Information Security Policy

Document Control

Date	22nd September 2023
Document Status	Live
Version	3.1
Date of Next Review	31st July 2024

CONTENTS

A.5 Information Security policies Objective

The established objectives of Information Security are;

Priority 1: Innovate

- To ensure OpenPlay's Leadership commit OP to the highest standards of Information Security
- To Achieve Cyber Security and ISO 27001 Certification: Develop a set of ISMS policy and procedures to maintain business continuity.

Priority 2: Operate

- Train all staff on information security to ensure responsibility for and awareness of ISMS procedures.
- To suffer 0 'Major' risks to OpenPlay's operations and information/cyber security
- All OP assets to be covered by antivirus protection.
- Improve audit and risk management activities to minimize risk and security breach.
- Embed ISMS and AnnexA policies into OP Business Management System and Risk Register

Priority 3: Grow

- Win future contracts and tenders as an outcome of enhanced Information Security commitments.
- Retain customers and supplier relationships by ensuring the security of our products and data.

To achieve its information security objectives, the organization shall monitor performance of;

- ISO 27001 Certification
- Review of ISMS risks as per defined process and closure of actions as per review
- Monitor Risk Treatment Plans and measure effectiveness of selected controls.
- Meet regulatory and legislative requirements
- Uptime of servers and Networks
- Customer feedback and Customer confidence
- Conducting of defined training requirements and awareness program as per the process
- Monitoring of security incidents as per process of Incident Management
- Report and investigate all breaches of information security and suspected weaknesses
- Closure of Non conformities in defined time frame
- Review of the BCP as per process and achievement of RT targets :
- Success rate of new contracts and customer contract renewal

The measures of these objectives are set out in 6.2.2 Information security objectives and planning to achieve them of the OPBMS.

The OP Information System Security Policy establishes requirements to ensure that information security controls remain current as business needs evolve and technology changes. This policy is published and communicated to all employees and relevant external parties.

A.5.1 Management Direction for Information Security

The **Head of Technology** is responsible for establishing, issuing and monitoring information security policies.

Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Information Security Policy Document

An OpenPlay Information System Security Policy document approved by the management exists. Information security policy has been published and communicated to all employees of OpenPlay through communications, training, and induction programs. The Information Security Policy contains operational policies, standards, guidelines, and metrics intended to establish minimum requirements for the secure delivery of our Products/ services. Secure service delivery requires the assurance of confidentiality, integrity, availability, and privacy of information assets through:

- Management and business processes that include and enable security processes;
- Ongoing employee awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Defining security responsibilities;
- Identifying, classifying, and labelling assets;
- Ensuring operational security, protection of networks, and the transfer of information;
- Safeguarding assets utilized by third parties;
- Reporting information security incidents and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

The **Head of Technology** recognises that information security is a process, which to be effective, requires executive and management commitment, the active participation of all employees, and ongoing awareness programs.

A.5.1.2 Review of the policies for information security

The Information Security Policy must be reviewed on an annual basis and updated when required. The purpose is to ensure information security policies remain current with evolving business needs, emerging risks, and technological changes.

The **Head of Technology** is responsible for the creation, maintenance, and updating of the policy. Information System Security Committee approves the policy prior to release. The review and evaluation of ISMS policy are conducted at least once a year. The review guidelines state that the policy is to be reviewed against its effectiveness, compliance to business process, and compliance to technology changes. The **Head of Technology** is responsible for reviewing information security policies, standards, and guidelines on an annual basis. Policies and standards reviews must be initiated:

- In conjunction with legislative, regulatory, or policy changes which have information security implications;
- During planning and implementation of new or significantly changed technology;
- Following a Security Threat and Risk Assessment of major initiatives (e.g., new information systems or contracting arrangements);
- When audit reports or security risk and controls reviews identify high-risk exposures involving information systems;
- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of the investigation into information security incidents;
- Prior to renewing third party access agreements which involve major programs or services;
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues; and,
- When associated external agencies (e.g., Information and Privacy Commissioner, Ministry on Information Technology) issue reports or identify emerging trends related to information security.

Signed on behalf of OpenPlay Ltd

Position: Sam Parton, OpenPlay Ltd CEO

Date: 22/09/2023