitigation measures will be applied based on risk appetite and impact.
- c. Risks introduced by third-party vendors, partners, and service providers will be reviewed and monitored.

5. Roles and Responsibilities

- a. **CEO/CTO:** Provide oversight and approve ISMS strategy.
- b. **ISMS Manager:** Owns and manages the ISMS, ensures compliance with standards.
- c. **Information Security Committee:** Coordinates security initiatives, reviews risks, and monitors ISMS KPIs.
- d. **Team Leaders/supervisors:** Ensure implementation of ISMS requirements within their teams.
- e. **All Employees:** Responsible for adhering to security policies, procedures, and reporting incidents.

*Please see the **Prestige Technology ISMS Manual** for detailed information on the information security roles and responsibilities*

6. Policy Statements

- a. **Access Control:** Access to information assets will be granted based on least privilege and need-to-know principles.
- b. **Data Protection & Privacy:** Customer and employee personal data will be processed lawfully, fairly, and transparently in line with Ghana's Data Protection Act.
- c. **Asset Management:** All information assets will be identified, classified, and protected according to their value and sensitivity.
- d. **Network & System Security:** Prestige will maintain secure network architectures, firewalls, intrusion detection/prevention systems, and strong encryption mechanisms.
- e. **Secure Development:** Security will be integrated into the software development lifecycle (SDLC). Code reviews, vulnerability assessments, and penetration tests will be performed regularly.
- f. **Incident Management:** All security incidents must be reported immediately. A structured incident response process will ensure timely detection, containment, investigation, and recovery.

- g. **Business Continuity & Disaster Recovery:** Prestige will maintain tested continuity and disaster recovery plans to ensure resilience of critical payment services.
- h. **Third-Party Security:** Vendors, fintech partners, and service providers must meet Prestige's ISMS requirements before engagement.
- i. **Training & Awareness:** All employees will receive periodic security training and awareness campaigns.
- j. **Compliance Monitoring:** Regular internal audits, external reviews, and penetration testing will be conducted to verify compliance with ISMS requirements.

7. Continuous Improvement

Prestige is committed to ensuring the continual improvement of the ISMS and information security management in general. The organisation will application the Plan-Do-Check-Act (PDCA) cycle in achieving this.

- a. **Plan:** Identify risks, set objectives, and define security controls.
- b. **Do:** Implement security measures and train stakeholders.
- c. **Check:** Monitor, audit, and review ISMS performance.
- d. **Act:** Apply corrective and preventive measures for improvement.

8. Policy Review and Approval

This policy will be reviewed Bi-annually, or upon significant changes in business processes, technology, or regulatory requirements. Updates must be approved by the CEO/CTO and communicated to all relevant stakeholders.

9. Policy Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, termination of vendor contracts, or legal action.

10. ISO 27001:2022 References

- Information Security Policies
- Organizational Controls (A5)
- People Controls (A6)
- Physical Controls (A7)
- Technological Controls (A8)