INFORMATION SECURITY POLICY

1.1 Terms and Definitions

"we", "us" and "our" refer to BuzzSaw Media. "staff" and "users" means all of those who work under our control, including employees, contractors, interns etc.

1.2 Purpose and Scope

The aim of this top-level policy is to define the purpose, direction, principles, and basic rules for information security management. The purpose of this document is to briefly communicate our security policies.

1.3 Users and Responsibilities

Users of this document are staff, as well as relevant external parties. Further details and explanations can be provided by the BuzzSaw Media Compliance Team on request. The Operations Manager is responsible for all aspects of the implementation and management of these arrangements, unless noted otherwise.

2. Compliance and Assurance

BuzzSaw Media has established a compliance framework that enables the organisation to effectively identify and manage information security, privacy, and business risks. BuzzSaw Media ensures the security and confidentiality of the Source Data that is supplied under the agreements from customers for the verification of their individuals.

3. Risk and Information Security

BuzzSaw Media analyses and evaluates identified risks to gauge their severity, probability, and controllability and determines a relative Risk score. The respective Risk scores are evaluated against approved criteria (for accepting risks and identifying the acceptable levels of risk) to identify and prioritise risks requiring treatment. BuzzSaw Media's risk assessment practices are continually reviewed internally to ensure that a pragmatic business-led approach is adopted, best practice is maintained, and continuous improvement is achieved.

4. Personally Identifiable Information (PII) Protection

BuzzSaw Media considers Personally Identifiable Information (PII) to be treated with utmost degree of sensitivity and deserving of the highest information classification. Confidentiality of PII stored for transactional purposes is achieved via SFTP processes. We do not store any PII unless advised otherwise. We ensure that all clients and related parties sign suitable contracts for access to the data. These contracts will highlight the penalties of any misuse by the company and that it is the responsibility of the company to ensure that their internal process implements the terms and use of the data.

5. Data Breach Notifications

Where a security incident involving a Personal Data breach is detected, the Operations/Privacy Officer is to be immediately notified. We will ensure all necessary parties and organisations are notified in accordance with our legal, contractual, and regulatory obligations and within the requisite stipulated timeframes.

As an Australian business, personal data breaches must be reported to both affected individuals and the Office of the Australian Information Commissioner (OAIC) and may need to be reported to other relevant authorities including financial services providers, law enforcement bodies, professional associations, and regulatory bodies.

6. Change Management

6.1 Change Management Procedures

BuzzSaw Media implements procedures to address risks related to changes in systems and business circumstances. All changes, whether code development, architecture, or infrastructure, require an appropriate level of testing to be undertaken which provides a high level of confidence that the change will be successful and will not negatively impact production functionality.

7. Security in Change Management

BuzzSaw Media takes into account the security requirements of each request for change from a risk perspective, considering the risk, likelihood, required mitigation, and ultimately the risk severity

8. System Security

8.1 Cloud Security

BuzzSaw Media's cloud servers are protected by RackCorp Firewall with intrusion prevention systems (IPS) to identify and block threats in real-time. The cloud service provider is responsible for controlling access, logging and monitoring of the systems and infrastructure

8.2 Backup and Recovery

Backup copies of information, software and system images are taken and tested regularly. We ensure that the extent, frequency, and retention period of backups reflect business requirements, security requirements, the criticality of the information to continued operations, and legal or audit requirements. BuzzSaw Media's backup data is subject to the same logical and physical security controls as other data to protect the confidentiality, availability, and integrity of data.

9. Data Centres

All data is stored on cloud-based servers, utilising firewalls, and advanced encryption, which is used to protect all data and applications. Databases have built-in security that prevents unauthorised access from malicious actors. All transactions are user and IP address logged.

Databases are backed up multiple times a day. Processes are in place to monitor and test the failover sites as required to ensure the capacity for redundancy remains in place.

10. Network Security

BuzzSaw Media does not have an internal network. Network security is managed and controlled by RackCorp Pty Ltd. to protect the information in systems and applications

11. Legal and Regulatory Compliance

11.1 Cross Border Transfer of Information

BuzzSaw Media's policies are designed to ensure that all information is secure both in internal databases and when our customers are accessing it. Access to systems is monitored electronically, providing an auditable record of who, what and when data was accessed.

12. Insurance

BuzzSaw Media maintains Public Liability, Product Liability, Professional Indemnity, and Cybersecurity insurance at all times. BuzzSaw Media actively reviews the insurance on a needs basis and at least once a year. We expect and request a similar level of insurance coverage from our contracting counterparts.

13. Client Information Security Requirements

All Clients or Customers using BuzzSaw Media Systems and Services, are expected to implement and maintain minimum information security requirements.

14. Supplier Due Diligence

BuzzSaw Media has measures in place to ensure our data sources are externally verified and certified to ensure reliability, accuracy, and legality of service. All our data source suppliers (“Suppliers”) undergo robust due diligence.

17. Breach of Policy

We will take all necessary measures to remedy any breach of this policy including the use of our disciplinary or contractual processes where appropriate.