IOG Global (Private) Limited

Information Security Policy

ISO/IEC 27001:2022

Document ID: IOG/ISMS/POL/01
Version: 1.0
Owner: Chief Executive Officer (CEO)
Approved by: Top Management
Effective Date: [Month Year]
Classification: Public

1. Context and Objectives

IOG Global (Private) Limited (hereafter referred to as *IOG Global*) provides international Business Process Management and professional services including but not limited to Accounting, Finance, Digital Marketing, Human Resource Outsourcing, IT Services, Virtual Assistance and Administrative Support.

Information security is a critical business requirement for IOG Global due to the nature of services provided, which involve processing client financial data, personal data, confidential business information and access to cloud-based systems. The purpose of this Information Security Policy is to establish the principles, direction and commitment for protecting information assets in accordance with **ISO/IEC 27001:2022**.

This policy defines the framework for the Information Security Management System (ISMS) and applies to all employees, consultants, contractors and relevant third parties who access or process IOG Global information.

Top management is fully committed to the establishment, implementation, maintenance and continual improvement of the ISMS.

2. Scope of the ISMS

The scope of the IOG Global ISMS covers all services, processes, information systems, personnel and assets involved in the delivery of Business Process Management and professional services to international clients.

In-scope services include (but not limited to):

- Australia-specific Accounting Services

- Finance & Accounting Services
- Digital Marketing Services
- Human Resource Outsourcing
- IT Services
- Virtual Assistance
- Administrative Support

In-scope departments:

- Accounting Services
- Marketing Services
- HR & Operations
- Client - Services

No departments or business activities are currently declared out of scope.

In-scope locations:

- **Main Office:** 58, Dharmapala Mawatha, Colombo 07, Sri Lanka

IOG Global does not operate its own data centres. Information systems and infrastructure are primarily cloud-based and managed through approved cloud service providers.

3. Information Security Objectives

IOG Global is committed to protecting information assets by ensuring: - **Confidentiality:** Information is accessible only to authorized persons - **Integrity:** Information is accurate, complete and protected from unauthorized modification - **Availability:** Information and systems are available when required.

Information security objectives are defined by top management, aligned with organizational context and stakeholder requirements and reviewed at least annually.

4. Stakeholder Analysis

IOG Global identifies and reviews the needs and expectations of interested parties that are relevant to information security, including: - Clients and customers - Employees and contractors - Regulatory and statutory authorities - Business partners and suppliers

Stakeholder requirements, including data protection and confidentiality obligations (e.g. GDPR and applicable local regulations), are documented and reviewed annually as part of the ISMS.

5. Leadership and Responsibilities

Top management demonstrates leadership and commitment to information security by: - Establishing this Information Security Policy and related objectives - Assigning roles and responsibilities for information security - Providing adequate resources for the ISMS - Promoting continual improvement

The **Chief Information Security Officer (CISO)** is designated as the management representative responsible for overseeing the ISMS and reporting its performance to top management.

All employees and contractors are responsible for complying with this policy and supporting information security objectives in their daily activities.

6. Resources, Awareness, and Training

IOG Global ensures that personnel performing information security–related tasks are competent based on education, training, or experience.

- Information security awareness training is provided during onboarding
- Refresher training is conducted at least annually
- Role-specific training is provided where additional responsibilities exist

7. Operations

IOG Global maintains documented processes and controls to manage information security risks and meet policy objectives.

Information security risks are identified, assessed, and treated through a formal risk management process. Controls are selected in accordance with ISO/IEC 27001 Annex A and documented in the Statement of Applicability.

8. Performance Evaluation

The effectiveness of the ISMS is evaluated through: - Monitoring and measurement of information security objectives - Internal ISMS audits conducted at planned intervals - Annual management reviews

Where necessary, independent external expertise may be engaged for audits, assessments, or technical security testing.

9. Continual Improvement

IOG Global is committed to continual improvement of the ISMS through: - Management reviews - Internal and external audit findings - Incident analysis and corrective actions - Changes in business context, risks, or stakeholder requirements

Nonconformities are addressed through corrective actions to prevent recurrence and enhance the effectiveness of information security controls.

10. Policy Review and Approval

This Information Security Policy is reviewed at least annually or upon significant organizational, technological, or regulatory changes.

All employees, contractors, and relevant third parties are required to comply with this policy.

Approved by:
CEO/Founder
IOG Global (Private) Limited