RISK MANAGEMENT POLICY

Regulatory Requirements

The board of Jumbo Interactive Limited ('the Company') has established a system of risk oversight and management and internal controls.
The purpose of the system is to:
❑ Identify, assess, monitor and manage risk;
❑ Inform investors of material changes to the Company's risk profile; and
❑ Enhance the environment for capitalising on value creation opportunities.

Responsibility

Responsibility for the implementation and ongoing review of business and attendant risks is given to the Chief Executive Officer. Duties in relation to risk management include but are not limited to:
❑ Initiate action to prevent or reduce the adverse effects of risk;
❑ Control further treatment of risks until the level of risk becomes acceptable;
❑ Identify and record any problems relating to the management of risk;
❑ Initiate, recommend or provide solutions through designated channels;
❑ Verify the implementation of solutions; and
❑ Communicate and consult internally and externally as appropriate.

Ongoing review of the overall risk management program (inclusive of the review of adequacy of treatment plans) is to be conducted by external parties (eg, the Company's auditors) where appropriate.

Operational Context

Business Objectives
Within the context of the Board's plans and policies, the principal activities of the Company can be summarised as follows:
i.   the identification, evaluation and possible execution of investment opportunities thought to be worthwhile for any short, medium or long term purpose, to whatever degree or magnitude deemed appropriate whether or not such opportunities relate to securities listed on a securities exchange or directly owned assets of any type; and/or
ii.   the review of existing assets/investments for determination of the preferred strategy in relation to each asset/investment; and/or
iii.   consideration of the financing alternatives for the matters set out in (i) or (ii) above and the implications thereof; and/or
iv.   the provision of financial and management services.

Size of Business
The business of the Company is conducted all over Australia, the South Pacific Islands, the UK, and the USA, controlled from Brisbane head office, and overseen by the Board.

Environmental/Regulatory Context

The Company's risk management program extends to all aspects of the business, including financial, regulatory, operational, reputation, people (clients and staff) and environmental risks.

Identification, Analysis & Treatment of Risks

Risks to the business will be considered in relation to the following categories:

Risk	Likelihood	Potential impact	Treatment
Commercial and legal relationships	Medium	High	Formal communication approach, written engagements to ensure compliance and eliminate potential disputes.
Financial	High	High	Adoption of formal authority limits. Monthly management accounts prepared; half yearly and full year external audit and review.
Economic circumstances	Medium	Medium	Management collect data and frequently monitor the environment within the context of the Company's activities. Report to the Board any material changes recommended.
Personnel	Low	Medium	Reward and encourage key staff to ensure job satisfaction and high morale.
Pandemic	Low	High	Work from home arrangements
Natural events	Low	Low	Maintain and monitor disaster recovery and contingency plans.
Political circumstances	Low	Low	Management to collect data and monitor the environment within the context of the Company's activities frequently. Report to the Board any material changes recommended.
Technology and technical issues	Low	High	Covered by separate IT Plan (detailed below) to minimize risks.
Management activities and controls	Med	High	Adoption of formal authority limits.
Individual activities	Low	Low	Act within the mandate of the Company and the authority limits.

Information Technology Plan

Role of IT within the Business

The Company views Information Technology (IT) as a key enabler in efficient and effective management of its internal and external data flows and its ongoing operating functions.

In order to properly deliver its business IT requirements, the Company utilises a variety of industry recognized products, including:

- Microsoft Office running on Windows 10;
- Microsoft Security Essentials
- Broadband connection to the internet
- Linux Servers

Responsibility

The CTO is responsible for the overall running and upkeep of the system on-site.

Strategy

- **Back-up**
  Back-ups are done on a daily basis from the servers to a backup server and copied once a week to an external hard drive stored off site.
- **Security**
  Access to physical IT infrastructure is restricted to Company personnel.
- **Communications**
  Connections to multiple providers for Internet redundancy.

Annual review

An annual review is undertaken by the CTO. The CTO will review the entire IT plan and position, making recommendations on software and hardware issues and ideas.

Reporting

As the system requirements of the office are small, a formal reporting system is not justified and has not been established. If anomalies are detected, they are dealt with on a situation specific basis.

IT Disaster Recovery Plan

- **Responsibility**
  It is the CTO's responsibility to implement the disaster recovery plan, i.e. bring in the external hard disk and download files onto the servers and desktop computers.
- **Testing and Monitoring**
  The system is automatically tested through the daily usage. If any faults occur, these are dealt with immediately and fixed as soon as possible, depending on their priority.