

---

**SCOUT BY MILLER HEIMAN GROUP™**  
**SOFTWARE AS A SERVICE TERMS AND CONDITIONS**

These Software as a Service Terms and Conditions (“**SaaS Terms**”) shall apply with respect to licensing by Client of Scout by Miller Heiman Group, and will apply to any agreement entered after March 4, 2019.

**1. SERVICES**

1.1 Hosted Service. Miller Heiman Group, Inc. and/or its affiliates identified in the agreement between the Parties (“**MHG**”) shall make available to Client those components of MHG’s Scout by Miller Heiman Group™ cloud-based solution and/or other related software or service (the “**Hosted Service**”) described in a Client Confirmation Form (“**CCF**”) or other ordering document agreed upon by the parties (“**Order Document**”) providing for the licensing of Scout. MHG also shall provide to Client those user guides, documentation, and training materials (including any updates or amendments to such guides, documentation, and materials) regarding the Hosted Service made generally available by MHG to its clients (the “**Documentation**”).

1.2 Implementation Services. MHG will provide the following services to support Client’s deployment of Scout by Miller Heiman Group, (“**Implementation Services**”), provided that Client shall assist MHG and carry out all tasks reasonably necessary for the implementation of the Hosted Service or Other Services (defined below), as applicable, including without limitation providing to MHG all requested information:

- (a) Implementation Services will include:
  - (i) Initial Discovery and Planning
  - (ii) Stand-up of SaaS and Provisioning Admin Access
  - (iii) Client Admin Training
  - (iv) User Training
- (b) Client Success Services will include periodic sharing of information about usage of the methodology and technology with recommendations for how to improve.
- (c) The Client will identify and assign the following resources for the implementation period to support the Company work:
  - (i) Project Manager: Key point of contact for all areas of deployment within the Client environment. Responsible for delivering communications, aligning with Client strategy, and working closely with the Company

resources to ensure alignment of the technology story with the Client strategy.

- (ii) IT Resource: Key Client IT point of contact to align on infrastructure needs, firewall and other security settings, any CRM integration options, and Client IT policy alignment.
- (iii) Sales Team Advocate: A senior leader in the Client sales team who acts as the champion of this change management project, providing strategic direction to the Client resources herein, and align closely with the client success lead to ensure adoption and change management with the Client sales resources.
- (iv) Helpdesk Support Contact: Client will provide end user support and will designate a single primary contact to interface with Miller Heiman Group support team

(d) Additional services beyond those set forth above, or in excess of 40 hours, may be provided in accordance with MHG’s then prevailing rates, as agreed upon by the Parties.

1.3 Other Services. MHG may also provide to Client services other than the Hosted Service or Implementation Services as described in a separate SOW (the “**Other Services**”), which may be subject to different or additional fees and terms as agreed by the Parties. The Hosted Service, Implementation Services and Other Services will collectively be referred to herein as the “**Services**”.

1.4 Statements of Work. Other Services, where applicable, will be specified in one or more CCFs or Statements of Work (“**SOW**”) executed by the parties and each of which will incorporate these SaaS Terms as though fully set forth therein. A CCF, Order Document or SOW (if applicable) together with these SaaS Terms is referred to as the “**Agreement**.” In the event of a conflict between any of the terms of these SaaS Terms and the terms of a SOW, the terms of the SOW shall prevail with respect to the Professional Services or Other Services that are the subject of such SOW only. In the event of a conflict between these SaaS Terms and an Order Document, these SaaS Terms shall prevail unless a specific provision that is intended to be modified is

expressly identified as being modified by written agreement.

1.5 Maintenance and Technical Support. MHG may install software updates, bug fixes, upgrades and error corrections in the Hosted Service as MHG deems necessary from time to time, provided that such updates or installations are not inconsistent with the terms of the Agreement.

1.6 Suspension of Access to Hosted Service. MHG may suspend Client's access to the Hosted Service at any time (a) in order to prevent damage to, or degradation of, MHG's network integrity; (b) if Client has failed to pay any amounts for thirty (30) days after MHG notifies Client of such past due amounts; (c) if Client has breached this Agreement in a way that affects MHG's provision of the Hosted Service or infringes on MHG's or any third party's intellectual property rights; or (d) if Client violates applicable laws (including without limitation any violation of Section 9.10 (Compliance with Laws)), or any obligations of confidentiality or privacy to any third party, or governmental regulations or is subject to a court order requiring suspension. If suspended, MHG will promptly restore use of the Hosted Service to the Client after the event giving rise to the suspension has been resolved to MHG's reasonable satisfaction. Any accounts that are restored after suspension under this paragraph may be subject to MHG's then-current reactivation fees. Client shall not be entitled to a refund or credit on any fees if access to the Hosted Service is suspended under subsections (b), (c) or (d).

## 2. RIGHTS

2.1 Right to Use the Hosted Service. Subject to Client's timely payment of all applicable fees, MHG hereby grants to Client, during the term of the corresponding CCF or other Ordering Document, a non-exclusive, non-transferable (except to the extent otherwise expressly permitted by Section 9 (General) below), right and license to provide the number of individual licenses to its employees ("User Licenses") to access and use the Hosted Service for internal business purposes only (and not as a service bureau) and subject to any limitations set forth herein or in the applicable SOW. Client shall not disclose or otherwise allow access to the Hosted Service or Documentation to any third party, including but not limited to, other system service providers, outsourcers, or to any party that it should reasonably be aware may compete with MHG, except as expressly permitted by MHG in writing. The Hosted Service includes unpublished software, trade secrets and

confidential or proprietary information of MHG or its licensors and is developed exclusively at private expense.

- (a) Client may add additional User Licenses for additional employees by (i) executing a CCF setting forth the number of additional User Licenses and applicable fees, or (ii) by Email or Telephone for the applicable per User License fee, which will be pro-rated and invoiced in such amount for the remainder of the then current Term. Each additional User License will be subject to these Terms and Conditions, and will renew concurrently with other User Licenses purchased.
- (b) User Licenses must not be shared by more than one employee, and at no time may the total number of users exceed the number of User Licenses purchased. Client will not receive a refund for any unused or partially used User Licenses. If an employee is terminated, Client must remove/terminate such employee's access to the Hosted Service. Client may reassign User Licenses of terminated employees to a different user.

2.2 Use Restrictions. Client shall not and shall not assist anyone else to: (a) access and/or use the Hosted Service or the Documentation in order to design, create or build a service or product that is competitive with the Hosted Service, or which uses ideas, features or functions that are similar to the Hosted Service; (b) license, sublicense, sell, resell, resyndicate, transfer, assign, distribute, lease, rent, loan, or otherwise commercially exploit or make available to any third party the Hosted Service or the Documentation; (c) combine or permit sharing of User Licenses by more than one employee; (d) use the Hosted Service for purposes of providing a service bureau; (e) modify, translate, or make derivative works based upon the Hosted Service or the Documentation or any part thereof, or directly or indirectly decrypt, decompile, disassemble, reverse engineer, or otherwise attempt to discover the source code of the Hosted Service or any portion thereof or its underlying ideas, techniques or algorithms, including the review of data structures or similar materials produced by the Hosted Service; or (f) directly or indirectly use the Hosted Service in violation of any applicable laws, including without limitation those set forth in Section 9.10 (Compliance with Laws). Except as explicitly granted in this Agreement, Client shall have no rights with respect to the Hosted Service or the Documentation.

2.3 Proprietary Rights. The Services, the MHG Data (excluding any Client Content included therein), and any modifications, configurations, enhancements or derivative works thereof to any of the foregoing (including all

intellectual property rights in or to any of the foregoing), are and shall remain the exclusive property of MHG and/or its licensors. No licenses or rights are granted to Client except for the limited rights expressly granted in this Agreement.

### 3. DATA

3.1 Client Content. Client hereby grants to MHG during the Term of this Agreement a limited right and license to use, process and reproduce, for the purpose of facilitating the performance of MHG's obligations under this Agreement, any information or data related to Client that is input or uploaded into the Hosted Service by Client, provided by Client to MHG for entry by MHG into the Hosted Service, or otherwise provided to MHG by Client pursuant to this Agreement (the "**Client Content**").

3.2 Data Usage and Data Security. MHG will use commercially reasonable efforts to adhere to the data security and privacy standards set forth in Exhibit A (Data Security Provisions) attached hereto and incorporated herein by reference.

3.3 Personally Identifiable Information. To the extent MHG has access to personally identifiable information, MHG agrees to use such information only for the purpose of this Agreement and as Client reasonably directs. Client and MHG will comply with all applicable laws relating to security and privacy and the protection of personally identifiable information.

3.4 MHG Data. Client agrees that MHG may (a) collect data arising out of Client's use of the Hosted Service, (b) collect metrics and data included in the Client Content, and (c) aggregate and analyze any metrics and data collected pursuant to subsections (a) and/or (b) of this sentence (collectively, the "**MHG Data**"). The MHG Data shall be de-identified to exclude any personally identifiable information. MHG shall not use the MHG Data in a way that identifies Client as the source of any data included in the MHG Data. Provided MHG complies with the two immediately preceding sentences, MHG Data does not constitute the Confidential Information of Client and MHG may provide the MHG Data to third parties. MHG may use, reproduce, distribute, and prepare derivative works from the Client Content solely as incorporated in the MHG Data.

3.5 Confidential Information. Through the relationship created by this Agreement each party may have access to certain information and materials considered by the other to be confidential and proprietary, or which should reasonably be considered confidential based on its subject matter or the circumstances of its

disclosure, including financial, corporate, personnel, client, supplier, operational and technological information, software, and trade secrets ("**Confidential Information**"). Except as otherwise expressly provided in this Agreement, MHG Data is the Confidential Information of MHG and Client Content is the Confidential Information of Client. All Confidential Information of the other may be used only for the purposes of this Agreement, will be protected from unnecessary disclosure within each party's respective organizations, and will not be disclosed to third parties (other than permitted subcontractors, attorneys, accountants, and other advisors who are bound by confidentiality and non-use restrictions at least as restrictive as those set forth herein). Further, Confidential Information will be subject to return or destruction in the event of termination or expiration of this Agreement. Each party will notify the other if such party learns of unauthorized use or disclosure of the other party's Confidential Information. Each party agrees that Confidential Information does not include information which is: (i) publicly known, (ii) already known to the recipient without an obligation of confidentiality, (iii) lawfully disclosed by a third party to a party without restriction, or (iv) independently developed without use of the other party's Confidential Information. In the event a judicial, legislative, or administrative body requests or threatens to compel disclosure of Confidential Information, the receiving party shall promptly notify the disclosing party and shall cooperate with the disclosing party's reasonable requests (at disclosing party's expense) to assist the disclosing party in obtaining a protective order and to prevent or minimize the disclosure of any Confidential Information. The receiving party may only disclose Confidential Information to the extent required by law.

3.6 Rights Notices. Client shall not remove any notices or legends that appear in the Services, Documentation, or on any output of the Services, that either serve to identify MHG as the owner, or that provide notice of the confidential and/or proprietary nature of such materials, and/or their contents, including without limitation copyright notices, trademark symbols and notices, and notices that such materials are "confidential" or "proprietary." Client's obligation not to remove such notices shall apply in all circumstances, including without limitation when Client copies or distributes materials as permitted by this Agreement.

### 4. FEES, PAYMENT, AND TAXES.

4.1 Fees. Fees for the Services are set forth in the applicable CCF or Order Document, and unless otherwise

set forth therein, undisputed fees are due and payable within thirty (30) days of the invoice date. All amounts that are past due will be subject to a monthly charge of one and one-half percent (1.5%) per month or the maximum rate permitted by the law, whichever is less. If Client fails to provide reasonable written notice of a good faith dispute after failing to make payments as required, MHG will be entitled, in addition to any other available remedies, to suspend all Services under this Agreement. Fees will be invoiced annually in advance (and as additional User Licenses are added) and are non-cancellable and non-refundable regardless of whether Client uses the services. If Client has received a discounted fee in connection with a multi-year commitment, and fails to pay the fees for subsequent years when they are due, MHG will invoice Client the difference between the standard Fee and the discounted fee paid for previous years, and client shall pay such invoice within thirty (30) days of the invoice date. Payments will be accepted via wire, ACH, check or credit card. If Client pays via credit card, Client shall pay MHG a 3% processing fee in addition to the invoice amount. Client acknowledges and agrees that the payment for any Services provided hereunder is not contingent on the provision of any purchase order or purchase order number.

4.2 Expenses. Client shall reimburse MHG for all reasonable out-of-pocket expenses incurred by MHG in connection with this Agreement, including travel-related expenses for pre-approved travel (with respect to Professional Services and Other Services, if applicable). Such expenses, may be separately invoiced to Client.

4.3 Taxes. Client will be responsible for and pay all applicable sales, use, excise, value added, services, consumption and other taxes and duties associated with MHG's performance or Client's receipt of MHG's Services, excluding taxes on MHG's income generally. Client will provide MHG with a copy of Client's certificate of tax-exemption, if applicable. If Client is required by the laws of any foreign tax jurisdiction to withhold income or profits taxes from MHG's payment, then the amount payable by Client upon which the withholding is based shall be paid to MHG net of such withholding. Client shall pay any such withholding to the applicable tax authority. However, if after 120 days of the withholding, Client does not provide MHG with official tax certificates documenting remittance of the taxes, Client shall pay to MHG an amount equal to such withholding. The tax certificates shall be in a form sufficient to document qualification of the taxes for the foreign tax credit allowable against MHG's corporation income tax. Should any agency,

entity, or authority pursue a claim against MHG to recover unpaid taxes or fees that should have been collected from Client, Client agrees to cooperate fully with MHG and/or the taxing authority and to reimburse MHG for any taxes determined to be due. Additionally, if MHG follows any instructions from Client regarding the collection of taxes and such collection results in interest and/or penalties being levied by a taxing authority, Client will reimburse MHG for such interest and/or penalties.

## 5. WARRANTIES.

MHG warrants that the Hosted Service will substantially perform in accordance with the Documentation and the Professional Services and Other Services will be performed in a professional and workmanlike manner. As Client's sole remedy for defective Services, MHG will repair or replace such Services. MHG represents and warrants that it will exercise commercially reasonable efforts, including the use of industry standard methods to detect and protect the Hosting Service and other electronically delivered materials against malicious program code insertions, and MHG will not knowingly introduce into the Hosting Service or other electronically delivered materials any virus or other malicious code. All service level commitments are set forth in Exhibit B (Service Level Agreement), attached hereto and incorporated herein by reference. EXCEPT AS OTHERWISE SET FORTH IN THIS SECTION 5, THE SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MHG EXPRESSLY DISCLAIMS (TO THE GREATEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW) ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT AND WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. MHG DOES NOT WARRANT THAT THE OPERATION OF THE SERVICES WILL BE COMPLETELY SECURE, ERROR-FREE OR UNINTERRUPTED, OR THAT ALL ERRORS WILL BE CORRECTED.

## 6. INDEMNIFICATION

MHG agrees to defend and indemnify Client and Client's owners, directors, employees, agents and representatives ("**Indemnified Parties**"), and to hold them harmless, from any and all claims and liabilities (including reasonable attorneys' fees) which may arise from third party patent, trademark or copyright infringement claims arising in connection with such

Indemnified Parties' authorized use of the Hosted Service, except to the extent that such infringement is attributable to (a) Client Content provided by Client or an Indemnified Party (b) any modification of the Hosted Service not performed by or authorized by MHG, or (c) the combination of the Hosted Service with any other technology, product or service not authorized by the Documentation, MHG or this Agreement. MHG reserves the right to control the defense of any such litigation, including the employment of counsel and payment of all expenses. Should the Hosted Service licensed hereunder, or any part thereof, become or, in MHG's exclusive opinion, be likely to become, the subject of a claim of infringement through no fault of Client, MHG shall at its sole option and expense either: (a) procure for Client the right to continue using the Hosted Service or portion thereof, (b) modify the Hosted Service to make it non-infringing, or (c) failing (a) or (b), terminate Client's access to the Hosted Service and refund any fees prepaid by Client for the Hosted Service.

## 7. LIMITED LIABILITY

EXCEPT WITH RESPECT TO CLAIMS ARISING FROM A BREACH OF CONFIDENTIALITY OBLIGATIONS, INDEMNIFICATION OR LICENSE RESTRICTIONS, EACH PARTY'S LIABILITY FOR ANY TYPE OF DAMAGES FOR ANY AND ALL CLAIMS, IN AGGREGATE, IS LIMITED TO THE AMOUNT OF FEES ACTUALLY PAID TO SERVICE PROVIDER DURING THE LAST 12 MONTHS UNDER THE AGREEMENT FROM WHICH THE CAUSE OF ACTION AROSE.

EXCEPT WITH RESPECT TO CLAIMS ARISING FROM A BREACH OF CONFIDENTIALITY OBLIGATIONS OR LICENSE RESTRICTIONS, NEITHER PARTY SHALL BE LIABLE FOR ANY PUNITIVE OR EXEMPLARY DAMAGES OR LOSS, NOR ANY LOST PROFITS, SAVINGS OR BUSINESS OPPORTUNITY, SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES.

## 8. TERM AND TERMINATION

8.1 Term. Unless otherwise specified in the CCF or Order Document, the initial term for all Services shall be one (1) year from the effective date of the applicable CCF or Order Document, and the term for the Hosted Service will automatically renew for consecutive one (1) year terms unless either party provides the other party with written notice at least thirty (30) days prior to the expiration of the then current term of its intention not to renew the Hosted Service. Unless otherwise set forth in the corresponding CCF or Order Document, all payments are non-refundable and all Services are non-cancelable during any current term except for any termination by Client for Cause pursuant to Section 8.2.

8.2 Termination for Cause. A party may terminate this Agreement for cause if the other party (a) materially breaches the terms of this Agreement and fails to cure such breach (if curable) within thirty (30) days of receiving written notification of such breach or (b) ceases to conduct business in the normal course, becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets, or avails of or becomes subject to any proceeding under the Federal Bankruptcy Code or any other statute of any state relating to insolvency or the protection of rights of creditors, or fails to have stayed, within sixty (60) days, any involuntary proceeding brought against it under the Federal Bankruptcy Code or similar statute.

8.3 Effects of Termination. Upon the termination of this Agreement or a SOW for any reason: the rights and licenses granted to Client in Section 2.1 (Right to Use the Hosted Service) shall terminate with respect to the Hosted Service and Client may not access the applicable Hosted Service, and (c) all amounts owed to MHG under the Agreement will become immediately due and payable. The following provisions of this Agreement shall survive any termination of this Agreement: 2.3 (Proprietary Rights), 3 (Data), 4 (Fees, Payment, and Taxes), 5 (Warranties), 7 (Limitation of Liability), 8.3 (Effects of Termination), and 9 (General).

## 9. GENERAL

9.1 Entire Agreement. This Agreement, together with the applicable CCF, SOW(s) and any exhibits hereto or thereto, constitute the entire understanding between the parties with respect to the subject matter contained herein and is intended as the complete and exclusive statement of the agreement between the parties with respect to the Services provided hereunder, superseding all prior agreements and negotiations relating to the Services contemplated hereunder.

9.2 Reference. MHG will not identify Client or Client's brand logo in promotional materials or on MHG's websites, presentations, or marketing collateral without Client's prior consent.

9.3 Irreparable Harm. The Parties acknowledge that any unauthorized use or disclosure of the Hosted Service or Documentation by Client or any breach by either Party of Section 3.5 (Confidential Information) would cause irreparable harm, and therefore, in addition to any other remedy available in law, the non-breaching Party will be entitled to immediate injunctive relief, without showing any actual damages sustained, to prevent such breach, disclosure or unauthorized use, and without obligation to

post a bond or other security in connection with obtaining an injunction, specific performance, or other relief.

9.4 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware without giving effect to conflict of law rules.

9.5 Force Majeure. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for payment obligations) on account of strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, data breach, earthquakes, material shortages, outages of electrical or Internet services, or any other cause that is beyond the reasonable control of such party (“**Force Majeure Event**”).

Upon the occurrence of a Force Majeure Event, the non-performing party shall promptly notify the other party of occurrence of that Force Majeure Event, its effect on performance, and how long that party expects it to last. During a Force Majeure Event, the nonperforming party will use reasonable efforts to limit damages to the performing party and to resume its performance under this Agreement.

9.6 Assignment. Neither party may assign its rights or delegate its duties under this Agreement without the prior written consent of the other party, which consent will not be unreasonably withheld or delayed. Notwithstanding the foregoing; a party may assign this Agreement to a successor to substantially all of its capital stock or assets (whether by sale, merger or otherwise), without the consent of the other party if such assignment does not materially alter the non-assigning party's burdens or obligations.

9.7 Severability. If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions shall remain in full force and effect.

9.8 Notices. All notices and other communications under this Agreement will be delivered in writing. Notices will be deemed to have been properly given (a) three (3) days after deposit in the mail, postage prepaid if mailed, (b) one (1) day after acceptance for overnight delivery by commercial courier, or (c) upon confirmation of delivery by the recipient if delivered in any other manner (e.g., by facsimile or email). Notices will be sent to Miller Heiman Group, Inc. at: 10901 W. Toller Dr., Suite 202, Attn Legal Department, Littleton, CO 80127. Notices will be sent to Client at the Client address set forth in the CCF or Order Document.

9.9 Waiver. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

9.10 Compliance with Laws. In performing this Agreement, Client and MHG agree to comply with all applicable laws and regulations including, but not limited, to all export control or other trade regulation. With regard to export control, Client hereby acknowledges that the Hosted Service may be subject to U.S. export control laws and may not be provided directly or indirectly to any country to which export is prohibited by U.S. export control laws (currently Iran, Syria, North Korea or Cuba), or individuals or entities based or resident in these countries. Client acknowledges that if MHG has reason to believe that U.S. export control laws may be or have been violated, MHG may, in its sole discretion, suspend or terminate this Agreement immediately upon written notice.

9.11 Independent Contractor Relationship. Nothing in this Agreement creates any special relationship between the parties, such as a partnership, joint venture, agency, franchise, or employee/employer relationship.

## Exhibit A

### **TO THE SCOUT BY MILLER HEIMAN GROUP™** **SOFTWARE AS A SERVICE TERMS AND CONDITIONS**

#### **Data Security Provisions**

1. **Purpose.** The purpose of this exhibit is to set forth the application data security practices related to Scout by Miller Heiman Group™.

2. **DEFINITIONS:**

A. **Nonpublic Information** means, in connection with the SaaS Terms, information maintained, owned or controlled by Client that is not publicly known or whose access is restricted internally by the company and includes:

- Any business related information of Client that the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to Client's business, operations, or security and includes, among other things: (i) trade secrets, (ii) intellectual property, (iii) Client business operational and financial information, such as customer lists, business forecasts, marketing plans, pricing information, product or business proposals, investment information, litigation claims, regulatory findings, materials subject to attorney-client privilege, projects and similar documents, (iv) technical or security information, (v) internal only communications between Client employees or agents; (vi) business communications involving a Client employee and a Client client, supplier, contractor, service provider, business partner, government representative or other third-party; and (vii) information about Client's relationships with its employees, agents, customers, suppliers, contractors, service providers, business partners or other third parties.
- Personal information related to any individual (e.g., customer, consumer, employee, agent) maintained by Client which because of name, number, personal mark, or other identifier can be used to identify such individual.

Anonymized and/or de-identified data does not constitute Nonpublic Information.

B. **Breach of Security** means actual or reasonably suspected: (i) unauthorized access to or acquisition, use, disclosure, modification or destruction or theft of any Nonpublic Information regardless of medium.

C. **Cybersecurity Event** means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or electronic data or information stored on such Information System.

3. **Information Security Safeguards.** MHG will maintain appropriate administrative, technical and physical safeguards (a) to maintain confidentiality of Nonpublic Information; (b) to protect against anticipated threats or hazards to the security or integrity of the Nonpublic Information; (c) to protect against unauthorized access to or use of Nonpublic Information; and (d) to detect, respond, and recover from identified risks or incidents including any actual or suspected Breach of Security or Cybersecurity Event.

3.1 **Standards & Practices.** Information Security Safeguards will incorporate all commercially reasonable and appropriate methods and safeguards to ensure the security, confidentiality, integrity, availability and privacy of the Nonpublic Information in accordance with applicable legal or regulatory requirements and industry practices. In addition, MHG will adhere to information security best practices as identified in the National Institute for Standards and Technology Cyber Security Framework (NIST CSF), International Organization for Standardization ISO/IEC 27002, or other equivalent authoritative sources.

3.2 **Appropriate Safeguards.** MHG Information Security Safeguards will include (i) safeguards

against the unauthorized destruction, loss, or alteration of Nonpublic Information; (ii) safeguards against unauthorized access to Nonpublic Information; and (iii) network and internet security procedures, protocols, security gateways and firewalls with respect to Nonpublic Information in accordance with applicable legal and regulatory requirements and applicable industry practices.

3.3 **Physical Security Safeguards.** MHG safeguards will include physical safety and security safeguards at any facilities where any Services are performed on Nonpublic Information. Such Information Security Safeguards will be at least as rigorous as those procedures in place to protect MHG's own Nonpublic Information.

3.4 **Use of Client Nonpublic Information in Non-Production Environments.** Nonpublic Information from production environments will not be used for non-production purposes (i.e., testing and development) unless the data has been de-identified. If Nonpublic Information cannot be de-identified, then MHG will obtain Client's approval prior to doing so. In addition, if Nonpublic information that cannot be de-identified is to be used for non-production purposes, the following controls will be in place:

- Log and monitor any access to the data;
- Use only the minimum amount of data required for testing and development activities
- Infrastructure components will be in conformance with MHG's security baselines

3.5 **Secure Code Development.** Developers will be trained in and follow secure coding best practices (e.g. OWASP, Microsoft Secure Development Lifecycle). MHG will perform application security analysis and testing according to the requirements of an appropriate standard (e.g. OWASP Application Security Verification Standard) prior to software/code delivery. MHG will not include in the software any code that weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, or other forms of malicious code.

#### **4. Due Diligence Assessments**

4.1 **Assessment.** Upon request, MHG will provide reasonable documentation to confirm its compliance with the security requirements included herein. Such documentation may include an independent assessment such as a Report on Controls at a Service Organization Relevant to Security, Availability, Processing, Integrity, Confidentiality or Privacy ("SOC2"), an applicable Report on Controls at a Service Organization ("SOC1" or "SSAE 18") or other such other assessment or certification by an independent third party organization. Delivery of such documentation may require a mutually agreeable non-disclosure agreement with a third party service provider (e.g. AWS for cloud services).

4.2 **Penetration Testing.** MHG, or its third party service provider, shall conduct an annual perimeter network vulnerability assessment or penetration test.

**5. Audit Logs and Reporting.** For systems, applications, or processes associated with the access, processing, storage, communication and/or transmission of Nonpublic Information, MHG will generate audit logs for all actual or attempted incidents of unauthorized use, access, disclosure, theft, manipulation or reproduction of the Client Information or any Breach of Security or Cybersecurity Event involving Client's Nonpublic Information. Audit logs will be maintained in accordance with MHG's record retention obligations or the minimum legal requirements for log retention based on the classification of information in scope. In the event that MHG's review of the audit logs reveals reasonable evidence of any unauthorized use, access, disclosure, theft, manipulation, reproduction and/or Breach of Security or Cybersecurity Event directly impacting Client's Nonpublic Information, MHG will notify Client and reasonably cooperate with Client and provide necessary information to enable Client to meet its obligations to investigate the incident and information individuals and/or regulatory authorities as may be required by applicable legal and/or regulatory requirements.

#### **6. Information Security Infrastructure.**

6.1 **Access Controls.** MHG will maintain appropriate access controls to protect the Nonpublic Information throughout the term of the Agreement and at all times while MHG has access to or possession



of the Client's Nonpublic Information. Client will be solely responsible for implementing and maintaining access controls on its own systems to which MHG may be granted access in accordance with the provision of services.

6.2 Authorized Persons. MHG will limit access to the Client's Nonpublic Information to those individuals who have a business need to access the Client's Nonpublic Information in connection with the services provided to Client ("Authorized Persons").

6.3 Administrative Password Requirements. MHG's passwords that are associated with access to the Client's Nonpublic Information are at least the following:

- Minimum password length: 13
- Require at least one uppercase letter, at least one lowercase letter, at least one number, at least one non-alphanumeric character
- Account lockout will occur after three failed access attempts.
- Passwords must be changed at least every ninety (90) days and the Five (5) most recent passwords must not be reused.

### **Scout internal authentication**

6.4 Multi-Factor Authentication. MHG implements and maintains in connection with Scout, Multi-Factor Authentication for administrative accounts containing Client's Nonpublic Information that is accessible from external or public networks.

6.5 Segregation of Data. MHG will use appropriate logical security controls to segment Client's Nonpublic Information from other clients' or other entities information or data.

6.6 Encryption. MHG will encrypt all Nonpublic Information in transit over external networks and at rest. Encryption must be provided through commercial grade, industry-standard strong cryptographic algorithms, protocols, and commercially reasonable key strengths. If Client requests its Nonpublic Information to be transmitted, MHG agrees to cooperate with Client to do so by reliable and secure transmission methods, provided that any additional cost (if applicable) would be at Client's expense. Physical transportation of encrypted tapes must use secure physical transport methods. Currently Scout uses 256-bit AES-GCM Data Encryption. The keys are secured by FIPS 140-2 [1] certified hardware security modules.

6.7 Network and Host Security. MHG will maintain commercially reasonable and efficient network intrusion detection, firewalls and anti-virus protection (the "Network and Host Security Methods"). MHG will patch any operating systems and applications that are associated with Client's Nonpublic Information within a commercially reasonable time period after MHG has knowledge of any security vulnerabilities. MHG will exercise generally accepted industry standards to ensure that any software, systems, or networks that may interact with Client's systems, networks or any Client Nonpublic Information are not and do not become infected by any malware or viruses, worms, time bombs, back doors, Trojan Horses, or Easter eggs. MHG will implement Distributed Denial of Service (DDoS) mitigation capabilities and maintain these in conjunction with Network and Host Security capabilities.

6.8 Network Connectivity. MHG shall maintain and provide when requested to Client, a network edge diagram that outlines the equipment used in relation to fulfilling of its obligations under this Agreement, including connectivity to Client and third parties who may access portion of MHG's network that contain Client Nonpublic Information.

**7. Compliance with Client Security Procedures.** When on premise at Client or when utilizing Client technology or technology resources, MHG will comply with all written security procedures (including, without limitation, procedures relating to Client's facilities and materials, the Client Nonpublic Information, and if applicable, any software) provided to MHG.

## **8. Breach of Security and Cybersecurity Event Notification**

8.1 Notice. MHG will notify Client promptly of any Breach of Security associated with Client Nonpublic Information in accordance with the terms of the Agreement, and of any Cybersecurity Event that directly impacts the Services being performed for Client or that directly impacts Client Nonpublic Information as described herein. MHG will cooperate with Client's reasonable requests for information regarding the Breach of Security and/or Cybersecurity Event, and MHG will provide regular updates on each Breach of Security or Cybersecurity Event and the investigative action and corrective action taken to permit Client to determine and fulfill its obligations under any applicable legal, regulatory or contractual requirements.

8.2 Remediation. In the event MHG knows or has reason to know of a Breach of Security of the Client Nonpublic Information, or a Cybersecurity Event directly impacting the Services to Client or the Client Nonpublic Information, MHG will, at its own expense, (i) investigate the actual or suspected Breach of Security and/or Cybersecurity Event (ii) provide Client with a remediation plan, acceptable to Client, to address the Breach of Security and/or Cybersecurity Event and to mitigate the incident and reasonably prevent any further similar incidents, (iii) remediate the effects of the Breach of Security and/or Cybersecurity Event in accordance with such remediation plan, and (iv) cooperate with Client and any law enforcement or regulatory official investigating such Breach of Security or Cybersecurity Event.

**9. Information Technology Disaster Recovery.** MHG will be responsible for data backups and disaster recovery, which will include, at a minimum, the following:

- i. Data backups, regardless of medium, should be stored securely at least fifty (50) miles from the primary data center ("Data Center") and accessible at all hours on all days throughout the year;
- ii. Disaster recovery capabilities to be carried out at least three hundred (300) miles from MHG's primary Data Center ("**Out-of-Region-Recovery**");
- iii. An Out-of-Region-Recovery time objective of less than two (2) hours; and
- iv. An Out-of-Region-Recovery that supports a recovery point objective of less than fifteen (15) minutes.

**10. Legal Hold/ Regulatory Demand Requirements.** MHG systems and those of any MHG storage vendor must be able to identify and flag any Client Nonpublic Information subject to Legal Hold/Regulatory Demand. In the event of Legal Hold/Regulatory Demand provided to MHG in writing by Client, and unless otherwise directed by an authorized representative of Client, Client Nonpublic Information must be tagged and preserved unaltered in place for the duration of the Legal Hold/Regulatory Demand period. Once the hold is released, the Client Nonpublic Information must be untagged. MHG will assist Client with the collection of Client Nonpublic Information during Client e-discovery and legal hold processes by providing, upon request by Client, a copy of the Client Nonpublic Information as a Postgresql database extract.

**11. Destruction and Disposal Requirements:** MHG is subject to the following procedures regarding the destruction and disposal of Client Nonpublic Information.

- Client Nonpublic Information must not be destroyed if subject to a Legal Hold/Regulatory Demand.
- Client Nonpublic Information must not be destroyed without the prior written approval of Client, except following termination of the Agreement.
- Media must be disposed of in a manner that ensures the Client Nonpublic Information cannot be reconstructed into a usable format or otherwise subject to unauthorized access, acquisition, use or disclosure in connection with its disposal.

**12. Termination.** Following termination of the relationship with Client, upon Client's request, all Client Nonpublic Information must be returned to Client in an agreed upon timeframe and, in the case of electronically stored Client Nonpublic Information, as a Postgresql database extract, or another format if mutually agreed. Or, at Client's request, Client Nonpublic Information shall be destroyed in accordance with the requirements herein.

**Exhibit B**  
**TO THE SCOUT BY MILLER HEIMAN GROUP™**  
**SOFTWARE AS A SERVICE TERMS AND CONDITIONS**

**Service Level Agreement**

Version 2.0 – March 2019

This Service Level Agreement (“**SLA**”) between Miller Heiman Group, Inc., on behalf of itself and its affiliates (“**MHG**,” “**us**” or “**we**”) and users of the Hosted Service (“**you**”) governs the use of the Hosted Service under the provisions of the Software as a Service Terms and Conditions (the “**SaaS Terms**”). Capitalized terms used but not defined herein shall have the meanings assigned to them in the SaaS Terms. Unless otherwise provided herein, this SLA is subject to the provisions of the SaaS Terms.

1. Scout Service Commitment: 99.5% Uptime

MHG will use commercially reasonable efforts to make the Hosted Service available with a Monthly Uptime Percentage of at least 99.5% during any month (the “**Service Commitment**”). Subject to the SLA Exclusions, if we do not meet the Service Commitment, you will be eligible to receive a Service Credit.

“**Monthly Uptime Percentage**” of 99.5% means that we guarantee you will experience no more than 3h 40m month of Unavailability.

2. Definitions

- “**Maintenance**” means scheduled Unavailability of the Hosted Service, as announced by us prior to the Hosted Service becoming Unavailable.
- “**Monthly Uptime Percentage**” is calculated by subtracting from 100% the percentage of minutes during the month in which the Hosted Service were Unavailable. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any SLA Exclusion.
- “**Service Credit**” means a credit denominated in US dollars, calculated as set forth below, that we may credit back to an eligible account.
- “**Unavailable**” and “**Unavailability**” mean, for app services and databases, when your service or database is not running or not reachable due to MHG’s fault.

3. Service Commitments and Service Credits

Service Credits are calculated as a percentage of the total fees paid and attributable to the month in which the Unavailability occurred, applied proportionally to the portion of the Hosted Service that was Unavailable, in accordance with the schedule below:

- For Monthly Uptime Percentage less than 99.5% but equal to or greater than 99.0%, you will be eligible for a Service Credit of 10% of the charges attributable to the affected resources
- For Monthly Uptime Percentage less than 99.0%, you will be eligible for a Service Credit of 30% of the charges attributable to the affected resources

For example, if the Hosted Service is Unavailable for 25 minutes, you would be eligible for a Service Credit for 10% of the Hosted Service usage for the month.

We will apply any Service Credits only against future payments for the Hosted Service otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing

cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from MHG. A Service Credit will be applicable and issued only if the credit amount for the applicable month is greater than ten dollars (\$10 USD). Service Credits may not be transferred or applied to any other account.

#### 4. Sole Remedy

Except as otherwise provided in the SaaS Terms, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Hosted Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

#### 5. Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by emailing [support@MillerHeimanGroup.com](mailto:support@MillerHeimanGroup.com). To be eligible, the credit request must be received within 30 days of the incident and must include:

- the words "SLA Credit Request" in the subject line;
- the dates and times of each Unavailability incident that you are claiming;
- the account handle(s); and
- logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

#### 6. SLA Exclusions

The Service Commitment does not apply to any Unavailability that results from or is caused by:

1. A suspension or remedial action, as described in the SaaS Terms;
2. Factors outside of our reasonable control, including any Force Majeure Event, Internet access, or problems beyond the demarcation point of the MHG network;
3. Any actions or inactions of you or any third party;
4. The equipment, software or other technology of you or any third party (other than third party equipment within our direct control);
5. Failures of Scout not attributable to Unavailability; or
6. Any schedule downtime or maintenance.

If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.