Compliance Policy & Procedure – ISO/IEC 27001

1. Compliance Policy

1.1 Purpose

This policy establishes the organization's commitment to comply with applicable legal, regulatory, and contractual requirements, as well as ISO/IEC 27001 standards, to support the Information Security Management System (ISMS).

1.2 Scope

This policy applies to all employees, interns, and contractors who access, process, or manage information assets within the organization.

1.3 Policy Statement

The organization shall:
- Identify and document all relevant legal, regulatory, and contractual compliance obligations.
- Ensure all business activities adhere to applicable compliance requirements.
- Assign roles and responsibilities to monitor, review, and enforce compliance.
- Report, investigate, and remediate compliance breaches.
- Provide training and awareness on compliance requirements.
- Maintain compliance records for audit purposes.

1.4 Roles & Responsibilities

Role	Responsibility
Compliance Officer	Maintain compliance register, coordinate audits, ensure implementation of controls
ISMS Manager	Integrate compliance into ISMS activities
Line Managers	Enforce compliance within departments
Employees	Comply with policies and report violations

1.5 Compliance Requirements

Includes but is not limited to:
- ISO/IEC 27001:2022
- POPIA (Protection of Personal Information Act)
- GDPR (if applicable)

- Contractual obligations with third parties
- Internal policies and procedures

1.6 Policy Review

This policy must be reviewed annually or upon significant changes to regulations, systems, or business activities.

1.7 Non-Compliance

Any deviation from this policy may result in disciplinary action, including legal or contractual penalties.

2. Compliance Management Procedure

2.1 Objective

To define the process for identifying, evaluating, managing, and monitoring compliance obligations across the organization.

2.2 Procedure Steps

- Step 1: Identify Compliance Requirements

Use a compliance register to log legal, regulatory, and contractual obligations. Sources include legislation, industry standards (e.g. ISO 27001), customer contracts, and internal policies.

- Step 2: Assess Applicability

Review each requirement and determine applicability based on organizational activities.

- Step 3: Implement Controls

Assign control owners. Implement procedures, systems, or training to meet each requirement.

- Step 4: Monitor Compliance

Conduct internal audits, spot checks, and compliance reviews. Use checklists and monitoring tools to track adherence.

- Step 5: Report & Resolve Issues

Document non-compliance. Investigate root causes. Apply corrective and preventive actions (CAPA).

- Step 6: Maintain Evidence

Retain logs, audit reports, policies, and training records. Ensure accessibility for auditors.

- Step 7: Review & Update

Conduct an annual review of compliance requirements and controls. Update the compliance register and procedures accordingly.

2.3 Documentation Requirements

- Compliance Register
- Internal Audit Reports
- Risk Register (linked to compliance risks)
- Evidence of Training & Awareness
- Corrective Action Records

2.4 Metrics for Compliance Monitoring

- Number of non-conformities reported
- Percentage of resolved compliance issues
- Audit findings and trends
- Employee training completion rate