DATA PROCESSING ADDENDUM

in accordance with Article 28 General Data Protection Regulation (GDPR)
(Revision of June 2020)

Preamble

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement or other written or electronic agreement between MIRAGE (Supplier) and Customer (Company) for the purchase of online services (including associated MIRAGE offline or mobile components) from MIRAGE (identified either as "Services" or otherwise in the applicable Agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent MIRAGE processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Supplier may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

All legal documents can be found at http://www.mirage-systems.de/legal

HOW TO EXECUTE THIS DPA

This DPA consists of two parts: the main body of the DPA, and Schedules 1 and 2.

To complete this DPA, Customer must:

- Request to sign the DPA by sending a sign request to privacy@mirage-systems.com. If possible add your Customer's Account Number (as set out on the applicable MIRAGE Order Form or invoice)

- Mirage will validate if customer is using a MIRAGE service or if there is an existing contract. After confirming that, MIRAGE will e-mail the customer to digitally sign the DPA. MIRAGE will provide the service for digitally signing.
- Once customer digitally signed the DPA, MIRAGE will sign it.

Upon receipt of the validly completed DPA by Customer and MIRAGE, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the MIRAGE entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with MIRAGE or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the MIRAGE entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor a Master Subscription Agreement directly with MIRAGE, but instead is a customer indirectly via an authorized reseller of MIRAGE services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

If the Customer entity signing this DPA has an individual contract which is not related to the above mentioned standard services of MIRAGE, this DPA can be applied for the duration of that contract. The contract information has to be added after the last page and it requires a separate signing of MIRAGE.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this

definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and MIRAGE, but has not signed its own Order Form with MIRAGE and is not a "Customer" as defined under the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data."

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"MIRAGE" means the MIRAGE entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being Mirage Computer Systems GmbH., a company incorporated in Germany.

"MIRAGE Group" means MIRAGE and its Affiliates engaged in the Processing of Personal Data.

"Sub-processor" means any Processor engaged by MIRAGE or a member of the MIRAGE Group.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, MIRAGE is the Processor and that MIRAGE or members of the MIRAGE Group will engage Sub-processors pursuant to the requirements set forth in Section 6 "Sub-processors" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer shall have sole responsibility for creating all conditions for the processing of the personal data disclosed to Processor being permissible in accordance with this Addendum and for furnishing proof of that permissibility. Customer shall in particular ensure that its instructions comply with the applicable Data Protection Laws. Customer shall have sole responsibility for the lawfulness of the processing operations ("Responsibility" as defined by Art. 4 no. 7 GDPR). This also applies in respect of the purposes and means of the processing provided for in this Addendum and the description of the relevant data. Customer shall inform Processor immediately and completely, if Customer discovers errors or irregularities in terms of data protection regulations applicable the processing operations. Processor shall inform Customer immediately, if Processor believes that an instruction might violate data protection regulations. The Parties agree that Processor in this respect relies on the accuracy and completeness of the information provided by Customer.

2.3 **MIRAGE's Processing of Personal Data.** MIRAGE shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii)

Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by MIRAGE is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. **RIGHTS OF DATA SUBJECTS**

3.1 **Data Subject Request.**

MIRAGE shall, to the extent legally permitted, promptly notify Customer if MIRAGE receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, MIRAGE shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, MIRAGE shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent MIRAGE is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from MIRAGE's provision of such assistance.

4. MIRAGE OBLIGATIONS

4.1 **Confidentiality**. MIRAGE shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. MIRAGE shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Reliability.** MIRAGE shall take commercially reasonable steps to ensure the reliability of any MIRAGE personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** MIRAGE shall ensure that MIRAGE's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 **Data Protection Officer.** MIRAGE is not obliged to appoint a Data Protection Officer. You can reach a designated contact person at privacy@mirage-systems.com.

Upon request, Customer and Processor shall cooperate with the Supervisory Authority in performing their duties. Processor shall inform Customer immediately about audits and measures of the Supervisory Authority in so far as they extend to this Addendum.

The creation of the register of the Customer's processing activities as required by Art. 30 (1) GDPR is the sole responsibility of Customer; upon request, Processor shall assist Customer by providing information relating to the processing of personal data under this Addendum.

Processor shall assist Customer in its efforts to fulfill the obligations as provided in Articles 32 to 36 of GDPR to protect personal data, to report data breaches, and to carry out data protection impact assessments and prior consultations.

5. Place of Processing

Processor shall process the relevant data in a member state of the European Union (EU) or in any other signatory state to the Agreement on the European Economic Area (EEA).

Processor shall only be entitled to transfer the data to countries outside the EU or outside the EEA (so-called "Third Country"), if the level of data protection as laid down in the General Data Protection Regulation (GDPR) is guaranteed for the relevant data in accordance with Articles 44 et seq. GDPR.

6. SUB-PROCESSORS

Customer hereby authorizes Processor to use Sub-processors.

In this respect, Processor undertakes:

a) to carefully select the Sub-processor in consideration of the Sub-processor's technical and organizational data protection measures
b) to engage the Sub-processor by written or electronic contract
c) to commit the Sub-processor to comply with the data protection requirements at least to the same extent as they apply to Processor in this Addendum

d) to ensure, where an involvement of Sub-processors in third countries is envisaged, that an adequate level of data protection as required by Articles 44 et seq. GDPR is ensured by the relevant Sub-processor, for example by concluding an agreement containing the EU Standard Contractual Clauses as approved by the EU Commission

6.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) MIRAGE's Affiliates may be retained as Sub-processors; and (b) MIRAGE and MIRAGE's Affiliates respectively may engage third-party Sub-processors as described in section 6.

6.2 **List of Current Sub-processors** and Notification of New Sub-processors. MIRAGE shall make available to Customer the current list of Sub-processors for the Services identified in Schedule 3. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("Sub- processor Lists"). Customer may find on MIRAGE's Legal Webpage (also accessible via http://www.mirage-systems.de/legal) a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, MIRAGE shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

6.3 **Right of Objection to New Sub-processors**. Customer may object to MIRAGE's use of a new Sub-processor by notifying MIRAGE promptly in writing within ten (10) business days after receipt of MIRAGE's notice in accordance with the mechanism set out in Section 6.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, MIRAGE will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If MIRAGE is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by MIRAGE without the use of the objected-to new Sub-processor by providing written notice to MIRAGE. MIRAGE will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

6.4 **Liability.** MIRAGE shall be liable for the acts and omissions of its Sub-processors to the same extent MIRAGE would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. SECURITY

Controls for the Protection of Customer Data. MIRAGE shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the schedule 2 - *Technical and Organizational Measures*. MIRAGE regularly monitors compliance with these measures. MIRAGE will not materially decrease the overall security of the Services during a subscription term.

Processor shall regularly control the internal processes as well as the technical and organizational measures so as to ensure that the processing operations in Processor's area of responsibility comply with the requirements of the applicable data protection law and the rights of the data subject are ensured.

8. Proofs; Inspections and Controls

Processor shall furnish proof to Customer on request compliance with the obligations as provided in this Addendum by appropriate means, such as:

- Presentation of the current technical and organizational measures;
- Self-disclosures or process descriptions of Processor;
- Proofs of the conduct of self-audits;
- In-house rules of conduct including an external proof of compliance;
- Certificates for data protection and/or information security;
- Approved rules of conduct pursuant to Art. 40 GDPR;
- Certificates pursuant to Art. 42 GDPR.

Nevertheless, if in individual cases inspections of Processor become necessary, these inspections shall be carried out at the expense of Customer by Customer itself or by an independent external auditor designated by Processor.

Processor may only designate auditors who have warranted to Customer their independence from Processor and have committed to maintain secrecy.

Inspections (on-site checks) of Processor by Customer or by auditors commissioned by Customer shall take place only upon prior agreement and announcement with a reasonable lead time (shall be announced 4 weeks in advance, if not necessary because of a wrongdoing/misconduct of the Processor) and at customary business hours. Customer shall ensure that the operations of Processor are not interrupted. The Customer will only carry out inspections to the extent necessary and that they have no influence on data security or the rights of third parties (e.g. other customer of Processor).

Customer shall bear, in addition to the charges of the auditor, the expenses incurred by Processor due to the inspection. This shall not apply, if the services are attributable to a wrongdoing/misconduct of the Processor, or are to be provided free of charge by law. Any costs incurred must be appropriate, must not hinder the Customer at fulfilling its legal obligations and have to be announced in advance by the Processor and agreed with the Customer. Control / audit reports are generally to be made available to the Customer free of charge.

9. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

MIRAGE maintains security incident management policies and procedures specified in the schedule 2 - *Technical and Organizational Measures* and shall, notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by MIRAGE or its Sub-processors of which MIRAGE becomes aware (a "Customer Data Incident"). MIRAGE shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as MIRAGE deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within MIRAGE's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

10. RETURN AND DELETION OF CUSTOMER DATA

MIRAGE shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the schedule 2 - *Technical and Organizational Measures*.

11. AUTHORIZED AFFILIATES

11.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between MIRAGE and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 11 and Section 12. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

11.2 **Communication**. The Customer who is the contracting party to the Agreement shall remain responsible for coordinating all communication with MIRAGE under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11.3 **Rights of Authorized Affiliates**. Where an Authorized Affiliate becomes a party to the DPA with MIRAGE, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

11.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against MIRAGE directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer who is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 11.3.2, below).

11.3.2 The parties agree that the Customer who is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on MIRAGE and its Sub-Processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

12. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and MIRAGE, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, MIRAGE's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

13. EUROPEAN SPECIFIC PROVISIONS

13.1 **GDPR.** With effect from 25 May 2018, MIRAGE will Process Personal Data in accordance with the GDPR requirements directly applicable to MIRAGE's provision of its Services.

13.2 **Data Protection Impact Assessment**. With effect from 25 May 2018, upon Customer's request, MIRAGE shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to MIRAGE. MIRAGE shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 13.2 of this DPA, to the extent required under the GDPR.

14. LEGAL EFFECT

This DPA shall only become legally binding between Customer and when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

15 Mandatory Written Form, Choice of Law

15.1 No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

15.2 In case of any conflict, the regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.

15.3 This addendum is subject to the laws of the Federal Republic of Germany.

Customer

Company Legal Name: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

Mirage Computer Systems GmbH

Signature: _____

Print Name: _____

Title: _____

Date: _____

If the DPA is regarding an individual contract add the contract information below. It requires an additional signing from Mirage to accept that contract information.

SCHEDULE 1 - DETAILS OF THE PROCESSING Nature and Purpose of Processing

MIRAGE will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 10 of the DPA, MIRAGE will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Customer history
- Billing and payment data
- Planning and management data
- Connection data
- Licensing data
- Phone call related data
- Localization data

Schedule 2 - Technical and Organizational Measures

MIRAGE's Corporate Trust Commitment

MIRAGE is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ("Customer Data").

Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to, the services listed in Schedule 3.

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

MIRAGE uses the Amazon Data Centers for all Services listed in Schedule 3. The Amazon - Mirage Data Processing addendum can be found at http://www.mirage-systems.de/legal

Control of Processing

MIRAGE has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by MIRAGE and its sub- processors. In particular, MIRAGE and its affiliates have entered into written agreements with their sub- processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by MIRAGE and its sub-processors are subject to regular audits.

Security Controls

The Covered Services include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use.

Security Policies and Procedures

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored encrypted
- User access log entries will be maintained. The logs could contain date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, MIRAGE can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

MIRAGE maintains security incident management policies and procedures. MIRAGE notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by MIRAGE or its agents of which MIRAGE becomes aware to the extent permitted by law.

MIRAGE publishes system status information on the MIRAGE Support Website.

User Authentication

Access to Covered Services requires authentication via one of the supported mechanisms as described including user ID/password, Two-Factor Authentication, Social Login as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. Details about the security measures are described in the Amazon / Mirage Data Processing Addendum which can be found at http://www.mirage-systems.de/legal

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Covered Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis. Any backups are verified for integrity and stored in the same data centers as their instance. The foregoing replication and backups may not be available to this extent for the Mirage uaCSTA Cloud service.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Covered Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event MIRAGE production facilities at the primary data centers were to be rendered unavailable.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Covered Services by a customer.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer).

MIRAGE shall provide such Customer Data via a downloadable file in comma separated value (.csv) format or as database backups .

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 40 days, after which it is securely overwritten or deleted from production

within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that MIRAGE uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, MIRAGE reserves the right to reduce the number of days it retains such data after contract termination.

Analytics

MIRAGE may track and analyze the usage of the Covered Services for purposes of security and helping MIRAGE improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

MIRAGE may share anonymous usage data with MIRAGE's service providers for the purpose of helping MIRAGE in such tracking, analysis and improvements. Additionally, MIRAGE may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

SCHEDULE 3 – Mirage Services

The following services are provided in Data Centers

- Activation Server – hosted cloud version
- License Protector – Cloud Edition
- All-In-One Protector – Cloud Edition
- Mirage Cloud Service - CTI
- Mirage uaCSTA Cloud Connect - CTI