INFORMATION SECURITY POLICY

Document Control

Author	Sam Parton
Policy Owner	Ian Jones
Policy Sponsor	Sam Parton
Date	May 2024
Document Status	Live
Version	2.0
Date of Next Review	June 2026
Document Reference	Information Security Policy

Document Reviewers

Name	Position	Date of Review
Sam Parton	CEO	16th April 2020
Shaun Keating	Head of Technology	12th Sept 2020
Shaun Keating	Head of Technology	11th May 2021
Ian Jones	Head of Technology	31st July 2023
Ian Jones	CTO	May 2024
Ian Jones	CTO	June 2025

Change Record

Date	Staff	Version	Change Description
16th April 2020	Sam Parton	1.2	Grammar & restructure
12th Sept 2020	Shaun Keating	1.3	Change of policy sponsor
11th May 2021	Shaun Keating	1.4	Updated Branding
31st July 2023	Ian Jones	1.5	Updated for Audit
25th Sept 2023	Ian Jones	1.6	Updated contents and headings
May 2024	Ian Jones	2.0	Updated for ISO 27001:2022 and added new control updates

CONTENTS

1. INTRODUCTION

Information is a high-value commodity and business asset. OpenPlay Ltd (OpenPlay) has legal, regulatory, and moral obligations to ensure that its business information (including that of its customers and clients), technology systems, and processes are afforded appropriate protection to preserve our corporate reputation, brand, and market credibility.

2. OBJECTIVES

The objectives of this policy are to:

a) Achieve our Strategic Ambition to improve and adapt a process approach.

b) Protect information assets that OpenPlay handles, stores, exchanges, processes, and has access to, ensuring the ongoing maintenance of their confidentiality, integrity, and availability.

c) Implement controls proportional to the value of information assets and threats to which they are exposed.

d) Define high-level information security governance practices and principles to address all known and perceived risks and threats to our information security.

e) Comply with relevant legislation, regulation, and best practices for the protection of data, intellectual property, brand, and reputation.

f) Continually improve the organisation's Information Security Management System (ISMS) and its resilience against threats that could compromise information security.

3. SCOPE

This policy applies to all business entities within OpenPlay, including:

a) All locations where business activities are conducted and information is processed.

b) All business, customer, and employee information processed, stored, or transmitted throughout our company, irrespective of its form.

c) Information technology (IT) systems and applications used for operational business activities, including telephony and mobile systems and devices.

d) External parties, service providers, and business partners who provide services in respect of information processing facilities and processes in support of our business activities.

4. POLICY STATEMENTS

In pursuance of our legitimate business activities, we shall implement and maintain an ISMS certified as compliant with ISO 27001:2022 to ensure:

a) Systematic identification of security threats and application of a risk assessment procedure to implement appropriate control measures.

b) Planning, implementing, and controlling business systems and operational processes to meet information security requirements based on our operational risk assessments.

c) Adoption of privacy and security by design processes to reduce risks associated with unauthorised access, use, disclosure, abuse, falsification, or destruction of information assets.

d) Maintenance of a register of information and technology assets.

e) Implementation of formal user registration and de-registration procedures for granting and revoking access to information systems.

f) Provision of appropriate information, instruction, and training for all employees to support ISMS implementation.

g) Denial of access to business information technology infrastructure systems and applications by default unless specifically authorised.

h) Revocation of access rights immediately upon termination of employment, contract, or agreement.

i) Compliance with statutory, legal, regulatory, and contractual obligations.

j) Ensuring that hardware, software/applications, and other materials are used according to contractual agreements and copyright laws.

k) Implementation and testing of Business Continuity and Incident Response policies.

l) Reporting and investigating breaches of security through an Incident Response Form and Risk Register.

m) Regular review and revision of policies to reflect system design and technical implementation.

n) Quarterly or as-needed reviews of information security procedures by the Senior Management Team.

5. USE OF THIRD PARTIES

Engagement of third parties for business operations shall involve identification, assessment, and management of risks. Formal contracts with third parties storing, processing, or transmitting our information will define obligations and security requirements, including responsibilities and expected behaviours. We may conduct periodic reviews of third parties to ensure service delivery targets, standards, and information security controls are met.

6. RISK MANAGEMENT

A systematic approach to risk impact assessments will consider potential threats and vulnerabilities to create an effective operational security framework. Risk assessments will include the likelihood and magnitude of harm from unauthorised access, use, disclosure, disruption, modification, or destruction of information systems. Regular risk assessments will identify evolving threats and associated technical vulnerabilities.

7. RESPONSIBILITIES

Roles and responsibilities for information security management and governance will be assigned to meet strategic aims and business objectives. The Head of Development is accountable for ensuring information security requirements are met and periodically measured for effectiveness.

8. ACCOUNTABILITY

The Senior Management Team will ensure appropriate information security requirements and controls are applied proportionately across the business. Responsibilities include approving and endorsing policies, supporting the implementation of an information security program, creating a security-aware culture, and continually assessing and improving the effectiveness of information security.

9. LEGAL COMPLIANCE

The CEO will manage information security at a governance level, ensuring alignment with OpenPlay's mission statement, vision, and values. Responsibilities include conducting annual risk assessments, maintaining contingency plans, ensuring third party compliance with information security policies, and conducting legal due diligence of third parties.

10. CTO

The CTO will handle technical matters including documentation, systems design, build, maintenance, and monitoring. Responsibilities include developing a strategy to manage information security risk, ensuring resources for implementing the information security governance program, and engaging independent security experts for periodic security controls assessments.

11. USERS

All OpenPlay users must be aware of their responsibilities for safeguarding data, IT systems, and information assets. Users will undergo induction training and annual refresher training on information security and data protection. User access permissions will be allocated, and users will be accountable for activities performed using their access.

12. INFORMATION CLASSIFICATION

Sensitive business information will be classified to indicate protection needs. Users will be made aware of appropriate controls for handling and storing information. Information will be retained, handled, and processed in accordance with applicable laws, regulations, and business requirements.

13. EMPLOYMENT SCREENING

Employment screening will be conducted for prospective employees, contractors, and part-time personnel according to job roles and potential exposures. Screening will be completed prior to granting access to business information and technology assets. Periodic rescreening may be conducted for individuals with regular access to sensitive information.

14. INFORMATION SECURITY REVIEWS

Processes will monitor and report on the performance and effectiveness of the information security program. Policies and standards will be reviewed annually or as needed. Technical testing, such as penetration tests and vulnerability scans, will be conducted annually or after significant changes to identify potential weaknesses and ensure correct implementation of security controls.

15. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

Security awareness training will be provided to all employees, contractors, and third-party service providers relevant to their roles. Training will be included in induction programs and refreshed annually or as required by legal/regulatory changes.

16. LEGAL AND REGULATORY CONSTRAINTS

Appropriate steps will be taken to comply with legal and regulatory obligations related to information security. Reasonable actions will be taken to assist law enforcement agencies with requests for records, audit trails, system logs, or other information.

17. DATA PROTECTION

Compliance with the Data Protection Act 2018 and other relevant regulations will be ensured. The Head of Development is responsible for discharging data controller duties on behalf of the Senior Management Team.

18. AUDIT

Audit activities will be planned and maintained to minimize business disruption. Audits will assess compliance with legal and regulatory requirements, policies, and procedures. Significant deviations will be reported for remediation and incorporated into the Risk Register.

19. EXCEPTIONS

Exceptions to policies require explicit approval from the Senior Management Team. An Exception Policy exists for processing and maintaining such instances.

20. VIOLATIONS

Violations of the Information Security Policy and supporting documents will be investigated and may result in disciplinary action, including termination of employment or contractual relations. Legal action may be taken against individuals or organisations breaching these rules.

Signed on behalf of Openplay Ltd

Position: Sam Parton, OpenPlay Ltd CEO

Date: 31/05/2024