

Master Agreement

This Master Agreement (the “**Agreement**”) dated December 1, 2025 is entered into by and between The City of Greenfield, an Indiana municipality with its principal office at 333 South Franklin Street, Greenfield, Indiana 46140 (“**Customer**”), and Brillion Inc. (f/k/a Apogee Interactive, Inc.), a Georgia corporation with its principal office at 100 Crescent Centre Parkway, Suite 450, Tucker, Georgia 30084 (“**Brillion**”) (individually a “**Party**” and collectively the “**Parties**”).

Brillion Inc. (f/k/a Apogee Interactive, Inc. and referred to as Brillion hereafter) is the legal assignee of, and successor-in-interest to, certain assets of Automated Energy, Inc. (“**AEI**”). Customer had a business relationship with AEI that has been assigned to Brillion. The Parties agree that this Agreement supersedes and replaces in its entirety all prior contracts entered into between the AEI and Customer before the effective date of this Agreement, including that certain Service Agreement dated June 2, 2015.

This Agreement, when combined with any related Orders or SOWs, sets out certain terms and conditions regarding (1) Brillion's delivery to Customer, and Customer's access to and use of, Brillion's proprietary SaaS Solution and Software and (2) Brillion's delivery to Customer of the Professional Services. Each Order or SOW represents a separate contract that will be governed by the terms and conditions of this Agreement. If there is a conflict between this Agreement and an Order or SOW, the Order or SOW takes precedence solely with respect to the SaaS Solution and Professional Services detailed in the Order or SOW.

In addition to the capitalized terms defined in this Agreement, capitalized terms shall have the meanings set forth in Exhibit A entitled “Definitions.”

1. SaaS Solution – Use Rights & Restrictions.

1.1 Use Rights. Specific terms of the SaaS Solution use rights granted by Brillion to Customer pursuant to this Agreement will be documented in one or more Orders; provided however, subject to the terms and conditions of this Agreement, Brillion will grant to Customer a nonexclusive, non-sublicensable, non-assignable (except as provided in Section 13.4), and limited license to access and use the SaaS Solution, including the applicable Software, for the Subscription Term set forth in the applicable Order solely by Customer's Personnel (and, as applicable, by End Users) for Customer's internal business operations. As applicable, Customer may make a reasonable number of copies of the Documentation solely for use by its Personnel.

1.2 Use Restrictions. Customer shall not, and shall take commercially reasonable efforts so that any other person or entity will not: (a) exceed the use rights regarding the SaaS Solution or Software granted and detailed in this Agreement and the applicable Order; (b) use the SaaS Solution or Software in a service bureau or time sharing environment; (c) except as permitted by Section 4.2 of this Agreement, sell, sublicense, lease, assign, delegate, transfer, distribute, or encumber the SaaS Solution or the Software or any Intellectual Property Rights embodied therein; (d) bypass or breach any security device or protection used by the SaaS Solution; or (e) input, upload, transmit, or otherwise provide to or through the SaaS Solution, any data, information or materials that are unlawful or injurious, or contain, transmit, or activate any harmful code.

2. Professional Services.

2.1 Professional Services Delivered. The specific Professional Services (defined in Exhibit A) that Brillion will deliver to Customer pursuant to this Agreement will be detailed and documented in one or more Orders or SOWs.

2.2 Customer's Responsibilities. Any Professional Services delivered by Brillion hereunder are subject to Customer's performance of its general obligations described in this Agreement and specific obligations described in the applicable Order or SOW. As applicable, Customer shall provide all necessary information, access, computing resources, support services, and materials as reasonably required by Brillion to perform its duties in a timely manner. Customer acknowledges and agrees that such cooperation and provision of information are essential to Brillion's ability to perform the Professional Services. Brillion is not responsible or liable for any delay or failure of performance caused in whole or in part by Customer's delay in performing, or failure to perform, any of its obligations under this Agreement.

2.3 Subcontractors & Offshore Resources. Brillion engages non-employee Personnel located within the United States as subcontractors to assist Brillion with the delivery of certain services pursuant to this Agreement. Additionally, Brillion has (a) employees located within Canada who may assist with the delivery of certain services pursuant to this Agreement and (b) existing, independent contractor arrangements with technology service providers located outside of the United States that hire and manage a dedicated team of professionals to assist Brillion with the delivery of certain services pursuant to this Agreement (the “**Offshore Resources**”).

Unless stated otherwise in an Order, Customer acknowledges and agrees that Brillion may use a combination of its employees with such subcontractors and/or Offshore Resources to assist Brillion with the delivery of certain Professional Services or Support Services pursuant to this Agreement. Any subcontractors or Offshore Resources used by Brillion hereunder will be legally bound to meet or exceed the confidentiality, nondisclosure, and security obligations imposed on Brillion in this Agreement. Furthermore, Brillion will remain responsible to Customer for the performance and conduct of such

subcontractors or Offshore Resources, including the obligations regarding Confidential Information, as if Brillion had performed such tasks with its own employees.

3. Support Services & Service Levels. During the applicable Subscription Term and as part of the delivery to Customer of the SaaS Solution, Brillion also will deliver to Customer the “**Support Services**” as detailed in the applicable Order and that generally will consist of: (a) web-based information support, telephone support, and/or email technical support for the SaaS Solution and Software and (b) any updates, fixes, and modifications to the SaaS Solution and Software that Brillion commercially releases to its other customers. Service level information, if applicable for a SaaS Solution, also will be detailed in the applicable SaaS Schedule attached to the applicable Order.

4. Orders, SOWs & Ancillary Documents.

4.1 Orders & SOWs. Each Order or SOW issued pursuant to and governed by this Agreement shall be in writing and executed by the Parties (or their Affiliates). A SOW may be attached to an Order or may be executed by the Parties (or their Affiliates) as a separate, stand-alone, mutually executed document.

4.2 For Benefit of an Affiliate. Without assigning this Agreement under Section 13.4, a Brillion Affiliate may (a) deliver to Customer the SaaS Solution or Professional Services and/or (b) enter into an Order or SOW that will, in turn, be governed by this Agreement. Similarly and without assigning this Agreement under Section 13.4, a Customer Affiliate may enter into an Order or SOW that will, in turn, be governed by this Agreement. In the alternative, any Customer Affiliate specifically identified in an Order or SOW may (i) access and use the SaaS Solution and Software and/or (ii) receive the Professional Services detailed in an Order or SOW executed by Customer as though they are Customer itself.

In each such instance, the Customer Affiliate shall be obligated to abide by all applicable terms and conditions of this Agreement and the applicable Order or SOW, including any SaaS Solution access and use restrictions or limitations detailed in the applicable Order.

As applicable, any references to “Customer” in this Agreement or the applicable Order or SOW will be deemed to apply to each Customer Affiliate that is a party to the Order or SOW or that is identified in the Order or SOW.

4.3 Change Orders. The Parties may modify an Order or SOW by entering into a written “change order” document in a mutually agreeable format (a “**Change Order**”). Each Change Order complying with this Section 4.3 will be deemed to be a legally binding modification of the underlying Order or SOW and will be governed by the terms and conditions of this Agreement.

4.4 Customer Purchase Orders. If Customer elects to deliver to Brillion a purchase order (or invoice or other business form or written authorization) regarding any Fees that are due and payable to Brillion pursuant to this Agreement, any terms and conditions attached to or included in the same that conflict with the terms and conditions of this Agreement or any Order or SOW will be void and deemed not accepted by Brillion.

5. Fees & Payment.

5.1 Pricing. The agreed-upon Fees related to the SaaS Solution and/or Professional Services delivered pursuant to this Agreement will be detailed in the applicable Order or SOW. Unless otherwise specified in this Agreement or agreed in an Order or SOW, all Fees are (a) non-cancelable and non-refundable unless Customer terminates in accordance with Section 11.5(b), in which case Brillion will issue to Customer a pro-rated refund of any pre-paid Fees and (b) payable in U.S. dollars.

5.2 Expenses. As applicable and as detailed in an Order or SOW, Customer shall reimburse Brillion for reasonable, pre-approved Expenses incurred in the performance of the Professional Services.

5.3 Taxes, Etc. Customer has provided Brillion copies of all applicable documents confirming governmental tax designations (e.g., exemption, self-assessment rights).

5.4 Fees, Payment Process, Invoice Dispute & Suspension Remedy.

(a) **Fees & Payment.** Brillion will invoice Customer for all applicable Fees in the manner set forth in the applicable Order or SOW. Unless stated otherwise in the applicable Order or SOW, within thirty (30) days from the date of Brillion's invoice, Customer shall pay all Fees owed Brillion thereunder, except for any amount disputed in good faith in accordance with subsection 5.4(b). Customer further agrees to remit payment of all Fees owed Brillion via ACH. The ACH processing details and routing information will be included in the applicable Order or SOW (or otherwise mutually agreed upon in writing by the Parties).

(b) **Invoice Dispute.** Customer shall notify Brillion in writing of any disputed fees within fifteen (15) days of Customer's receipt of an invoice, setting forth in reasonable detail the grounds for disputing the invoice. Brillion will investigate and respond to any dispute raised by Customer within thirty (30) days of such notice. If the Parties determine that Customer

owes any portion of the disputed amount, Customer shall have fifteen (15) days from the date of the resolution of the dispute to pay such amount, which will not bear interest or late charges until such expiration of the fifteen (15) day period. Otherwise, Brillion may charge a late fee equal to 0.67 percent of the past-due amount per month (not to exceed eight percent (8%) per annum). Unless otherwise agreed in writing by Brillion, all amounts payable to Brillion under this Agreement shall be paid by Customer in full without any setoff, recoupment, counterclaim, deduction, debit, or withholding for any reason (other than any deduction or withholding of tax as may be required by applicable law).

(c) Suspension Right. Without waiving or limiting any other rights or remedies Brillion has for any other breach (such as Section 11.5), Brillion shall have no obligation to deliver, or continue to deliver, the SaaS Solution or any Professional Services and shall otherwise have the right to suspend and withhold performance under this Agreement if Customer is in arrears on any payments rightfully due to Brillion and does not pay within ten (10) days after written notice that Brillion is invoking the remedy set forth in this Section 5.4(c).

6. Limited Warranty and Disclaimers.

6.1 Limited Performance Warranty – SaaS Solution. Subject to any additional warranty terms set forth in an Order or SOW, Brillion warrants to Customer that: **(a)** the SaaS Solution (and applicable Software) will function materially in accordance with the Documentation and the SaaS Schedule; **(b)** any upgrades, changes, enhancements, modifications, or updates to the SaaS Solution (or applicable Software) will not adversely reduce the functionality of the same; **(c)** the Support Services will be delivered materially in accordance with the terms detailed in the Order; and **(d)** the SaaS Solution (and applicable Software) will not contain any viruses, trojan horses, logic bombs, time bombs, disabling code, or malware.

6.2 Limited Performance Warranty – Professional Services. Subject to any additional warranty terms set forth in an Order or SOW, Brillion warrants to Customer that Brillion will perform the Professional Services hereunder in a timely and professional manner by qualified Personnel.

6.3 Disclaimer. Except for the limited warranties detailed in this Section 6, all SaaS Solutions, Software, Professional Services, and Support Services are provided “AS IS” and Brillion makes no, and disclaims all other, warranties, representations, or conditions, written or oral, or express, implied, or statutory, including any implied warranties of merchantability, non-infringement, interoperability, data accuracy, or fitness for a particular purpose with respect to any SaaS Solution, Software, Professional Services, Support Services, or any components thereof, and any other products or services provided by Brillion. Without limiting the foregoing, Brillion does not warrant that all errors can be corrected, or that operation of the Software shall be uninterrupted or error-free. Additionally, and without limiting the foregoing, statements made by Brillion’s sales representatives or in promotional materials do not constitute warranties. Finally, Brillion’s third party licensors make no, and disclaim any and all, warranties or representations to Customer.

7. Indemnification.

7.1 Brillion shall indemnify, hold harmless, and defend Customer from and against any and all losses, damages, liabilities, and costs (including reasonable attorneys’ fees) incurred by Customer resulting from any third party claim, suit, action, or proceeding resulting from or based on a claim that the SaaS Solution (or Software) infringes the Intellectual Property Rights of such third party. Notwithstanding the foregoing, Brillion will have no indemnification obligation to the extent such claim arises out of or relates to **(a)** use of the SaaS Solution (or Software) by Customer other than in accordance with its Documentation; **(b)** design modifications, hardware, or software specifications, designs, or written instructions implemented by Customer without Brillion’s written approval; or **(c)** Customer’s Intellectual Property Rights or Customer Data.

7.2 If a claim for which Customer is entitled to be indemnified under Section 7.1 above has occurred, or in Brillion’s opinion is likely to occur, Brillion shall, at Brillion’s expense, do one of the following: **(a)** procure for Customer the right to continue using the relevant SaaS Solution (or Software); **(b)** replace with non-infringing alternates or modify the relevant SaaS Solution (or Software) so that it becomes non-infringing, but its functionality after modification is substantially equivalent; or **(c)** cease delivering the relevant SaaS Solution (or Software) and refund any prepaid fees applicable to the period after cessation. With respect to any intellectual property infringement claim, the collective obligations of Brillion pursuant to Section 7.1 and this Section 7.2 state the sole and exclusive liability of Brillion and Customer’s sole and exclusive remedy.

7.3 Customer shall indemnify, hold harmless, and defend Brillion from and against any and all losses, damages, liabilities, and costs (including reasonable attorneys’ fees) incurred by Brillion resulting from any third party claim, suit, action, or proceeding resulting from or based on: **(a)** the unauthorized disclosure or delivery by Customer to Brillion of Customer Data (in breach of Section 9.3 below); **(b)** Customer’s use of the SaaS Solution or Software in a manner not authorized or contemplated by this Agreement; or **(c)** Customer’s violation of any applicable data processing or privacy laws.

7.4 Promptly after a Party obtains knowledge of a claim for which it is entitled to be indemnified under Section 7.1 or 7.3 above, such Party will notify the other Party of such claim in writing, provided, however, that any failure to give such notice will not waive any rights of the indemnified Party except to the extent that its rights are actually prejudiced or liability increased thereby. The indemnifying Party will have exclusive control of the defense and settlement of such claim and the indemnified Party must reasonably cooperate with the indemnifying Party in the defense and settlement of the claim.

8. Limitation of Liability.

8.1 Direct Damages. Except for: (a) each Party's indemnification obligations under Section 7; (b) a Party's misappropriation or unauthorized disclosure of Confidential Information or breach of its data security obligations; or (c) intentional misconduct by a Party or its Personnel, each Party's maximum liability arising out of, or in any way connected to, this Agreement shall be in the aggregate and limited (on a claim-by-claim basis) to actual (direct) damages not to exceed two times (2X) the actual Fees paid to Brillion under the relevant Order or SOW during the twelve (12) months preceding the act or omission under said Order or SOW that gave rise to the claim.

8.2 No Consequential Damages. Except for claims (a) which may not be limited as a matter of law; (b) for personal injury or death; or (c) which arise from the intentional misconduct by a Party or its Personnel, in no event shall either Party, any parent, subsidiary, or Affiliate, or any of their officers, directors, employees, shareholders, or representatives, be liable to the other Party for any consequential, indirect, exemplary, incidental, punitive, or special damages or costs (including but not limited to procurement costs of substitute products or services, lost profits, loss of business opportunities, lost savings, or loss of goodwill) arising out of, or in any way connected to, this Agreement or resulting from or in connection with the use, misuse, or inability to use the SaaS Solution, Software, Professional Services, or any other products or services, regardless of the cause of action and even if a Party has been advised of the possibility thereof or such damages or costs were otherwise foreseeable. Notwithstanding the foregoing, if a Party's indemnification obligations are considered consequential damages, this Section 8.2 shall not bar any indemnification claim under Section 7.

9. Intellectual Property Rights and Use of Customer Data.

9.1 Brillion – Intellectual Property Rights. As of the Effective Date, Brillion represents and warrants that it owns or has the right to license the SaaS Solution and the Software, including, as applicable, any third party software integrated therein. Brillion asserts that it has created and developed proprietary configuration processes, methodologies, and know how (the "**Brillion Processes**"). Brillion, or its licensor(s), shall retain all right, title, and interest in and to the Intellectual Property Rights embodied in and to: (a) the SaaS Solution and the Software and (b) the Brillion Processes, whether tangible or intangible and whether developed independently by Brillion outside the scope of this Agreement or as a result of discussions with Customer within the scope of this Agreement. Except for the limited license granted hereunder, Customer shall not assert any right, title, or interest in or to the SaaS Solution, the Software, or the Brillion Processes. Subject to the foregoing, Customer shall own all right, title, and interest in the tangible reports or analyses created or prepared using the SaaS Solution, the Software, or the Brillion Processes within the scope of this Agreement and, to the extent that such reports or analyses contain Intellectual Property Rights, Brillion further grants Customer the limited, royalty-free, global rights and licenses necessary to use such reports and analyses for its own business purposes. As applicable and except where such restrictions are prohibited under mandatory applicable law, Customer shall not, and shall take commercially reasonable efforts so that any other entity will not: (i) disassemble, decompile, decrypt, or reverse engineer, or in any way attempt to discover or reproduce source code for, any part of the SaaS Solution or the Software or adapt, modify, or prepare derivative works based on the SaaS Solution or the Software; or use the Software to create any computer program or other material that performs, replicates, or utilizes the same or substantially similar functions as the SaaS Solution or the Software or (ii) alter, remove, or suppress any copyright, trademark, confidentiality, or other proprietary notices or legends placed on, embedded in, or otherwise appearing in or on the SaaS Solution or the Software or tangible reports prepared using the SaaS Solution or the Software.

9.2 Feedback. If Customer or any of its Personnel sends or transmits any communications or materials to Brillion by mail, email, telephone, or otherwise, suggesting or recommending changes to the Brillion SaaS Solution, Software, Professional Services, or other services delivered pursuant to this Agreement, including without limitation, new features or functionality relating thereto, or any comments, questions, suggestions, or the like ("**Feedback**"), then, subject to any confidentiality provisions of this Agreement, Brillion is free to use such Feedback for purposes of enhancing the Brillion SaaS Solution, Software, or Professional Services delivered pursuant to this Agreement, although Brillion is not required to use any Feedback and, as applicable, Customer hereby grants to Brillion a nonexclusive, perpetual, irrevocable, worldwide, and royalty-free license to access and use any Intellectual Property Rights contained in the Feedback.

9.3 Customer Data. During the applicable Subscription Term, Customer represents and warrants that it has the right to authorize Brillion to store, process, and use the Customer Data and Customer further grants to Brillion a limited, revocable, and non-exclusive right and license during the applicable Subscription Term to reproduce, distribute, transmit, display, reformat, and otherwise use any Customer Data in order to perform Brillion's obligations under this Agreement. Customer acknowledges and agrees that it will not include in such Customer Data any data or information that is subject to either (i) the HIPAA (the Health Insurance Portability and Accountability Act of 1996) or (ii) PCI-DSS. Unless otherwise agreed by the Parties, any Customer Data delivered to Brillion will remain stored or maintained on servers and computer systems located within the United States of America.

Brillion acknowledges and agrees that, as between Brillion and Customer, Customer shall own all right, title and interest in the Customer Data and any reports or analyses resulting from or arising out of Customer's use of the SaaS Solution. Furthermore, to the extent that there are any Intellectual Property Rights embodied in such reports or analyses, Brillion shall retain such Intellectual Property Rights, but hereby grants Customer a perpetual license to use such reports or analyses.

9.4 Brillion's use of De-Identified & Aggregated Data. For purposes of this Section 9.4, "De-identified Data" means user statistics, metadata, and quantitative data derived from Customer's use of the SaaS Solution that Brillion will anonymize so as not to contain any information that identifies or can be reasonably used to identify an individual person or End User of Customer. Customer grants Brillion the right to use such De-identified Data solely for the purposes of its own internal analysis, benchmarking, analytics, A/B testing, metrics, research, reporting, machine learning, marketing, and other lawful business purposes.

10. Confidentiality & Data Security.

10.1 Protection of Confidential Information. Confidential Information is, and remains, the disclosing Party's, or the lawful owner's, sole and exclusive property, and this Agreement grants no licenses or other rights of any kind to the receiving Party unless expressly stated herein. The receiving Party may use and disclose Confidential Information solely in connection with performance of its obligations or exercise of its rights under the Agreement. The unauthorized disclosure or use of Confidential Information of the other Party or of the other Party's third party licensors, and all information and services related thereto, may cause injury and harm to its owner. Therefore, during the term of this Agreement and so long as such Confidential Information remains confidential, each Party agrees to take all appropriate action to ensure the confidentiality and security of the other Party's Confidential Information, but in any event no less than the same standard of care it uses to protect its own Confidential Information of like kind and value. Without limiting the generality of the foregoing, Customer and Brillion each agree that it: (a) shall maintain the other's Confidential Information in the strictest confidence, including compliance with reasonable remote access security requirements; (b) shall not disclose, display, publish, transmit, or otherwise make available such Confidential Information, except in confidence to its own Personnel; or (c) except as expressly permitted hereunder, shall not copy, duplicate, replicate, transform, or reproduce such Confidential Information. Finally, during the term of this Agreement and upon receipt of a written request, one Party shall promptly return to the other Party or destroy any Confidential Information of the other Party. Upon written request by Customer, Brillion will deliver a written certification that it has destroyed any Customer Confidential Information.

10.2 Obligations Regarding Processing of Customer Data. Brillion acknowledges and agrees that certain Customer Data may include Personal Data that is subject to certain privacy and data protection laws. Any Customer Data that Customer delivers to Brillion will be stored (a) in a secure environment that meets industry standards, including but not limited to the "Data and System Security Schedule" attached hereto as Exhibit B and (b) in an encrypted or otherwise secure form. If there is a breach of security of any system, database, equipment, or storage medium or facility that results in unauthorized access to Customer Data by any third party, Brillion shall notify Customer promptly and make best efforts to re-secure its systems.

10.3 Exclusions. Notwithstanding any other provision of this Section 10, neither Party shall be liable to the other for damages resulting from disclosure of any Confidential Information required by law, regulation, or valid court order; provided, if permitted by law, prior written notice is provided to the other Party sufficiently in advance of such required disclosure to allow the other Party to respond and take reasonable and lawful action to avoid and/or minimize the degree of such disclosure or seek appropriate protective orders.

11. Term & Termination.

11.1 Term of Agreement. This Agreement shall commence on the date of the final signature to this Agreement (the "Effective Date") and continue until terminated as provided in Section 11.2.

11.2 Termination of Agreement. This Agreement may be terminated (a) by mutual written consent or (b) by either Party upon the material breach of this Agreement by the other Party which remains uncured thirty (30) days after written notice of such breach. Additionally, if the terms of all Orders or SOWs entered into between the Parties under this Agreement have expired and been fully performed, then either Party may terminate this Agreement for convenience after giving thirty (30) days written notice to the other Party of its intent to terminate.

11.3 Effect of Termination of Agreement. Upon the termination of this Agreement, Customer shall pay to Brillion all undisputed, outstanding Fees and other amounts owed Brillion within thirty (30) days of such termination. Additionally, upon termination of this Agreement and subject to applicable law, one Party shall promptly return to the other Party or destroy any Confidential Information of the other Party. Consistent with Section 10.1, upon written request by Customer, Brillion will deliver a written certification that it has destroyed any Customer Confidential Information.

11.4 Term of an Order or SOW. As applicable, each Order or SOW will detail (a) the Subscription Term for use of the SaaS Solution and/or (b) the delivery term of any Professional Services to be delivered thereunder.

11.5 Termination of an Order or SOW. An Order or SOW may be terminated: (a) by Brillion (and notwithstanding Section 5.4(c)), if any undisputed payment owed under an Order or SOW remains due and unpaid thirty (30) days after Brillion's written notice to Customer thereof or (b) by either Party if the other Party fails to perform any material obligation set forth in an Order, SOW, or this Agreement, and such non-performing Party does not cure such failure within thirty (30) days after written notice of such failure. Only if expressly authorized in the applicable Order or SOW may a Party

terminate such Order or SOW for convenience. The termination or expiration of one Order or SOW by itself shall not result in the termination or expiration of any other Order or SOW. Furthermore, if the Agreement is terminated, but an Order or SOW remains in effect, such Order or SOW shall continue to be governed by this Agreement unless the Order or SOW also is terminated.

11.6 Effect of Expiration or Termination of an Order or SOW. Subject to Section 11.3, upon the expiration or termination of an Order or SOW, this Agreement shall continue in full force and effect. As applicable, upon the expiration or termination of any Order or SOW: **(a)** Customer shall pay to Brillion all outstanding and undisputed Fees and other amounts owed Brillion within thirty (30) days of such expiration or termination and **(b)** Brillion shall have no further performance obligations thereunder, including, but not limited to delivery of the SaaS Solution detailed therein.

11.7 Survival. Provisions of this Agreement which by their context and content are intended to survive termination or expiration hereof shall so survive.

12. Dispute Resolution & Governing Law.

12.1 Negotiation & Waiver of Jury Trial. If any disputes, differences, or controversies between the Parties arise out of, under, or in relation to this Agreement (or an Order or SOW), except for claims for provisional equitable relief (e.g., the right to pursue injunctive relief, or any other relief to preserve the status quo) (a "**Dispute**"), the Parties shall thoroughly explore all possibilities for the amicable settlement through negotiation among executives. If the Dispute has not been resolved by negotiation within sixty (60) days, then, subject to Section 12.3, one Party may initiate legal action against the other Party. Notwithstanding the foregoing, each Party hereby waives any right it may have to a jury trial in any action, proceeding, or litigation directly or indirectly arising out of, under, or in connection with this Agreement and whether made by claim, counterclaim, or otherwise.

12.2 Equitable Relief. A breach or threatened breach by a Party of any of its obligations of confidentiality or by Customer of any use restrictions applicable to the SaaS Solution may cause the other Party irreparable harm for which monetary damages may not be an adequate remedy and, in the event of such breach or threatened breach, the other Party may be entitled to seek equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

12.3 Governing Law & Venue. This Agreement shall be governed by and construed in accordance with the substantive laws of the State of Georgia without regard to its conflict of laws principles. The U.S. federal courts and state courts sitting in the jurisdiction of DeKalb County, Georgia, United States of America, shall have sole and exclusive jurisdiction over a claim or Dispute brought by Customer or Brillion, which may arise out of or in connection with this Agreement, and both Customer and Brillion consent to those forums. The Parties agree that The United Nations Convention on Contracts for the International Sale of Goods shall not apply hereto in any respect to this Agreement.

12.4 Litigation Costs. Except for litigation costs awarded under Section 7 (indemnification) or recoverable pursuant to an applicable statute, each Party shall be responsible for paying its own costs and expenses, including attorneys' fees, related to or arising out of a Dispute and one Party shall not be responsible for the Dispute resolution costs or expenses of the other Party.

13. General.

13.1 Counterparts & Electronic Signatures. This Agreement and any Order or SOW may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall be deemed for all purposes to constitute one and the same instrument. The Parties have agreed to accept electronic signatures pursuant to the United States Electronic Signatures in Global and National Commerce Act. The Parties hereby agree that hardcopy signatures transmitted via electronic means shall be treated as original signatures for all purposes of this Agreement, an Order or SOW.

13.2 Entire Agreement. This Agreement and any related Orders or SOWs will be the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing any and all prior agreements, communications, and understandings (both written and verbal) regarding such subject matter.

13.3 Amendment. This Agreement and any related Orders or SOWs may be amended, modified, or supplemented only by a writing that refers explicitly to this Agreement or the applicable Order or SOW and that is signed by an authorized representative on behalf of each of the Parties.

13.4 Assignment. Neither this Agreement nor any rights granted hereunder may be sold, leased, assigned, or otherwise transferred, in whole or in part, by either Party and any such attempted assignment shall be void and of no effect without the prior written consent of the other Party. Notwithstanding the foregoing, such consent shall not be required if either Party assigns this Agreement to an Affiliate or in connection with a merger, or sale of all its stock, or all or substantially all of its assets; provided in either case, **(a)** the Affiliate or surviving entity is not a direct competitor of the other Party and **(b)** any

such assignee has the financial and other abilities required to perform the assignor's obligations and agrees to be bound in writing to assignor's obligations under this Agreement.

13.5 Notices. All notices or other communications required hereunder will be made in writing and will be deemed to be effectively given: (a) if hand delivered, when received; (b) if sent via overnight delivery, when delivery by the overnight carrier is made; or (c) if sent by email, on the date of the sending Party's receipt of confirmation email transmission, in each instance at the applicable address set forth below. For the avoidance of doubt, notice given under this Agreement will be validly served if sent by electronic mail; provided however, notice of breach may not be served by email. Each Party may change its notices address by giving notice in the manner set forth herein. As of the Effective Date, each Party's initial contact information for notices or other communications is as follows:

Brillion Inc. (f/k/a Apogee Interactive, Inc.)
100 Crescent Centre Parkway, Suite 450
Tucker, Georgia 30084
Attn: CFO
Email: contracts@brillion.ai

The City of Greenfield
333 South Franklin Street
Greenfield, Indiana 46140
Attn: Jane Webb
Email: jwebb@greenfieldin.org

13.6 Severability; Waiver. If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect to the extent legally permitted. The invalidity or unenforceability of any provision shall not constitute a failure of consideration hereunder. Any failure or delay in exercising, or any single or partial exercise of, any right or remedy by either Party hereto shall not be deemed a waiver of any further, prior, or future right or remedy hereunder, including the right of such Party at any time to seek such remedies as may be available for any breach or breaches of such term or condition.

13.7 Compliance with Laws. Each Party shall comply with all applicable US and foreign laws, rules, and regulations relating to: (a) the control or processing of Personal Data, including the California Consumer Privacy Act of 2018 and California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 et seq. and implementing regulations (collectively, the "CCPA/CPRA"); (b) anti-bribery and anti-corruption, including the US Foreign Corrupt Practices Act; (c) applicable employment laws and laws which relate to anti-slavery, servitude, compulsory labor, or trafficking, including the Modern Slavery Act; and (d) its activities hereunder or in connection with this Agreement, the license or use of any SaaS Solution and Software, and the delivery of any Professional Services.

13.8 Nature of Relationship. Neither this Agreement nor the Parties' business relationship established hereunder will be construed as a partnership, joint venture, or agency relationship, or as granting any franchise.

13.9 Force Majeure. Neither Party shall be liable for any failure to perform any of its obligations under this Agreement (other than the payment of money) due to unforeseen circumstances or causes beyond the Party's reasonable control, including acts of God, riot, embargoes, acts of governmental authorities, fire, earthquake, flood, acts of terror, and epidemics.

13.10 No Third Party Beneficiaries. This Agreement is solely for the benefit of the Parties hereto (and their Affiliates), and nothing in this Agreement will be deemed to create any third party beneficiary rights in any person or entity not a party to this Agreement.

13.11 Publicity. Either Party may publicly refer to the other by name as a provider or customer, as applicable, and may disclose the general nature and existence of the Agreement, but not any of its specific terms or performance information. Neither Party will issue a press release regarding the Agreement or the relationship without the other Party's prior review and written consent.

[signature page follows]

ACCEPTED:

Brillion Inc. (f/k/a Apogee Interactive, Inc.)

Signed by:

Jon Ezrine

AUTHORIZED REPRESENTATIVE

Jon Ezrine, CEO

NAME & TITLE PRINTED

12/15/2025

DATE

ACCEPTED:

The City of Greenfield

Guy Titus

AUTHORIZED REPRESENTATIVE

Guy Titus Mayor

NAME & TITLE PRINTED

12/15/25

DATE

Exhibit A

(Definitions)

Affiliate. Means any entity which now or in the future controls, is controlled by, or is under common control with a Party, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise. For each Order or SOW entered into on behalf of Customer's Affiliate, "Customer" and "Party" as used herein shall mean the Affiliate identified therein.

Confidential Information. Means any proprietary or confidential information or data, intellectual property, or know-how, including, without limitation: (a) research, product plans, business plans, marketing plans, pricing information, customer lists, personnel information, software code, software documentation, inventions, trade secrets, data compilations, processes, designs, drawings, engineering reports, computer system configuration information, marketing, or finances; (b) any SaaS Solution and Software delivered hereunder and/or materials resulting from the Professional Services, and any derivatives thereof; (c) Customer Data and Personal Data; or (d) information that, given the nature of the information and circumstances surrounding the disclosure, a reasonable person would understand to be confidential, including, but not limited to, the terms of this Agreement. Notwithstanding the foregoing, Confidential Information does not include information, technical data, or know-how that, without restriction on disclosure, is: (i) in the public domain or becomes available to the public and not as a result of the act or omission of the receiving Party; (ii) rightfully obtained by the receiving Party from a third party; (iii) is lawfully in the possession of the receiving Party at the time of disclosure; or (iv) is approved for release by written authorization of the disclosing Party.

Customer Data. Means the information, including as applicable Personal Data contained therein, that Customer enters into the SaaS Solution, either directly or indirectly (which includes an End User entering such Personal Data into the SaaS Solution as authorized by Customer to do so) or that is processed or generated in the course of Customer's use of the SaaS Solution. For the avoidance of doubt, Customer Data is considered Customer Confidential Information.

Documentation. Means Brillion's then-current written documentation delivered electronically upon implementation of (and any upgrades to) the SaaS Solution and that describes the specifications and use of the SaaS Solution and applicable Software. As applicable, the license to use such Documentation shall be deemed included in the applicable SaaS Solution use rights granted by Brillion to Customer.

End User. Means a customer of Customer and about whom certain Personal Data might constitute Customer Data as processed pursuant to this Agreement.

Expenses. Means all pre-approved out-of-pocket expenses incurred by Brillion in performing hereunder.

Fees. Means collectively, any and all fees related to Brillion's delivery of the SaaS Solution (and Software) and/or any Professional Services detailed in an Order or SOW.

Intellectual Property Rights. Means any and all tangible and intangible rights, title and interest in and to: (a) works of authorship, including but not limited to copyrights, moral rights, and mask works, and all derivative works thereof; (b) trademarks, service marks, and trade names; (c) trade secrets or proprietary know-how; (d) inventions, patents, designs, or algorithms; (e) all other intellectual or industrial property rights whether arising by operation of law, contract, license, or otherwise; and (f) all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter in force.

Order. Means any written document that is ancillary to the Agreement, but governed by and issued pursuant to this Agreement, and that details the agreement between Brillion and Customer regarding: (a) the type of SaaS Solution, including Software, licensed under this Agreement and the terms of the license granted and/or (b) the Professional Services to be delivered by Brillion to Customer (or for and on behalf of Customer), and (c) the related Fees payable to Brillion. Additional documents, such as a SOW, may be attached to and made a part of an Order or may be executed separately.

Personnel. Means a Party's (a) employees or (b) authorized subcontractors, independent contractors, and/or third party service providers that are under legally binding obligations of confidentiality, nondisclosure, and security.

Personal Data. Means (a) any information that identifies, or makes possible the identification of, an individual including an End User, such as name, address, email address, telephone number, customer account number, or other personally identifiable information or makes possible the identification of an individual; (b) "non-public personal information" as that term is defined in the Gramm-Leach-Bliley Act found at 15 USC Subchapter 1, § 6809(4); and/or (c) any other information identified as personal information or non-public information under Federal, state or local privacy laws.

Professional Services. Means implementation, training, advisory, consulting, or other technical or professional services delivered by Brillion to Customer (as detailed in an Order or SOW), but excluding the SaaS Solution, the Software, and Support Services (as defined in Section 3 of the Agreement).

SaaS Schedule. Means the applicable Schedule (or Schedules) attached to the applicable Order that details the hosting services delivered by, or on behalf of, Brillion for the applicable SaaS Solution and Software.

SaaS Solution. Means, as applicable (a) Brillion's proprietary software as a service (SaaS) solution as detailed in the applicable Order and/or (b) a third party's proprietary SaaS system resold by Brillion to Customer and also as detailed in the applicable Order. For purposes of this Agreement and any Order, "SaaS Solution" includes any upgrades, changes, enhancements, modifications, or updates to the SaaS Solution, if any, made by Brillion and commercially delivered during the applicable Subscription Term.

Software. Means Brillion's proprietary software, in executable form, identified in the applicable Order (including, as applicable, any third party software integrated into such Brillion software or third party software that is integrated into the SaaS Solution), that will be hosted on computer systems controlled by Brillion. For purposes of this Agreement and any Order, "Software" includes any upgrades, changes, enhancements, modifications, or updates to the Software, if any, made by Brillion and commercially delivered during the applicable Subscription Term.

SOW. Means any written "Statement of Work" that is ancillary to the Agreement, but governed by and issued pursuant to this Agreement, and that details the agreement between Brillion and Customer regarding: **(a)** the Professional Services to be delivered by Brillion to Customer (or for and on behalf of Customer) and **(b)** the related Fees owed to Brillion.

Subscription Term. Means the time period during which Brillion will deliver the SaaS Solution and applicable Software to Customer as specified in the applicable Order and which may be either an initial or renewal Subscription Term.

Exhibit B
(Data and System Security Schedule)

This Data and System Security Schedule (the “**Schedule**”) is attached to and made a part of the Agreement.

CLOUD PLATFORM SECURITY STATEMENT

Brillion ensures the security and reliability of our SaaS Solutions by leveraging industry-leading cloud platforms such as Salesforce, Amazon Web Services (AWS), and Microsoft Azure. These platforms provide robust and proven cybersecurity infrastructure, including comprehensive disaster recovery capabilities. Brillion's SaaS Solutions are built and run on top of these PaaS offerings, benefiting from their extensive security measures, regular audits, and compliance with global security standards. This allows us to focus on delivering secure and reliable software solutions while ensuring that the underlying infrastructure is continuously monitored, updated, and protected against threats. Whenever relevant, this document refers to this PaaS infrastructure as “**PaaS providers**”.

1. LOGICAL ACCESS CONTROL

a. Access

- i. Brillion denies all access to information systems and resources by default. Access is granted by request for specific business purposes, and in accordance with the principles of least privilege and separation of duties. Brillion controls the use of administrative privileges by tracking and preventing the use, assignment, and configuration of administrative privileges on computers, networks, and applications through a formal access recertification process.
- ii. Brillion maintains appropriate usage restrictions and configuration/connection requirements for information systems (including wireless) access, which requires prior authorization for access to the systems prior to allowing such connections. All access to Brillion's information systems and resources is granted in accordance with established and published security policies.
- iii. Brillion maintains appropriate usage restrictions, configuration/connection requirements, and implementation guidance for organization-controlled mobile devices, and authorizes (as described above) the connection of mobile devices to organizational information systems in accordance with established and published security policies.

b. Account Management.

- i. Brillion configures its information systems and resources to enforce account-based access control policies and standards.

2. AWARENESS AND TRAINING

a. Security Awareness Training

- i. Brillion maintains, regularly reviews, documents, and administers security awareness training for all Brillion Personnel. The training addresses, at minimum, security roles and responsibilities, social engineering techniques, and business continuity/disaster recovery. Brillion provides incident response training to individuals with incident response roles.
- ii. Brillion provides additional security training to Personnel with security responsibilities or privileged access rights.
- iii. Training is administered as part of the new hire onboarding process and periodically thereafter.

3. AUDIT AND ACCOUNTABILITY

- a. Audit Logs.** Brillion's or its PaaS providers' information systems will generate audit logs containing the type of event, the date and time of the event, the location of the event, the source of the event, the outcome of and response to the event, the individual(s) associated with the event and any other information relevant to the event and provide such information to Customer upon request.

b. System Logging and Review

- i. Brillion's or its PaaS providers' information systems protect audit information, including audit records, audit settings, audit reports, and audit tools from unauthorized access, modification, and deletion. Audit information must be backed up onto a physically different system or system component than the system or component being audited.
- ii. Brillion retains audit logs to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
- iii. Depending on the relevant hosting environment in which the SaaS Solution will reside, and Customer Data will be processed, and as detailed in the applicable SaaS Schedule, such hosting environment will **(a)** have achieved SOC2 certification and **(b)** be subject to annual SOC2 audits.

- iv. Brillion's PaaS providers engage a qualified third party to conduct an audit of, and perform penetration testing on, the subject hosting environment. In lieu of authorizing Customer to conduct its own audit or penetration testing of the subject SaaS environment (but subject to a requirement under applicable law for Customer to have such audit conducted) and upon Customer's written request, Brillion will deliver to Customer: **(1)** as applicable, a copy of its latest SOC 2 report; and **(2)** a summary of the related annual penetration testing results.
- v. Brillion will respond to additional Customer information security questionnaires so long as such questionnaires are submitted to Brillion not more than once per twelve (12) month time period.

4. SECURITY ASSESSMENT AND AUTHORIZATION

- a. **Security Authorization.** Brillion has in place a security governance committee that serves as the authorizing entity for the information systems, ensures that such appropriate procedures are followed in authorizing the information systems for processing before commencing operations, and periodically updates the security authorization as needed.
- b. **Continuous Monitoring.** Brillion's PaaS providers maintain Intrusion Detection and Prevention Systems (IDPS) in order to enhance cybersecurity by continuously monitoring network traffic for suspicious activities, enabling real-time threat detection and automated responses to prevent unauthorized access and mitigate potential damage.

5. CONFIGURATION MANAGEMENT

- a. **Information System Component Inventory.** Brillion develops, documents, and regularly updates an inventory of information system components. Brillion detects, tracks, and restricts all hardware devices on its non-public networks so that only authorized devices are given access, and detects, tracks, and restricts all software on such networks so that only authorized software is installed.
- b. **Configuration Change Control.** Brillion establishes and implements change control processes designed to prevent unauthorized security changes to system configuration related to Customer Data that it maintains. Brillion tests, validates, and documents changes to the information systems before implementing the changes on the operational systems, and requires that an information security representative be a member of the security configuration change control team.

6. CONTINGENCY PLANNING

- a. **Contingency Plan.** Brillion develops a contingency plan for the information systems, which identifies essential business missions/functions and associated contingency requirements, provides recovery objectives and restoration responses, addresses contingency roles and responsibilities, addresses maintaining essential business functions in the event of system disruption or failure, and addresses full system restoration without deterioration of the security safeguards in place. The contingency plan is regularly reviewed and updated at least annually, and as needed to address changes in the threat environment.
- b. **Information System Recovery and Reconstitution.** Brillion and its PaaS providers promptly provide for the recovery and reconstitution of information systems to a state of normal operation after disruption, compromise, or failure. This recovery plan includes transaction-based recovery, and protects backup and restoration hardware, software, and firmware.

7. IDENTIFICATION AND AUTHENTICATION

- a. **Unique Identification.** Brillion's information systems uniquely identify and authenticate both organizational and non-organizational users and/or processes acting on behalf of users, such that all user activity can be traced back to the individual(s) who performed the activity. Brillion's systems employ industry standard encryption for all authentication mechanisms, provide for federated identity capabilities, and, whenever appropriate, implement replay-resistant authentication mechanisms, such as multifactor authentication.
- b. **Authentication Management.** Brillion manages information system credentials/authenticators using industry best practices. Brillion takes into consideration the type of authentication (e.g., hardware token-based, software/SMS multi-factor, PKI-based, password-based, biometric-based, etc.) and applies additional security controls as appropriate.

8. INCIDENT RESPONSE

- a. **Incident Response Program.** Brillion maintains a written incident response program that addresses cybersecurity event preparation, detection, analysis, containment, eradication, and recovery. This program includes procedures that describe: **(i)** roles and responsibilities of the incident response team; **(ii)** communication requirements with internal and external partners; **(iii)** plans to detect, respond to, and contain common incident categories; **(iv)** methods to preserve evidence, maintain chain of custody, and perform forensic analysis; **(v)** coordination of recovery processes; **(vi)** follow-up processes; and **(vii)** reporting to ensure critical details of incidents are tracked and lessons learned are incorporated into ongoing response procedures, training, and testing. The incident response program is reviewed and updated at least annually.
- b. **Incident Handling.** If Brillion discovers or is notified of any security incident that impacts or may impact Customer Data and/or systems, Brillion will promptly: **(i)** investigate the security incident; **(ii)** remediate, mitigate, or remediate

and mitigate, the risk to the Customer Data or systems and other effects of the security incident; (iii) preserve all related records and other evidence; and (iv) implement a plan to prevent such a security incident from reoccurring.

- c. **Incident Notification.** If Brillion discovers or is notified of any security incident, Brillion will immediately notify Customer thereof in writing, but no later than seventy two (72) hours from the time Brillion becomes aware of a security incident, including disclosing (i) the date, time, and cause of the incident if known; (ii) the Customer Data and/or systems that were exposed or reasonably believed to have been exposed; and (iii) whether nonpublic personally identifiable information was accessed.
- d. **Reporting.** Brillion will provide Customer with a written report on the outcome of its investigation including any risk to Customer Data and/or systems, the corrective action Brillion has taken to respond to the security incident, and such other information as Customer may reasonably request regarding the security incident.

9. MAINTENANCE

- a. **Nonlocal Maintenance.** Brillion: (i) approves, documents, and monitors nonlocal maintenance and diagnostic activities; (ii) allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; (iv) maintains records for nonlocal maintenance and diagnostic activities; and (v) terminates session and network connections when nonlocal maintenance is completed.
- b. **Timely Maintenance.** Brillion and its PaaS providers approve, obtain, and document the maintenance, support, and repair of information systems and information system components in a timely manner following system or component failure. Security controls potentially impacted during maintenance or repair activities are inspected for proper function post-activity. Brillion promptly applies software patches, updates, and code fixes, when available.

10. MEDIA PROTECTION

- a. **Media Use.** Brillion will not store unencrypted confidential information on any portable device.
- b. **Media Sanitization.** Brillion sanitizes information system media prior to disposal, release from organizational control, or release for reuse in accordance with organizational policies, employing sanitation mechanisms with the strength and integrity commensurate with the security category or classification of the information.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

- a. **Physical Access Control.** Brillion's PaaS providers: (i) enforce physical access authorizations at facility entrance/exit points by verifying individual access authorizations before granting access to the facility; (ii) maintain physical access audit logs for entry/exit points; and (iii) use security safeguards to control access of such facilities, including the use of security guards, as appropriate, and physical access control devices (e.g. alarms, card swipe, keypads).
- b. **Power Equipment and Cabling.** Brillion's PaaS providers protect power equipment and cabling for the information systems from damage and destruction, including leveraging of physically separate, redundant power cables to ensure that power continues to flow if one cable is cut or otherwise damaged, as well as automatic voltage controls for critical information system components.
- c. **Location of Information System Components.** Brillion's PaaS providers position information system components within the facility to minimize potential damage from environmental hazards (e.g. flooding, fire, tornados, earthquakes, hurricanes, vandalism, acts of terrorism, electromagnetic pulse, electrical interference, etc.) as well as physical hazards, including the opportunity for unauthorized access.

12. PLANNING

- a. **Information Security Architecture.** Brillion maintains cognizance of information security principles in the architecture of all of its products and services, including the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface.
- b. The information security architecture is reviewed and updated regularly to reflect updates in the enterprise architecture, external impacts, and industry practices, reflecting them in its security planning and operations.

13. PERSONNEL SECURITY

- a. **Personnel Screening.** Brillion screens individuals prior to authorizing access to Brillion's information systems and performs re-screening (as reasonably determined by Brillion), including background checks.
- b. **Personnel Termination.** Upon termination, Brillion promptly: (i) disables the individual's information system access; (ii) terminates/revokes any authenticators/credentials associated with the individual; (iii) conducts exit interviews that include information security topics; (iv) retrieves all security-related organizational information system-related property (e.g. hardware authentication tokens, system administration technical manuals, keys, identification cards, building passes, etc.); and (v) retains access to organizational information and information systems formerly controlled by terminated individual.

14. RISK ASSESSMENT

- a. **Risk Assessment.** Brillion: (i) conducts a risk assessment, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems and the information they process, store, or transmit; (ii) documents and reviews the risk assessment results; and (iii) updates the risk assessment regularly, and whenever there are significant changes to the information system or environment of operation (e.g. the identification of new threats and vulnerabilities).
- b. **Vulnerability Scanning.** Brillion and its PaaS providers: (i) periodically scan for vulnerabilities in the hosted applications and when new vulnerabilities potentially affecting the system/applications are identified; ; (ii) analyze vulnerability scan reports and results from security control assessments; (iii) remediate vulnerabilities in accordance with organizational risk assessment; (iv) share information from the vulnerability scanning and security control assessments with appropriate Personnel to help eliminate similar vulnerabilities in other information systems; and (vi) employ periodic external vulnerability scanning and annual penetration testing to assess the overall strength of Brillion's defenses (technology, processes, and employees). Upon Customer's written request, and whenever this is under Brillion's control, Brillion will deliver to Customer a summary of the results of the most recent vulnerability scans and penetration tests.

15. SYSTEM DEVELOPMENT LIFE-CYCLE

Brillion manages information systems using industry standard System Development Life Cycle ("SDLC") that incorporates information security considerations, defines and documents information security roles and responsibilities throughout the SDLC, identifies individuals having such roles or responsibilities, and integrates Brillion's information security risk management process into SDLC activities.

16. SYSTEMS AND COMMUNICATIONS PROTECTION

- a. **Transmission Confidentiality and Integrity.** Information systems protect the confidentiality and integrity of transmitted information through both physical and logical means, including employing protected distribution procedures and limiting access to peripherals (e.g. servers, computers, printers, scanners, facsimile machines), and through the use of encryption.
- b. **Information Protection.** Any Customer Confidential Information, either at rest or in transit, will be encrypted in accordance with FIPS Publication 140-2 (FIPS PUB 140-2). Use of encryption will be compliant with all applicable export laws, rules, and regulations.

17. SYSTEM AND INFORMATION SYSTEM INTEGRITY

- a. **Flaw Remediation.** Brillion: (i) identifies, reports, and corrects information system flaws; and (ii) installs security-relevant software updates, including patches, service packs, hot fixes, and anti-virus signatures, once they are available. Brillion centrally manages the flaw remediation process, which establishes procedures for taking corrective actions.
- b. **Malicious Code Protection.** Brillion: (i) employs malicious code protection mechanisms at information system exit and entry points (including web browsers and email) to detect and eradicate malicious code; (ii) updates malicious code protection mechanisms whenever new releases are available and maintains organizational configuration management policy and procedures for managing such updates; (iii) configures malicious code protection mechanisms to perform periodic scans of the information systems and real-time scans of files from external sources, as the files are downloaded, opened, or executed; (iv) blocks, quarantines, or both, malicious code and maintains systems that send alerts to system administrator(s) in response to malicious code detection; and (v) addresses the receipt of false positives during malicious code detection and eradication, as well as all resulting potential impact on the availability of the information systems.