INFORMATION SECURITY POLICY FOR LANKRIS LTD.

Version Number: 1.0

Classification: Internal

**Document Contents**

## 1. Title Page i

## 2. Document Contents ii

## 3. Purpose

## 4. Scope

## 5. Information Security Policy Principles

## 6. Chief Executive Statement of Commitment

## 7. Introduction 1

## 8. Information Security Definitions

## 9. Information Security Objectives 10. Information Security Policy Framework

## 11. Information Security Roles and Responsibilities

## 12. Monitoring

## 13. Legal and Regulatory Obligations

## 14. Policy Compliance

## 15. Compliance Measurement

## 16. Exceptions

## 17. Continuous Improvement

# **Purpose**

The purpose of this Information Security Policy is to establish a company-wide approach to information security, aimed at safeguarding Lankiris Ltd’s information assets from all threats, whether internal or external, deliberate or accidental. This aligns with our commitment to providing top-tier export services to our clients globally while upholding the highest standards of data and cybersecurity best practices.

# **Scope**

# This policy applies to all employees, contractors, and third-party users of information systems and services within Lankris Ltd.

**Information Security Policy**

Our principles include ensuring the confidentiality, integrity, and availability of all data in our care; protecting against threats to information security; and ensuring compliance with statutory and regulatory requirements like GDPR and PCI DSS. This is in line to sustain the business continuity and sustainability of the business operations of Lankris Ltd.

**Chief Technical Officer Statement of Commitment**

As the Chief Technical Officer (CTO) of Lankris Nig Ltd, I wholeheartedly endorse this Information Security Policy. Our commitment to information security is unwavering, and we recognize its critical role in safeguarding our business, our stakeholders, and our reputation.

**Context and Importance**  
- Business Imperative: Information security is not merely a technical concern; it is a strategic imperative. Our success, sustainability, reputation and business continuity depend on maintaining the confidentiality, integrity, and availability of our data.  
- Legal and Regulatory Landscape: The ever-evolving legal and regulatory landscape demands that we protect sensitive information. Compliance with data protection laws, industry standards, and contractual obligations is non-negotiable.  
- Reputation and Trust: Our clients, partners, and employees trust us with their data. A breach could irreparably damage our reputation and erode that trust, so it is very imperative that all stakeholders take this policy seriously.

**Our Commitments**1. Leadership Support: Senior management is fully committed to allocating resources, setting priorities, and championing information security initiatives.  
2. Risk-Informed Decision-Making: Inline with business sustainability, top management will make risk-informed decisions, committed to balancing business needs with security requirements.  
3. Budget and Investment: Adequate budget and resources will be allocated to information security projects, training, and awareness as it forms an important basis of our cybersecurity framework.

4. Policy Adherence: We expect all employees and 3employment vendors to adhere to this policy (where applicable). Compliance is not optional; it is a condition of employment and business continuity.

5. Continuous Improvement: We will regularly review and enhance our security posture, adapting to emerging threats and technological advancements.  
6. Incident Response: In the event of a security incident, we commit to swift and effective response, minimizing impact and learning from each incident.  
7. Employee Empowerment: We empower employees to report security concerns without fear of reprisal. Reporting incidents promptly is essential.  
8. Third-Party Accountability: Our vendors and partners must meet our security standards because We will hold them accountable.

**Our Expectations**  
- Senior Management: We expect senior leaders to lead by example, champion security awareness, and actively participate in security initiatives.  
- Department Heads: Each department head is responsible for implementing security measures within their teams.  
- Employee Training: All employees, regardless of role, will undergo regular security training. Training and awareness cannot be over-emphasised.   
- Security Culture: We will foster a security-conscious culture where everyone understands their role in protecting our assets.

**Conclusion**  
Our commitment to information security is not a checkbox exercise; it is a continuous journey. By adhering to this policy, we protect our business, our clients, and our future. Together, we build a resilient and secure organization.

Chris Lancaster  
Chief Technical Officer  
Lankris Ltd

## **Introduction**

Information is a critical asset for LanKiris Ltd. This policy sets out the requirements for the protection of information assets to ensure business continuity, minimize business damage in the event of a cyberattack, and maximize return on investments and business opportunities.

## **Information Security Definitions**

- Confidentiality: Ensuring that information is accessible only to those authorized to have access.

- Integrity: Safeguarding the accuracy and completeness of information and processing methods.

- Availability: Ensuring that authorized users have access to information and associated assets when required.

## **Information Security Objectives**

To protect the organization's operational capability and to protect sensitive and critical information from unauthorized access, disclosure, modification, destruction, or interference.

**Information Security Policy Framework**

The framework is based on the risk assessment and management process, aligning with [ISO/IEC 27001] standards, and includes policies, procedures, guidelines, and related documents.

The information security management system is built upon an information security policy framework. In conjunction with this policy, the following policies make up the policy framework:

DP 01 Data protection Policy

DP 02 Data Retention Policy

IS 01 Information Security Policy (this policy)

IS 02 Access Control Policy

IS 03 Asset Management Policy

IS 04 Risk Management Policy

IS 05 Information Classification and Handling Policy

IS 06 Information Security Awareness and Training Policy

IS 07 Acceptable Use Policy

IS 08 Clear Desk and Clear Screen Policy

IS 04 Risk Management Policy

IS 05 Information Classification and Handling Policy

IS 06 Information Security Awareness and Training Policy

IS 07 Acceptable Use Policy

IS 08 Clear Desk and Clear Screen Policy

IS 09 Mobile and Teleworking Policy

IS 10 Business Continuity Policy

IS 11 Backup Policy

IS 12 Malware and Antivirus Policy

IS 13 Change Management Policy

IS 14 Third Party Supplier Security Policy

IS 15 Continual Improvement Policy

IS 16 Logging and Monitoring Policy

IS 17 Network Security Management Policy

IS 18 Information Transfer Policy

IS 19 Secure Development Policy

IS 20 Physical and Environmental Security Policy

IS 21 Cryptographic Key Management Policy

IS 22 Cryptographic Control and Encryption Policy

IS 23 Document and Record Policy

**Information Security Roles and Responsibilities**

- Information Security Officer (ISO): Responsible for implementing and enforcing security policies.

- Employees: Required to comply with all information security policies and procedures.

**Monitoring Legal and Regulatory Obligations**

LanKiris Ltd will regularly monitor legal and regulatory requirements to ensure compliance with data protection laws such GDPR, intellectual property rights, and other relevant security standards.

**Policy Compliance**

Employees must understand their responsibilities under this policy. Non-compliance may result in disciplinary action up to and including termination.

**Compliance Measurement**

The ISO will report on the compliance with this policy through regular audits and reviews.

**Exceptions**

Any exceptions to this policy must be approved by the ISO in writing and approved by the CTO.

## **Continuous Improvement**

The policy will be reviewed and updated regularly to respond to the evolving security landscape and business needs.