Information Security Policy (ISO/IEC 27001:2022)

1. Purpose

Cyberintelsys Consulting Services Pte Ltd is committed to establishing and maintaining an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. As this is the organization's first ISMS implementation and certification audit, the primary objective is to build a strong foundation for protecting information assets, fostering a security-conscious culture, and meeting applicable legal, regulatory, and contractual requirements.

2. Scope

The scope of the initial ISMS implementation includes the following information assets and environments:

- AWS-hosted infrastructure

This policy applies to all Cyberintelsys Consulting Services Pte Ltd employees, contractors, and relevant stakeholders who access or manage information within the defined ISMS scope.

3. Information Security Policy Statement

Cyberintelsys Consulting Services Pte Ltd recognizes that information is a valuable business asset and is committed to protecting the confidentiality, integrity, and availability of its information and client data.

To achieve this, the organization is committed to:

- Protecting the confidentiality, integrity, and availability (CIA) of organizational and client information.
- Implementing a structured risk-based approach to information security.
- Complying with applicable statutory, regulatory, and contractual requirements.
- Establishing an incident response process to identify, report, and respond to information security events promptly.
- Promoting information security awareness, training, and engagement among all employees.
- Continually reviewing and improving the effectiveness of the Information Security Management System (ISMS) and its controls.

Information Security Policy (ISO/IEC 27001:2022)

4. Information Security Objectives

Objective	Initial Target	Review Frequency
Complete ISMS master documentation and obtain approval	100% of core documents	Annually
Identify and assess key information assets and associated risks	AWS, Office 365, Routers, Endpoints	Annually
Train all staff on information security awareness	100% of team trained	Annually
Respond to and resolve reported information security incidents	100% response within SLA	Monthly

These objectives provide a practical and scalable approach based on the organization's current infrastructure and operational size. As the ISMS matures, additional objectives and performance metrics will be established to support continual improvement.

5. Management Commitment

Top Management approves this Information Security Policy and is committed to supporting the implementation, maintenance, and continual improvement of the Information Security Management System (ISMS). The organization will ensure that appropriate resources are provided to achieve the defined information security objectives.

6. Policy Review

This Information Security Policy shall be reviewed annually or whenever significant changes occur to the organization's business operations, technology, legal requirements, or ISMS scope to ensure its continued suitability, adequacy, and effectiveness.