DATA PROCESSING ADDENDUM FOR ADVERTISERS

This Data Processing Addendum ("**DPA**") forms an integral part of the Magic Affiliates Terms and Conditions for Advertisers ("**Main Agreement**") between Magic Square Int Ltd (**"Company**") and the counterparty agreeing to its terms ("**Advertiser**"; each a "**Party**" and together the "**Parties**"), in the context of which Personal Data is disclosed to or processed by the Advertiser, and are agreeing to this Data Protection Addendum ("**DPA**").

This DPA will be effective, and replaces any previously applicable terms relating to its subject matter, from the Terms Effective Date.

If you are accepting this DPA on behalf of Advertiser, you warrant that: (a) you have full legal authority to bind Advertiser to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Advertiser, to this DPA. If you do not have the legal authority to bind Advertiser, please do not accept this DPA.

1. INTRODUCTION

1.1 This DPA reflect the Parties' agreement on the processing of Personal Data in connection with the Data Protection Laws.

1.2 Any ambiguity in this DPA shall be resolved to permit the Parties to comply with all Data Protection Laws.

1.3 In the event and to the extent that the Data Protection Laws impose stricter obligations on the Parties than under this DPA, the Data Protection Laws shall prevail.

2. DEFINITIONS AND INTERPRETATION

2.1 In this DPA:

2.1.1 "**Approved Jurisdiction**" means a jurisdiction approved as having adequate legal protections for data by the European Commission, or by the UK Information Commissioner's Office, where applicable.

2.1.2 "**Data Protection Laws**" means, as applicable, any and/or all applicable domestic and federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"), Data Protection Act 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. ("**CCPA**"), and any amendment or replacements to the foregoing.

2.1.3 "**Data Subject**" means a natural person to whom Personal Data relates.

2.1.4 "**Personal Data**" means any information which could be used, either directly or by employing additional means, to identify a natural person, and that is shared with or processed by the Advertiser in the context of the performance of the Main Agreement.

2.1.5 "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data Breach will comprise a Security Incident

2.1.6 "**Standard Contractual Clauses**" mean Module One (Controller to Controller) of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council from 4 June 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en, subject to the applicable amendments contained in Schedule A.

2.1.7 "**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses, as issued by the UK Information Commissioner's Office, under S119A(1) of the Data Protection Act 2018.

2.1.8 "**Terms Effective Date**" means the effective date of the Main Agreement.

2.1.9 The terms "**Controller**", "**Processing**", "**Process**" and "**Processor**" as used in this DPA have the meanings given to them in Data Protection Laws. Where applicable, controller shall be deemed as a "**Business**" and processor shall be deemed to be a "**Service Provider**", as these terms are defined in the CCPA.

2.1.10 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. APPLICATION OF THIS DPA

3.1 This DPA will only apply to the extent all of the following conditions are met:

3.1.1 Either Party processes Personal Data that is made available by the other Party in connection with the Main Agreement;

3.1.2 The Data Protection Laws apply to the processing of Personal Data.

3.2 This DPA will only apply to the services for which the Parties agreed to in the Main Agreement, which incorporates the DPA by reference.

4. ROLES AND RESTRICTIONS ON PROCESSING

4.1 **Independent Controllers**. Each Party:

(a) is an independent controller of Personal Data under the Data Protection Laws;

(b) as required under the Data Protection Laws, maintain accurate written records of all the processing activities conducted by that Party in relation to any Personal Data for the purposes of performing its respective obligations under the Main Agreement;

(c) will individually determine the purposes and means of its processing of Personal Data;

(d) will be responsible to ensure that any Personal Data collected and processed by such Party is accurate and remains accurate for the duration of its processing;

(e) will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of Personal Data;

(f) will be responsible to exercise and respond to any requests by data subjects to exercise their rights under Data Protection Law, including (but not limited to) Articles 15-22 of the GDPR ("**Data Subject Rights**"), and shall provide reasonable cooperation and assistance to the other Party in connection with exercising Data Subject Rights;

(g) will promptly notify the other Party of any circumstances in which such Party is unable or becomes unable to comply with this DPA or Data Protection Laws, or any actual or potential changes to Data Protection Laws, if this shall affect the other Party's ability to comply with its obligations under this DPA or Data Protection Laws.

4.2 **Restrictions on Processing**. Section 4.1 (Independent Controllers) will not affect any restrictions on either Party's rights to use or otherwise process Personal Data under the Main Agreement.

4.3 **Sharing of Personal Data**. In performing its obligations under the Main Agreement, the Advertiser shall process Personal Data provided by the Company (i) only for the purposes set forth in the Main Agreement or as otherwise agreed to in writing by the Parties, provided such processing strictly complies with (a) Data Protection Laws, and (b) its obligations under the Main Agreement (the "**Permitted Purposes**"), provided that it will not do or permit any act or omission which would cause the Company to incur any liability under Data Protection Laws, and (ii) solely during the term of the Main Agreement, and shall securely delete or return the copies of the disclosed Personal Data to the Company (by secure file transfer in such format as the Company reasonably requests) and cease the processing of the disclosed Personal Data, and shall certify to the Company to that effect, unless and only insofar as the processing of the Personal Data is required for the fulfillment of the Permitted Purposes or is permissible under Data Protection Laws, and in which case the Advertiser will inform the Company of any such requirement and only further process the Personal Data as necessary to comply with the foregoing.

4.4 **Lawful grounds and transparency.** Each Party shall maintain a publicly-accessible privacy notice that satisfies transparency disclosure requirements of Data Protection Laws, and warrants and represents that it has provided Data Subjects with appropriate transparency regarding data collection and use and all required notices, in accordance with Data Protection Law, including Articles 13 and 14 of the GDPR. Where either Party collects Personal Data and discloses such Personal Data to the other Party, then the disclosing Party shall ensure it has obtained and recorded any and all consents or permissions necessary under Data Protection Laws, or other applicable lawful grounds, in order for itself and the other Party to Process such Personal Data as set out herein. The foregoing shall not derogate from either Party's responsibilities under the Data Protection Laws (such as the requirement to provide information to the Data Subject in connection with the processing of Personal Data). Both Parties will cooperate in good faith in order to identify the information disclosure requirements and each party hereby permits the other Party to identify it in the other Party's privacy policy, and to provide a link to the other Party's privacy policy in its privacy policy.

4.5 **Subcontracting.** Where either Party subcontracts the processing activities of Personal Data contemplated herein to a third party, it shall ensure that such third party enters into written contractual obligations which are (in the case of a third party controller) no less onerous than those imposed by this DPA or (in the case of a third party processor) compliant with Article 28 of the GDPR. Each Party shall be liable for the acts or omissions of its subcontractors to the same extent it is liable for its own actions or omissions under this DPA.

5. PERSONAL DATA TRANSFERS

5.1 Where the GDPR is applicable, either Party may transfer Personal Data outside the European Economic Area or an Approved Jurisdiction, subject to one of the appropriate safeguards in Article 46 of the GDPR.

5.2 Where the UK GDPR is applicable, either Party may transfer Personal Data outside the UK or an Approved Jurisdiction, subject to one of the appropriate safeguards in Article 46 of the UK GDPR.

5.3 Where the GDPR is applicable, then to the extent that Advertiser or its subcontractors process Personal Data outside the European Economic Area ("**EEA**") or an Approved Jurisdiction, then the Parties shall be deemed to enter into the Standard Contractual Clauses, which are incorporated herein by reference, subject to any amendments contained in Schedule A.

5.4 Where the UK GDPR is applicable, then to the extent Advertiser or its subcontractors process Personal Data outside the UK or a third country's system covered by UK adequacy regulations issued under the UK GDPR, the Parties shall be deemed to enter into the Standard Contractual Clauses, including and subject to the UK Addendum, which are incorporated herein by reference, subject to any amendments contained in Schedule A.

5.5 If the Standard Contractual Clauses or the UK Addendum (where applicable) are superseded by a new or modified legal mechanism for transfers of Personal Data, the new or modified legal mechanism for transfers of Personal Data shall be deemed to be incorporated into this Addendum, and the Parties will promptly begin complying with such legal mechanism for transfers of Personal Data.

6. PROTECTION OF PERSONAL DATA.

6.1 The Parties will provide a level of protection for Personal Data that is at least equivalent to that required under Data Protection Laws. Both Parties shall implement appropriate technical and organizational measures to protect the Personal Data.

6.2 In the event that a Party suffers a confirmed Security Incident with respect to Personal Data disclosed from the other Party, such Party shall notify the other Party without undue delay and the Parties shall cooperate in good faith to agree and take such measures as may be necessary to mitigate or remedy the effects of the Security Incident. In the event that a Party suffers a confirmed Security Incident, then such Party shall be responsible to notify the supervisory authority and/or the Data Subjects with respect to such Security Incident, as required under Data Protection Laws.

7. MUTUAL ASSISTANCE

7.1 Each Party shall:

7.1.1 appoint at least one representative as point of contact and responsible manager for all issues arising out of the Data Protection Laws (a "**Designated Representative**"); the Designated Representative(s) of both Parties will work together in good faith to reach an agreement with regards to any issues arising from time to time in relation to the processing of Personal Data in connection with the Main Agreement and this DPA;

7.1.2 use reasonable measures to consult with the other Party about any notices given to Data Subjects in relation to the processing of Personal Data under the Main Agreement;

7.1.3 inform the other Party (without undue delay) in the event that it receives a Data Subject request related solely and exclusively to the other Party's respective processing activities and provide all reasonable assistance to ensure Data Subject requests are completed within the timeframe set out in Data Protection Laws;

7.1.4 provide the other Party with reasonable assistance (having regard to the data available to it) to enable the other Party to comply with any Data Subject request received by the other Party and to respond to any other queries or complaints from Data Subjects;

7.1.5 provide the other Party with such assistance as the other Party may reasonably request from time to time to enable the other Party to comply with its obligations under the Data Protection Laws including (without limitation) in respect of security, breach notifications, impact assessments and consultations with supervisory authorities or other regulators;

7.1.6 provide the other Party with such information as it may reasonably request in order to: (a) monitor the technical and organizational measures being taken to ensure compliance with the Data Protection Laws, or (b) satisfy any legal or regulatory requirements, including information reporting, disclosure and other related obligations to any regulatory authority from time to time;

7.1.7 in the event of an actual or potential Security Incident which does or is reasonably likely to affect the respective processing activities of both Parties, liaise with the other Party in good faith to consider what action is required in order to resolve the issue in accordance with the Data Protection Laws, and provide such reasonable assistance as is necessary to the other Party to facilitate the handling of such Security Incident in an expeditious and compliant manner.

8. OBLIGATIONS UNDER THE CCPA

8.1 To the extent that Advertiser processes Personal Data of Californian residents for a Business Purpose (as it is defined under the CCPA), it shall be regarded as a Service Provider and be subject to the following obligations:

8.1.1 Advertiser shall not sell such Personal Data (as the term "sell" is defined under the CCPA).

8.1.2 Advertiser is prohibited from retaining, using, or disclosing such Personal Data for a commercial purpose other than providing the services to the Company under the Main Agreement and from retaining, using, or disclosing such Personal Data outside of the Main Agreement.

8.1.3 Advertiser understands its obligations under this clause and will comply with them.

8.2 Notwithstanding the above, Advertiser shall not sell Personal Data it received from or collected on behalf of the Company.

9. DIRECT MARKETING

9.1 If Advertiser collects or processes Personal Data for the purpose of carrying out direct marketing activities (including, without limitation, email campaigns or text-message campaigns; collectively "**Direct Marketing**")**,** which promote services or products offered by the Advertiser or other third parties ("**Communications**"), then Advertiser shall:

9.1.1 Comply with any and all Data Protection Laws that apply to such activity, including without limitation the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and the e-Privacy Directive;

9.1.2 Ensure that is has provided the Data Subjects with any notice necessary as required under Data Protection Laws, prior to delivering any Communications;

9.1.3 Ensure that is has obtained and recorded the Data Subjects' affirmative consent or otherwise has a legitimate interest, as expressly permissible under applicable Data Protection Laws, for the purpose of carrying out Direct Marketing, prior to delivering any Communications;

9.1.4 Upon Company's request, provide the Company with any and all records relating to the Data Subjects' affirmative consent and notices provided to the Data Subjects;

9.1.5 Ensure that any and all Communications include a clear and conspicuous notice of the opportunity to opt-out of receiving future Communications, in an easy manner;

9.1.6 Comply with any request to opt-out or unsubscribe from receiving Communications, as soon as technically feasible, and in any event within no later than seven (7) days as of the receipt of such request;

9.1.7 Ensure that the recipient of a Communications shall not be required to pay a fee or provide any other information for the purpose of opting-out of receiving Communications;

9.1.8 Ensure that Communications are not delivered to any data subject that were indicated, either by the Company or otherwise, to be excluded from the receipt of Communications, as directed by the Company, from time to time.

9.1.9 Ensure that any and all Communications contain a clear and conspicuous identification that it is an advertisement or solicitation, and that the Communications do not contain any false or misleading information.

10. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR SUPERVISORY AUTHORITIES

10.1 If either Party is the subject of a claim by a Data Subject or a supervisory authority or receives a notice or complaint from a supervisory authority relating to its respective processing activities (a "**DP Claim**"), it shall promptly inform the other Party of the DP Claim and provide the other Party with such information as it may reasonably request regarding the DP Claim.

10.2 Where the DP Claim concerns the respective processing activities of one Party only, then that Party shall assume sole responsibility for disputing or settling the DP Claim.

10.3 Where the DP Claim concerns the respective processing activities of both Parties, then the Parties shall use all reasonable endeavors to cooperate with a view to disputing or settling the DP Claim in a timely manner; provided always that neither Party shall make any admission or offer of settlement or compromise without using all reasonable endeavors to consult with the other Party in advance.

11. LIABILITY

11.1 Notwithstanding anything else in the Main Agreement, the total liability of either Party towards the other party under or in connection with this DPA will be limited to the maximum monetary or payment-based amount at which that Party's liability is capped under the Main Agreement.

12. PRIORITY

12.1 If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

12.2 If there is any conflict or inconsistency between the terms of this DPA and the Standard Contractual Clauses or the UK Addendum (where applicable), the provisions providing the more stringent protection to Personal Data and the rights of individuals shall govern.

13. CHANGES TO THIS DPA.

13.1 No changes, modifications or amendments to this DPA shall be valid or binding, unless made in writing and signed by both Parties.

13.2 If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Data Protection Laws shall be deemed to be incorporated into this DPA, and each Party will promptly begin complying with such Data Protection Laws in respect of its respective processing activities.

Schedule A – Standard Contractual Clauses and UK Addendum Stipulations

1. This Schedule A sets out the Parties' agreed interpretation of their respective obligations under Module One of the Standard Contractual Clauses and under the UK Addendum.

2. The Parties agree that for the purpose of transfer of Personal Data between the Parties Company shall be deemed as the Data Exporter, and Advertiser shall be deemed as the Data Importer.

3. Where the transfer of Personal Data is subject to the GDPR and the transfer relies on the Standard Contractual Clauses, then the following amendments shall apply to the Standard Contractual Clauses:

   3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

   3.2. In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.

   3.3. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of The Republic of Ireland.

   3.4. In Clause 18(b) the Parties choose the courts of Dublin, the Republic of Ireland as their choice of forum and jurisdiction.

4. Where the transfer of Personal Data is subject to the UK GDPR and the transfer relies on the Standard Contractual Clauses, subject to the UK Addendum, then the following amendments shall apply to the UK Addendum:

   4.1. In Table 1: the “Exporter” is Company; the “Importer” is Advertiser; and the Parties details and signatures are included in this DPA and the Main Agreement;

   4.2. In Table 2: the first option is selected and the “Approved EU SCCs” are those Standard Contractual Clauses incorporated into this DPA;

   4.3. In Table 3: (1) Annex 1A and Annex 1B of the “Approved EU SCCs” shall be replaced by Annex I of this DPA; and (2) Annex II of the “Approved EU SCCs” shall be replaced by Annex II of this DPA;

   4.4. In Table 4: both the “Importer” and the “Exporter” can terminate the UK Addendum in accordance with section 19 of the UK Addendum.

5. For the avoidance of doubt, any changes required under the UK Addendum shall only apply to the processing of Personal Data which is subject to the UK GDPR.

6. The Parties shall complete Annexes I–II below, which are incorporated in the Standard Contractual Clauses by reference.

Annex I – Description of processing activities

A. Identification of Parties

"**Data Exporter**": Company;

"**Data Importer**": Advertiser.

B. Description of Transfer

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):
☐ Company's end-users or potential end-users or customers

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify):
☐ Contact information (name, age, gender, address, telephone number, email address etc.)
☐ Financial and payment data (e.g. credit card number, bank account, transactions)
☐ Device identifiers and internet or electronic network activity (IP addresses, GAID/IDFA, browsing history, timestamps)

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):
☐ None

The frequency of the transfer

The frequency of the transfer:
☐ One-off
☐ Continuous

Nature of the processing

☐ Storage
☐ Disclosure, dissemination or otherwise making available
☐ Erasure or destruction

Purpose of the transfer and further processing

As defined in the Main Agreement.

Retention period

Personal Data will be retained for the term of the Main Agreement.

Supervisory Authority

The competent supervisory authority shall be set in accordance with the provisions of Clause 13 of the Standard Contractual Clauses.

Annex II – Technical and Organizational Measures to Ensure the Security of the Data

Description of the technical and organizational measures implemented by the Data Importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Security Management

Advertiser maintains a written information security management system (ISMS), in accordance with this Annex, that includes policies, processes, enforcement and controls governing all storage/processing/transmitting of Personal Data, designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure; (b) identify reasonable foreseeable and internal risks to security and authorized access to Advertiser System, and (c) minimize security risks, including through risk assessment and regular testing. The information security program will include the following measures:

- Advertiser actively follows information security trends and developments as well as legal developments with regards to the services provided and especially with regards to Personal Data and uses such insights to maintain its ISMS, as appropriate.
- To the extent Advertiser processes cardholder or payment data (such as payment or credit cards), Advertiser will maintain its ISMS in accordance with the PCI DSS standard, augmented to cover Personal Data, or such other alternative standards that are substantially equivalent to PCI DSS for the establishment, implementation, and control of its ISMS. Additionally, Advertiser will be assessed against PCI DSS annually by an on-site assessment carried out by an independent QSA (Qualified Security Assessor) and upon Company's request, not to exceed once annually, Advertiser will provide Company with PCI DSS attestation of compliance.

Maintain an Information Security Policy

Advertiser's ISMS is based on its security policies that are regularly reviewed (at least yearly) and maintained and disseminated to all relevant Parties, including all personnel. Security policies and derived procedures clearly define information security responsibilities including responsibilities for:

- Maintaining security policies and procedures;
- Secure development, operation and maintenance of software and systems;
- Security alert handling;
- Security incident response and escalation procedures;
- User account administration;
- Monitoring and control of all systems as well as access to Personal Data.

Personnel is screened prior to hire and trained (and tested) through a formal security awareness program upon hire and annually. For service providers with whom Personal Data is shared or that could affect the security of Personal Data a process has been set up that includes initial due diligence prior to engagement and regular (typically yearly) monitoring.

Personal Data has implemented a risk-assessment process that is based on ISO 27005.

Secure Networks and Systems

Advertiser has installed and maintains a firewall configurations to protect Personal Data that controls all traffic allowed between Advertiser's (internal) network and untrusted (external) networks, as well as traffic into and out of more sensitive areas within its internal network. This includes current documentation, change control and regular reviews.

Advertiser does not use vendor-supplied defaults for system passwords and other security parameters on any systems and has developed configuration standards for all system components consistent with industry-accepted system hardening standards.

Protection of Personal Data

Advertiser keeps Personal Data storage to a minimum and implements data retention and disposal policies to limit data storage to that which is necessary, in accordance with the needs of its customers.

Advertiser uses strong encryption and hashing for Personal Data anywhere it is stored. Advertiser has documented and implemented all necessary procedures to protect (cryptographic) keys used to secure stored Personal Data against disclosure and misuse. All transmission of Personal Data across open, public networks is encrypted using strong cryptography and security protocols.

Vulnerability Management Program

Advertiser protects all systems against malware and regularly updates anti-virus software or programs to protect against malware – including viruses, worms, and Trojans. Anti-virus software is used on all systems commonly affected by malware to protect such systems from current and evolving malicious software threats.

Advertiser develops and maintains secure systems and applications by:

- Having established and evolving a process to identify and fix (e.g. through patching) security vulnerabilities, that ensures that all systems components and software are protected from known vulnerabilities,
- Developing internal and external software applications, including web-applications, securely using a secure software development process based on best practices, e.g. such as code reviews and OWASP secure coding practices, that incorporates information security throughout the software-development lifecycle,
- Implementing a stringent change management process and procedures for all changes to system components that include strict separation of development and test environments from production environments and prevents the use of production data for testing or development.

Implementation of Strong Access Control Measures

"**Advertiser System**" means the Advertiser's data center facilities, servers, networking equipment, and host software systems (e.g. virtual firewalls) as employed by the Advertiser to process or store Personal Data.

The Advertiser System will be accessible to employees, contractors and any other person as necessary to provide the services to Company. Advertiser will maintain access controls and policies to manage what access is allowed to the Advertiser System from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Advertiser will maintain corrective action and incident response plans to respond to potential security threats.

Advertiser strictly restricts access to Personal Data on a need to know basis to ensure that critical data can only be accessed by authorized personnel. This is achieved by:

- Limiting access to system components and Personal Data to only those individuals whose job requires such access; and
- Establishing and maintaining an access control system for system components that restricts access based on a user's need to know, with a default "deny-all" setting.

Advertiser identifies and authenticates access to all systems components by assigning a unique identification to each person with access. This ensures that each individual is uniquely accountable for its actions and any actions taken on critical data and systems can be traced to known and authorized users and processes. Necessary processes to ensure proper user identification management, including control of addition/deletion/modification/revocation/disabling of IDs and/or credentials as well as lock out of users after repeated failed access attempts and timely termination of idling session, have been implemented.

User authentication utilizes at least passwords that have to meet complexity rules, which need to be changed on a regular basis and which are cryptographically secured during transmission and storage on all system components. All individual non-console and administrative access and all remote access use multi-factor authentication.

Authentication policies and procedures are communicated to all users and group, shared or generic IDs/passwords are strictly prohibited.

Restriction of Physical Access to Personal Data

Any physical access to data or systems that house Personal Data are appropriately restricted using appropriate entry controls and procedures to distinguish between onsite personnel and visitors. Access to sensitive areas is controlled and includes processes for authorization based on job function and access revocation for personnel and visitors.

Media and backups are secured and (internal and external) distribution is strictly controlled. Media containing Personal Data no longer needed for business or legal reasons is rendered unrecoverable or physically destroyed.

Regular Monitoring and Testing of Networks

All access to network resources and Personal Data is tracked and monitored using centralized logging mechanisms that allow thorough tracking, alerting, and analysis on a regular basis (at least daily) as well as when something does go wrong. All systems are provided with correct and consistent time and audit trails are secured and protected, including file-integrity monitoring to prevent change of existing log data and/or generate alerts in cases of unauthorized access or anomalies of access. Audit trails for critical systems are kept for a year.

Security of systems and processes is regularly tested, at least yearly. This is to ensure that security controls for system components, processes and custom software continue to reflect a changing environment. Security testing includes:

- Processes to test rogue wireless access points,
- Internal and external network vulnerability tests that are carried out at least quarterly. An external, qualified party carries out the external network vulnerability tests,
- External and internal penetration tests using Advertiser's penetration test methodology that is based on industry-accepted penetration testing approaches that cover the all relevant systems and include application-layer as well as network-layer tests.

All test results are kept on record and any findings are remediated in a timely manner.

Advertiser does not allow penetration tests carried out by or on behalf of its customers.

In daily operations IDS (intrusion detection system) is used to detect and alert on intrusions into the network and file-integrity monitoring has been deployed to alert personnel to unauthorized modification of critical systems.

Incident Management

Advertiser has implemented and maintains an incident response plan and is prepared to respond immediately to a system breach. Incident management includes:

- Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of customers,
- Specific incident response procedures,
- Analysis of legal requirements for reporting compromises,
- Coverage of all critical system components,
- Regular review and testing of the plan,
- Incident management personnel that is available 24/7,
- Training of staff,
- Inclusion of alerts from all security monitoring systems,
- Modification and evolution of the plan according to lessons learned and to incorporate industry developments.

Advertiser has also implemented a business continuity process (BCP) and a disaster recovery process (DRP) that is maintained and regularly tested. Data backup processes have been implemented and are tested regularly.

Physical Security

Physical Access Controls

Physical components of the Advertiser System are housed in nondescript facilities ("**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned are assigned photo-ID badges that must be worn while the employees and contractors are at any of the

Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access

Advertiser provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Advertiser or of its affiliates.

Physical Security Protections

All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. Advertiser also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, etc.) with door contacts, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

Continued Evaluation

Advertiser will conduct periodic reviews of the Security of its Advertiser System and adequacy of its information security program as measured against industry security standards and its policies and procedures. Advertiser will continually evaluate the security of its Advertiser System to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.