Marshall Creative Data Security and Protection Policy

1. Purpose and Scope

Protecting the confidentiality, integrity, and availability of data is of utmost importance to Marshall Creative. This Data Security and Protection Policy aims to establish a framework for safeguarding sensitive information, ensuring compliance with data protection laws, and maintaining the trust of our clients, employees, and partners.

2. Data Security Objectives

- Confidentiality: Ensure that sensitive data is only accessible to authorized individuals and is not disclosed to unauthorized entities.
- Integrity: Guarantee the accuracy and reliability of data by preventing unauthorized alterations, deletions, or modifications.
- Availability: Ensure that data is available to authorized users when needed and that disruptions to data access are minimized.

3. Compliance with Data Protection Laws

Marshall Creative is committed to complying with all applicable data protection laws and regulations, including but not limited to GDPR, CCPA, and any other relevant local or international standards.

4. Risk Assessment and Management

Regular risk assessments will be conducted to identify potential threats and vulnerabilities to data security. Appropriate measures will be implemented to manage and mitigate these risks effectively.

5. Data Classification and Handling

All data will be classified based on its sensitivity, and appropriate security controls will be implemented accordingly. Employees will be educated on the proper handling and storage of different types of data.

6. Access Controls

Access to sensitive data will be restricted to authorized individuals based on their job roles and responsibilities. Access controls will be regularly reviewed and updated to align with changes in personnel or responsibilities.

7. Data Encryption

Sensitive data, both in transit and at rest, will be encrypted to prevent unauthorized access and ensure that even in the event of a security breach, the data remains secure.

8. Data Breach Response and Notification

In the event of a data breach, Marshall Creative will have a well-defined response plan to contain the incident, assess the impact, and notify affected parties in accordance with legal requirements.

9. Employee Training and Awareness

All employees will undergo training on data security practices, including the recognition of potential security threats, the proper handling of sensitive information, and their responsibilities in maintaining data security.

10. Vendor Management

When third-party vendors are involved in data processing, we will ensure that they adhere to similar data security standards. Vendor contracts will include provisions to safeguard the data they handle on our behalf.

11. Data Retention and Disposal

Data will only be retained for the necessary duration, and its disposal will be carried out securely, ensuring that no sensitive information remains accessible after it is no longer needed.

12. Continuous Monitoring and Improvement

Marshall Creative is committed to continuously monitoring and improving our data security practices. Regular audits, reviews, and updates to security protocols will be conducted to ensure the ongoing effectiveness of our data protection measures.

13. Review and Revision

This Data Security and Protection Policy will be reviewed periodically to ensure its continued relevance and effectiveness. Necessary revisions will be made to adapt to changes in laws, regulations, and industry best practices.

This Data Security and Protection Policy reflects Marshall Creative's dedication to maintaining the highest standards in data security, protecting the confidentiality of sensitive information, and ensuring the trust of our clients and stakeholders.

Signed
Darren Marshall [DIRETCTOR]

21st Jan 2024