

## Attachment E (continued)

### EMC Infrastructure Managed Services (IMS) Terms

#### 1. Disengagement/Transition/Wind-Down Services

In the event of termination or expiration of the Agreement or any SOW, Customer and Provider shall use commercially reasonable efforts to agree on a Disengagement Plan (a) at least sixty (60) days prior to the expiration of the applicable SOW; or (b) in the event of termination, within thirty (30) days immediately following notice of such termination. The terms of the Agreement will continue to apply during any Disengagement Period except to the extent mutually agreed to in the Disengagement Plan.

#### 2. Change in Customer Laws

Customer shall promptly identify and notify Provider of any changes in law, including regulatory requirements, that may relate to Customer's use or Provider's delivery of the Services. The parties shall work together to identify the impact of such changes on how Customer uses, and Provider delivers, the Services. In the event that a change in law results in Provider being unable to deliver the Services, or results in an increase in the cost of providing the Services that Customer declines to pay, Provider may suspend its obligation to provide the affected Services with no further liability under the applicable SOW, and Customer shall be responsible for any losses arising from any noncompliance by Customer with any law relating to Customer's use or consumption of the affected Services. If a change in law prevents or delays Provider from performing its obligations under this Agreement, the parties shall endeavor to develop and implement such changes to the Services as may be required in order to comply with changes in law; provided that Customer shall be responsible for any additional fees for the Services and costs incurred by Provider in connection with the changes to Services, at Provider's then-current rates.

#### 3. Service Levels

Provider shall perform the Services in accordance with Appendix 2 (Service Level Methodology) and the Service Levels set forth in the applicable SOW. In the event Provider fails to meet the applicable Service Levels, the Service Credit calculated in accordance with Appendix 2 (Service Level Methodology) and the applicable SOW shall be Customer's sole and exclusive remedy. Provider shall not be responsible for the failure to meet any Service Level to the extent that any such failure is attributable to any of the Excused Events set forth in Appendix 2 (Service Level Methodology).

#### 4. Tracking of Use/Consumption of Services

For consumption-based Services, Provider shall monitor and/or audit the billable volumes in order to calculate the applicable fees. Provider shall conduct such activity through the use of electronic means, remote access and/or on-site inspection by Provider's Personnel in order to authenticate Customer as the user of the Services and verify the Customer's billable volumes. Customer will take any actions required by Provider to permit such tracking of billable volumes and provide access to all necessary equipment. If Provider is unable to monitor billable volumes for any reason, Customer shall pay an amount for the affected Service period based on Customer's average billable volumes during the previous three (3) months. Provider shall promptly notify Customer of an inability to electronically and or physically access the Assets, as applicable, and work cooperatively to reestablish access. Once access is reestablished, then Provider shall provide a corrected invoice for the affected Service Period.

5. Audit

***Audits Generally***

Provider shall cooperate with Customer's reasonable audit requirements as such requirements are articulated in an applicable SOW, to enable Customer and its Approved Auditors to conduct appropriate audits of the Services as required by the applicable SOW; provided, however, that in no event shall Provider be obligated to (a) disclose confidential information of any third party to whom Provider owes a duty of confidentiality, or (b) disclose proprietary information regarding the means and methods by which Provider provides the Services. In furtherance and not in limitation of the foregoing, if reasonably required to protect Provider's confidential and proprietary information or to avoid breaching a confidentiality obligation owed to a third party, Provider may elect to provide (in good faith) data/information responsive to an inquiry rather than access to the associated systems, controls, equipment, or other materials. Customer will not be granted access to any facilities, equipment, or materials that (a) are not directly and solely related to the provision of the Services for Customer and/or (b) contain the proprietary or confidential information of a third party. The results of any audit shall be considered the Confidential Information of Provider.

***Audit Procedures***

Upon request, at reasonable times during business hours, and upon at least thirty (30) business days' prior notice to Provider and no more than once per year, Customer and Approved Auditors shall have access to Customer's records and Provider records directly related to the Services in order to audit Service Level performance and the accuracy of Provider's invoices, provided that no such information shall be taken offsite or otherwise disclosed to any third party. Notwithstanding anything herein, Customer and its Approved Auditors shall not have access to other Provider records, records of other Provider customers or suppliers, or records related to Provider's internal or third party costs or cost structure. Approved Auditors shall observe such procedures as Provider may reasonably require to protect any information disclosed to them, all of which shall be deemed to be Provider's Confidential Information. Customer shall cause Approved Auditors to perform entry and exit interviews, and to provide Provider with copies of the audit reports.

***Costs***

If Provider is required to provide services or incur costs, other than of a routine nature, in connection with any audit performed pursuant to this Section, then Customer shall pay for such services and costs at Provider's then-current rates.

6. Security

Provider will comply with the Provider security framework detailed in Appendix 3 (Security Framework), and any additional security requirements set forth in an SOW.

7. Relationship Management

***Governance***

Governance of the parties' relationship pursuant to this Agreement will follow the guidelines and principles set out in Appendix 4 (Governance). Each party will make management decisions, respond to the communications and perform the other governance responsibilities set forth in Appendix 4 (Governance) in a timely manner.

***Dispute Resolution***

Any dispute arising under this Agreement shall be considered in person or by telephone by the Customer Relationship Manager and the Provider Service Manager within seven (7) business days of receipt of a notice from either party specifying the nature of the dispute; provided, however, that a dispute relating to Provider's proprietary rights or intellectual property rights shall not be subject to this Section and Provider shall retain

the right to pursue its rights and remedies in law and equity. Unless the Customer Relationship Manager and the Provider Service Manager resolve the dispute, such dispute will be escalated through the process described in Appendix 4 (Governance).

## 8. Customer Responsibilities

### ***Use of Services***

Except as otherwise provided in an SOW, the Services shall only be used for the internal use and benefit of Customer and Customer shall not permit any third party to access or use the Services. Customer will not use, and will not authorize any third party (other than Provider, if applicable), to use any open source software in connection with the Services in any manner that requires, pursuant to the license applicable to such open source software, that any Provider Confidential Information or Services be (i) disclosed or distributed in source code form, (ii) made available free of charge to recipients, or (iii) modifiable without restriction by recipients. Provider owns all intellectual property rights in the Services, or Provider has the rights necessary to provide to provide Services as contemplated by this Agreement. Except the right to use the Services as set out herein, this Agreement does not grant Customer any rights to, or in, any intellectual property or any other rights or licenses in respect of the Services and Provider and its third party providers reserve all rights not expressly granted herein. Provider owns any ideas, suggestions or other feedback that the Customer may provide to Provider with respect to the Provider business, products and/or services (including the Services), and Customer hereby assigns all right, title and interest to such feedback to Provider.

### ***Customer Data and Licenses***

Customer represents that it: (i) owns or has the right to use all Customer Materials, data and content which are processed by, stored on or used in relation to the Services; and (ii) has all necessary licenses and permissions for usage of any third party software to be supplied/provided by Customer to Provider and used with the Services. Customer hereby grants to Provider the right to use all such data, content and third party software solely for the purposes of this Agreement and the performance of Provider's obligations hereunder. Customer shall encrypt any data or content prior to storage of such data or content on Provider's platform.

Provider offers Services to other customers in addition to Customer, and with respect to tenant compute security capabilities, the responsibility for deploying, implementing and measuring compliance is the responsibility of the applicable customer/Customer. To the extent applicable to the delivery of agreed upon specific contracted for Services, Provider will comply with the intent of the security controls agreed upon in this Agreement or an applicable SOW. Applicability of specific agreed upon controls for Services shall be listed in the applicable SOW.

### ***Customer Managers***

Customer shall maintain an individual who shall serve as the primary Customer representative under this Agreement ("**Customer Relationship Manager**"). The Customer Relationship Manager shall: (a) have overall responsibility for managing and coordinating the performance of Customer's obligations under this Agreement and (b) be authorized to act for and on behalf of Customer with respect to all matters relating to this Agreement.

### ***Customer Responsibilities***

Customer shall, upon Provider's request: (1) make available to Provider, Customer technical personnel familiar with Customer's business requirements; (2) provide to Provider complete and accurate information regarding Customer's business requirements in respect of any work to be performed by Provider under the applicable SOW; (3) respond within the time period specified in this Agreement or the applicable SOW (or if no time period is specified, within three (3) business days) to all Deliverables presented to Customer by Provider for Customer's approval, or other requests for approvals, which approval shall not be unreasonably

withheld or delayed, provided however approval shall be deemed to have been provided if Customer has not responded within the applicable time; (4) cooperate with Provider; (5) promptly notify Provider of any third party claims or invalid or nonexistent licenses that may have an impact on this Agreement or the Services; (6) give Provider Personnel and its subcontractors access to the Customer Service Location to the extent reasonably necessary for them to perform the Services, including to effect the necessary adjustments, maintenance and repairs; (7) provide any Required Data, and (8) perform all other obligations of Customer described in this Agreement and any SOW. Customer shall not act in a way that affects or impacts the Assets or Services without Provider's prior written approval.

***Remote Access***

Customer shall provide and maintain remote access to Provider for the purposes of providing the Services. Any equipment and software needed to enable electronic communications for the purposes of providing remote access shall be provided by Customer to the specifications stated in the applicable SOW. Customer authorizes Provider to store at the Customer Service Location, or load onto the products used for electronic communications, such equipment and programming as may be needed by Provider to track usage levels or perform any repair or maintenance related services for the Assets.

***Customer Resources***

Customer shall provide to Provider, at no charge to Provider: (a) use of space for the Assets (if any), at a time on or before arrival of the Assets; (b) necessary power, cooling and space required to support the Assets; (c) servers, power and network connectivity required to support the Assets and any related software; (d) access to any Customer Service Location(s) and related facilities and infrastructure that Provider reasonably requires for business purposes in connection with the performance of the Services; (e) full access to, and use of, the Customer Supplied Products, which Customer shall maintain in good repair and working and usable condition as required by Provider to provide the Services; and (f) such other resources specified in the Agreement and the applicable SOW. Customer shall further provide Provider with the services, utilities, equipment and supplies reasonably necessary for Provider to provide the Services consistent with that which Customer provides to its own personnel, including office space, office furnishings, janitorial service, local telephone service, utilities (including air conditioning), office-related equipment, supplies, duplicating services, and premises security in the Customer Service Locations. At all Customer Service Locations, Customer will provide Provider access to and use of Customer's voice and data telecommunications equipment and transmission lines, including printers, terminals and cabling. Customer will give Provider access to such facilities twenty-four (24) hours a day, seven (7) days a week. Customer shall provide adequate storage space for spare parts and adequate working space including heat, light, ventilation, electrical current and outlets for the use by Provider's Personnel. These facilities will be within a reasonable distance from the Assets to be serviced and will be provided at no charge to Provider. Customer shall maintain and repair all facilities accessible by Provider in compliance with all laws. Customer will be responsible for all reasonable leasehold improvements to the Customer Service Locations required for Provider to deliver the Services. Customer will also be responsible for all costs and expenses associated with any relocation of Provider's operations that are done at Customer's request, provided that nothing contained herein shall obligate Provider to relocate operations unless mutually agreed to by the parties in a Change Order. Customer shall ensure that Provider is legally authorized to use any resources provided by Customer.

***Product Utility***

To the extent Provider is providing Assets for Customer's use, such use shall be in accordance with Appendix 5 (Assets).

9. Proprietary Rights

### ***Customer Software***

Customer hereby grants to Provider, or undertakes to secure the necessary rights for Provider from the owner of the Customer Software on behalf of Provider as applicable, at no cost to Provider, a nonexclusive right to access and use, load, execute, store, transmit, display, copy, maintain, the Customer Software in connection with the provision of the Services. Upon the expiration or termination of the Agreement, the rights granted to Provider in this Section shall immediately terminate and Provider shall, at Customer's request, cease all use and make available for return to Customer, or at Provider's option, certify destruction of Customer Software (including copies) to Customer. Unless otherwise specified in an SOW, Customer shall pay all costs and expenses with respect to the Customer Software, including the costs associated with maintenance, license payments, insurance, taxes and the consents. Except as set forth in an SOW, Customer is responsible for maintaining, upgrading, and replacing the Customer Software as necessary for Provider to deliver the Services. In the event that Customer does not comply with such obligations, Provider shall be excused from its obligation to perform the Services, including Provider's obligation to meet the Service Levels, to the extent that its inability to meet such obligations is caused by Customer's failure to comply with its obligations under this Section.

### ***Provider Proprietary Software***

To the extent use by Customer of Provider Proprietary Software or other Provider proprietary information is authorized or contemplated by an SOW, Provider grants Customer a limited license to use the Provider Proprietary Software solely for Customer's internal use in connection with its receipt of Services for the Term unless sooner terminated or cancelled. The foregoing licenses shall be non-exclusive, non-transferable, non-sublicensable, revocable and subject to the restriction that the Provider Proprietary Software be used solely in the manner described in the applicable SOW and for no other purpose. If authorized, the license contemplated herein shall solely apply to Provider Proprietary Software. Provider may terminate licenses, without liability, if Customer breaches this Agreement or any SOW, or if this Agreement is otherwise terminated or suspended. Upon any such termination Customer shall cease all use and if applicable, certify destruction or erasure of Provider Proprietary Software (including all copies). Customer shall not, without Provider's prior written consent, copy, provide, disclose or otherwise make available Provider Proprietary Software in any form to anyone other than Customer or Customer Representatives, who shall use Provider Proprietary Software solely to the extent necessary to receive the Services as contemplated by the applicable SOW and solely for Customer's internal business purposes. In no event shall Customer's internal business purposes be construed to include use of the Provider Proprietary Software by Customer's customers, unless otherwise stated in the applicable SOW. Customer shall be liable to Provider for the compliance of its personnel herewith.

### ***Provider Third Party Software***

Where Provider Third Party Software is licensed by Provider for use in the provision of Services, Provider will procure a license for Customer to access and use the Provider Third Party Software, solely to the extent necessary for the receipt of Services under the relevant SOW. The license insofar as it relates to an SOW will terminate on the expiration or termination of that SOW. Provider may be required to flow down terms related to Provider Third Party Software to Customer. In such event, Provider shall provide such additional terms and conditions to Customer upon request.

### ***Deliverables***

Provider shall retain ownership of all Deliverables, work product and all other materials provided to Customer (Provider does not perform work for hire), provided that Customer shall retain ownership of its Confidential Information embedded (if any) in any such Deliverables or other materials. Provider grants Customer for a period of one year following termination of the Services, a non-exclusive, non-sublicensable, non-transferable license to use, copy, maintain and modify such Deliverables or other materials solely for Customer's internal business purposes and solely in conjunction with the Services or disengagement from the Services; Customer shall not provide or otherwise disclose Deliverables or any Provider intellectual property to any third party,

including any third party service providers or Provider competitors (as reasonably determined by Provider), without prior written consent from Provider.

***Ownership of Provider IP***

No title to, or ownership of, the Provider Proprietary Software or documentation is transferred to Customer. Neither Customer nor any of its agents, personnel, or independent contractors shall modify, enhance, supplement, create derivative works from, reverse assemble, reverse engineer, reverse compile or otherwise reduce to human readable form the Provider Proprietary Software without Provider's prior written consent. Any Provider Proprietary Software that is accompanied by a "break-the-seal" hard-copy license agreement or is obtained after indicating acceptance of a license agreement by electronic means shall be governed solely by the terms of this Agreement and the applicable SOW and not by the terms of such accompanying license. Any Provider Third Party Software shall be governed by the terms applicable thereto. Provider does not convey nor does Customer obtain any right in programs, configurations, systems or materials utilized or provided by Provider in the ordinary course of business in the performance of the Services other than as described in this Agreement. Provider may bring onto and store at Customer's premises certain manuals, tools and software which will be used by Provider to maintain the Assets, and Assets may have maintenance code loaded on them from time to time. Such manuals, tools and software, including maintenance code, are the property of Provider, regardless of whether or not such items contain any confidential markings, and Provider may remove all such manuals, tools and software at any time. To the extent required, Customer hereby grants Provider the right to execute Provider's maintenance-related software on the Assets and any host central processing unit to which such Assets are attached. Notwithstanding anything to the contrary in this Agreement, Provider shall retain all right, title and interest in and to any and all ideas, concepts, know-how, development tools, developments, methodologies, processes, procedures, technologies or algorithms and tools which are based upon trade secrets or proprietary information of Provider, including all enhancements, modifications or improvements thereto. Provider retains all rights not expressly granted herein.

***Reservation of Proprietary Rights***

Each party reserves for itself all proprietary rights that it has not expressly granted to the other. Provider and/or its licensors own all intellectual property rights in the Services and any Deliverables. Except as expressly stated herein, this Agreement does not grant Customer any rights to, or in, any intellectual property or any other rights or licenses in respect of the Services. Provider shall not be limited in developing, using or marketing services or products which are similar to the Deliverables or Services provided hereunder, or, subject to Provider's confidentiality obligations to Customer, in using the Deliverables or performing similar Services for any other projects or customers.

10. Warranties

***Mutual***

Each party hereby warrants to the other that: (a) it is a corporation duly incorporated and in good standing under the laws of its state of incorporation; (b) the execution of this Agreement has been duly authorized by the requisite corporate action on the part of such party; (c) it has obtained (or will obtain) all licenses, authorizations, approvals or permits required to perform its obligations under this Agreement, except to the extent the failure to obtain any such license, authorizations, approvals, consents or permits is, in the aggregate, immaterial; (d) it shall comply with all laws applicable to such party during the Term.

***By Provider***

Provider warrants that all Services provided hereunder will be provided in a professional and workmanlike manner. Provider shall use commercially reasonable efforts to deliver the Services in accordance with the applicable SOW.

### ***By Customer***

Customer warrants that: (a) all Customer information systems, Customer Service Locations and Customer Supplied Products that are required under an SOW shall be made available for use by Provider to provide the Services and are available and operating in accordance with their specifications; and (b) the Required Data is and shall be true and accurate and shall meet the requirements specified in the applicable SOW.

### **DISCLAIMER**

**PROVIDER DOES NOT WARRANT THE ACCURACY OF ANY ADVICE, REPORT, DATA OR DELIVERABLES PROVIDED TO CUSTOMER BY PROVIDER THAT ARE PRODUCED WITH OR FROM DATA OR SOFTWARE PROVIDED BY CUSTOMER. SUCH ADVICE, REPORTS, DATA OR DELIVERABLES ARE PROVIDED "AS IS", AND PROVIDER SHALL NOT BE LIABLE FOR ANY INACCURACY THEREOF. OTHER THAN AS EXPRESSLY SET FORTH HEREIN, THE SERVICES, CLOUD SERVICES AND ANY RELATED EQUIPMENT, SOFTWARE AND OTHER MATERIALS PROVIDED BY PROVIDER IN CONNECTION WITH THE SERVICES ARE PROVIDED WITHOUT ANY WARRANTIES OR REPRESENTATIONS OF ANY KIND, WHETHER STATUTORY OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS OR ANY RESULTS TO BE ACHIEVED HEREFROM. PROVIDER MAKES NO WARRANTIES OR REPRESENTATIONS CONCERNING THE COMPATIBILITY OF SOFTWARE OR EQUIPMENT OR ANY RESULTS TO BE ACHIEVED THEREFROM, OR THAT ANY SERVICES WILL BE FREE FROM LOSS OR LIABILITY ARISING OUT OF ANY THIRD PARTY TECHNOLOGY, ANY THIRD PARTY ACTION SUCH AS HACKING, OR ANY ACT OR OMISSION OF CUSTOMER, INCLUDING FAILURE TO ENCRYPT, AND PROVIDER SHALL HAVE NO RESPONSIBILITY THEREFOR. PROVIDER EXPRESSLY DISCLAIMS ANY WARRANTY OR LIABILITY WITH RESPECT TO COMPLIANCE WITH LAWS, REGULATIONS, OR OTHER OFFICIAL GOVERNMENT RELEASES APPLICABLE TO CUSTOMER, WHICH SHALL BE THE SOLE RESPONSIBILITY OF CUSTOMER.**

### 11. IP Infringement

Provider shall, at its own expense defend Customer against any claim by a third party that the Services infringe any copyright or United States patent and pay the resulting costs and damages finally awarded against Customer by a court of competent jurisdiction to the extent that such are the result of the third party claim, or pay the amounts stated in a written settlement negotiated and approved by Provider. If the Services are subject to a claim of infringement or misappropriation or, in Provider's opinion, is likely to become, the subject of such a claim, Provider shall, at Provider's option and expense: (i) procure for Customer the right to continue use the Service; (b) replace or modify such Service so that it becomes non-infringing while retaining substantially equivalent functionality; or (c) if Provider determines that none of the foregoing are commercially reasonable, terminate this Agreement and/or the applicable SOW and refund to Customer the price paid for the allegedly infringing Services by Customer in the immediately preceding six (6) month period. Provider shall have no liability if the alleged infringement is based on: (1) combination of the Services or any Provider provided materials with (a) any products, services, items, or technology not provided by Provider, or (b) any non-Provider products or services; (2) use of Service (i) for a purpose or in a manner that is not expressly permitted by the Agreement, or applicable SOW, and/or (ii) after Provider notifies Customer to cease such use due to a possible or pending claim of infringement; (3) any modification to the Services not made by Provider; (4) any modifications made by Provider pursuant to Customer's or an end-user's specific instructions; (5) any intellectual property right owned or licensed by Customer (or any End User), including any data or information that Customer or a third party provides, records on or utilizes in connection with Customer's use of the Services and/or Provider's provision of the Services; (6) violation by Customer or an End User of Service Provider's acceptable use policy (to the extent applicable); and/or (7) any Provider product that was licensed or purchased by Customer under a separate agreement, in which case any third party infringement claim brought against Customer alleging infringement in connection with Customer's use

of such Provider product will be governed exclusively by the provisions of such separate agreement. This section states Customer's sole and exclusive remedy and Provider's entire liability for infringement claims related to the Services.

## 12. Third Party Products

To the extent Provider is responsible for the provision of Third Party Products hereunder, such Third Party Products shall be identified in the applicable SOW and this Section shall apply. Unless otherwise stated in the applicable SOW, Provider shall have no responsibility for the provision of Third Party Products. Notwithstanding anything herein to the contrary, Customer shall comply with all terms and conditions applicable to such Third Party Products as included in the SOW and such terms and conditions shall supersede any conflicting terms in this Agreement.

With respect to any Third Party Products provided by Provider under this Agreement, Provider shall pass through to Customer, to the extent possible under Provider's agreement with the relevant vendor, the applicable indemnification rights it obtains from such vendor for such Third Party Products and Provider shall have no indemnification obligations with respect to such Third Party Products.

## Appendix 1 – Definitions

**“Approved Auditor”** means Customer's auditors, with the exception of auditors that compete directly or through affiliates with Provider, that execute a non-disclosure agreement in a form acceptable to Provider.

**“Asset”** means the hardware, software and related assets installed at a Customer Service Location and used to provide the Services, including those detailed in an SOW.

**“Asset Life”** means the refresh lifecycle defined for that class of Asset in the SOW.

**“At Risk Amount”** means the maximum percentage of the monthly Charges which are available to be paid or accrued as Service Credits for that month.

**“Business Day”** means Monday through Friday, local time, excluding public holidays observed by Provider.

**“Change”** means with reference to the Agreement, Appendices and SOWs, a proposed change which would require a Change Order to be agreed between the Parties; and with reference to the technical environment, the proposed addition, modification or removal of an item that could have an effect on the Services.

**“Change Order”** means a document agreed upon by the parties in accordance with the Change Control Process that alters the terms or services described within an SOW.

**“Change Window”** means the period of time during which a technical Change has been approved for implementation, having regard to potential downtime and other impacts.



**“Charges”** means the monthly fees for the Services calculated in accordance with an SOW.

**“Commencement Date”** means the date defined as such in an SOW.

**“Customer Material”** means hardware, software, and any other materials and information to which Provider has been provided access in connection with the Services.

**“Customer Supplied Products”** means the products referenced as such in an SOW.

**“Customer Representatives”** means contractors and agents of Customer.

**“Customer Service Location”** means the Customer’s location where Services will be delivered and where Assets may be located, as listed in an SOW.

**“Customer Software”** means software developed or owned by the Customer, and software used, licensed or leased by the Customer from a third party.

**“Deliverable”** means those written deliverables expressly identified as such in the applicable SOW.

**“Disengagement Period”** means the period during which Disengagement Services are delivered.

**“Disengagement Plan”** means the plan detailing the method and schedule of delivery of Disengagement Services, and the associated fees.

**“Disengagement Services”** means the services delivered by Provider to assist Customer in disengaging from the Services, as defined in an SOW.

**“Earnback”** means the process described in Section 7 of Appendix 2 (Service Level Methodology) by which Provider is able to earn financial relief from incurred Service Credits.

**“Earnback Period”** means the six (6) calendar months immediately following the month in which a Service Level Default is experienced, not including that month in which the Service Level Default occurs.

**“Earnback Report”** means a report, issued monthly, showing average performance against the Service Levels over the Earnback Period.

**“Escalation Process”** means the process set out in Section 6 of Appendix 4 (Governance Model).

**“Excused Event”** means an event aligning with an event type listed as such in Appendix 2 (Service Level Methodology).

**“Go Live”** means the date, specified in each SOW, on which the Steady State Services commence.

**“Governance Model”** means the model by which the relationship between the parties is governed, as set forth in Appendix 4 (Governance).

**“In-Scope Environment”** means the environment to which the Provider supplies the Services, as defined in an SOW.

**“Key Performance Indicator”**, or **“KPI”** means a measure of Provider’s performance of the Services which are not Service Levels and are not subject to Service Credits, but are specifically stated in the SOW or a run book.

**“Measurement Period”** means a calendar month during which Service Levels are in force.

**“Personnel”** means Employees, agents, subcontractors, consultants and representatives provided or to be provided by Provider to perform the Services pursuant to this Agreement.

**“Provider Proprietary Software”** means any and all versions of software licensed directly by Provider or Provider Affiliate (and not through distribution or sublicensing) as a standard Provider product.

**“Provider Service Location”** means the Provider locations from where Provider will deliver the Services.

**“Provider Third Party Hardware”** means hardware provided by Provider and manufactured by a third party that is used in connection with the Services.

**“Provider Third Party Software”** means any and all versions of software that is licensed by Provider from a third party that is used in connection with the Services.

**“Required Data”** means any data reasonably required by Provider from Customer to support Provider’s performance of the Services.

**“Root Cause Analysis”** means the process and review by which the primary cause of an Incident or Problem is identified and determined.

**“Security Incident”** means any event, act or omission which is defined as a security incident within Provider’s information security policies.

**“Service Credit Allocation”** means the weighting allocated to each Service Level within an SOW, expressed as a percentage, and referenced in the calculation of Service Level Credits.

**“Service Credit”** means the amount, calculated in accordance with Section 5 of Appendix 2 (Service Level Methodology), payable by Provider to Customer as a result of a Service Level Default.

**“Service Establishment Services”** means the activities performed in preparation for Go Live and the commencement of Steady State Services, as defined in an applicable SOW.

**“Service Level”** or **“SLA”** means a target performance standard applicable to Provider’s delivery of the Services, as defined in an SOW.

**“Service Level Dashboard Report”** means a monthly report prepared by Provider and presented to Customer, detailing Provider’s achievement against the Service Levels during the previous Measurement Period.

**“Service Level Default”** means a failure by Provider to meet or exceed a Service Level, determined in accordance with Section 4 of Appendix 2 (Service Level Methodology).

**“Service Level Target”** means the level of performance agreed between the parties for a particular Service Level.

**“Service Window”** means the period during each day within the Measurement Window when specific Service Levels are to be measured.

**“Services”** means the services specifically defined within an SOW.

**“SOW”** means a statement of work executed by the parties that describes the various services to be provided to Customer by Provider, including Services.

**“Stabilization Period”** means the period after Go Live during which any remaining Service Establishment Services are completed and any Provider-defined service improvement activities are undertaken in order to achieve stability within the Services, the length of such period to be defined in the SOW.

**“Steady-State Services”** means the Services defined as such in the applicable SOW.

**“Third Party Products”** means any equipment, software or other products and services provided by Provider to Customer under this Agreement but were obtained by Provider from a third party (such as an EMC select product, brokerage product, or any other technology, item or service not developed or manufactured by Provider) which Provider utilizes in providing the Services, including Provider Third Party Hardware and Provider Third Party Software.

## Appendix 2 – Service Level Methodology

---

### 1 General

- 1.1 The methodology set out in this Appendix 2 will support the Service Level management cycle of agreeing, monitoring, reporting and improving the delivery of the Services to Customer.
- 1.2 Specific terms applicable to Service Levels are set out in SOWs (where relevant) including the Service Level definitions, their measurement criteria and how they are calculated.
- 1.3 Commencing on the first of the month following expiration of any Stabilization Period defined within an SOW, or where no Stabilization Period is defined, the first of the month following commencement of Steady-State Services, Provider will perform the Services with the goal of meeting or exceeding the Service Levels.
- 1.4 If the Services provided under any SOW are changed, modified or enhanced in accordance with the Agreement, the parties will review the Service Levels then in effect and in good faith determine whether the Service Levels should be adjusted, or whether additional Service Levels should be implemented in accordance with the Change Control Process set out in Appendix 4 (Governance Model).
- 1.5 If there is a Service Level Default in any Measurement Period, Provider will provide a Service Credit to Customer calculated in accordance with Section 5.1 below and take the other action described in this Appendix.
- 1.6 The parties acknowledge that the achievement of the Service Levels by Provider will require the coordinated, collaborative effort of Provider and Customer.

---

## **2 Measurements**

- 2.1 Each Service Level will be measured during the Service Window applicable to the particular Service Level. The default Service Window, if none is specified for a particular Service Level, is 24 hours per day 365 days per year.
- 2.2 Provider will use appropriate tools and procedures to measure and report Service Level performance which will report at a level of detail sufficient to verify compliance with the Service Levels as set forth in this Appendix.
- 2.3 The Service Level Target for certain Service Levels is expressed as a percentage of events occurring during a Measurement Period. In such circumstances, if the number of events which occurred during a Measurement Period is less than or equal to 100, the following calculation will be applied to determine the number of events that Provider must successfully resolve to meet the relevant Service Level Target (and notwithstanding the percentage set out in the relevant Service Level description as the required level of performance):
- 2.3.1 the number of events which occurred during the Measurement Period will be multiplied by the relevant percentage; and
- 2.3.2 if the result of the multiplication referred to in Section 2.3.1 above is not a whole number, that result will be rounded down to the nearest whole number (or zero where the result is less than 1).
- 2.3.3 By way of example, if a Service Level description states that Provider must successfully resolve 95% of events within a specified period of time to meet the relevant Service Level:
- i) if the number of events is 100, Provider must successfully resolve 95 events to meet the relevant Service Level ( $100 \times 95\% = 95$  events);
  - ii) if the number of events is 99, Provider must successfully resolve 94 events to meet the relevant Service Level ( $99 \times 95\% = 94.05$  events which is rounded down to 94 events); and
  - iii) if the number of events is 9, Provider must successfully resolve 8 events ( $9 \times 95\% = 8.55$  events which is rounded down to 8 events).

---

## **3 Reporting**

- 3.1 Unless otherwise set out in an SOW, Provider will report performance against all Service Levels monthly in the Service Level Dashboard Report.
- 3.2 Unless otherwise set out in an SOW, Provider will provide the Service Level Dashboard Report within fifteen (15) Business Days after the beginning of the month following the end of each Measurement Period.
- 3.3 In the Service Level Dashboard Report, Provider will state reasons for any Service Level Default and corrective actions being performed to prevent recurrence, and will report any Service Credits accruing.
- 3.4 The Service Level Dashboard Report data and detailed supporting information will be Confidential Information of Provider.

---

## **4 Failure to Meet Service Levels**

- 4.1 If a Service Level Default occurs in any Measurement Period, Provider will:
- 4.1.1 Investigate, assemble and preserve pertinent information with respect to, and report on the causes of, the Incidents or other factors which led to the Service Level Default, including performing a Root Cause Analysis if Provider considers that it is warranted;
- 4.1.2 Promptly propose an appropriate, written corrective action plan for each Incident for which a Root Cause Analysis is conducted (unless a corrective action plan has already been implemented) and proceed to execute the action plan;

- 4.1.3 Advise Customer, as requested, of the status of remedial efforts being undertaken with respect to Incidents and Problems; and
- 4.1.4 Take appropriate preventive measures (where the measures are within the responsibility of Provider) so that in the reasonable opinion of Provider, the Incidents and Problem will not recur.
- 4.2 If a Service Level Default has occurred, and if Provider or Customer identifies a trend in Service Level performance which reasonably indicates that there will be a future Service Level Default, then Provider will perform a Root Cause Analysis of the trend, report to Customer on its findings and take any necessary steps indicated by the Root Cause Analysis to prevent an actual Service Level Default.
- 4.3 If there is dispute between the parties regarding achievement of Service Levels, the Escalation Process set out in Appendix 4 (Governance Model) will apply.

---

## **5 Service Credits**

- 5.1 If a Service Level Default occurs under an SOW, and that Service Level Default is not excused in accordance with Section 10 below, subject to any Earnback opportunity in accordance with Section 7 Provider must calculate the Service Credits that may be payable in respect of that Service Level Default in accordance with this Section 5.
- 5.2 Any Service Credits calculated in accordance with 5.1 above will be reported to Customer in the Service Level Dashboard Report. Subject to any reductions resulting from Section 5.3 below, the value of such Service Credits will be accrued by Provider for the duration of the Earnback Period which applies to such Service Credit.
- 5.3 In no event will the total amount of Service Credits calculated in respect of all Service Level Defaults occurring during any Measurement Period exceed the At Risk Amount. The At Risk Amount is 8% of the Charges applicable to the relevant SOW. By way of example, if the actual amount of all Service Credits calculated for accrual for Service Level Defaults occurring under that SOW for a Measurement Period is greater than 8% of the Charges applicable to that month under that SOW, then each of those Service Credits will be reduced in equal proportions such that the total amount accrued is equal to 8% of those Charges.
- 5.4 In the event of a Service Level Default, the Service Credit is calculated by multiplying the Service Credit Allocation for the associated missed Service Level by the At Risk Amount, by the Charges applicable to that month under that SOW.
- 5.5 If Provider misses more than one Service Level in the month, then the Service Credit will be accumulated but at no time shall the Service Credit for a month exceed the At Risk Amount.
- 5.6 Any Service Credit calculated in accordance with this Section 5 shall be the sole and exclusive remedy for the act or omission that led to the failure to meet the relevant Service Level.
- 5.7 If multiple Service Level Defaults occur during a Measurement Period as the result of a single event, Provider shall only be liable for Service Credits related to the Service Level with the highest Service Credit amount.

---

## **6 Allocation of Service Credit Percentages**

- 6.1 Customer will allocate Service Credit Allocations to the Service Levels, provided that at no time shall the sum of the Service Credit Allocations exceed 100%, nor shall the Service Credit Allocation to any individual Service Level exceed 20%.
- 6.2 Customer may provide written request to Provider increasing or decreasing the then-current Service Credit Allocation for one or more Service Levels.
- 6.3 The changes noted in Section 6.2 above may be made no more frequently than once every six (6) months, subject to the Change Control Process.

---

## **7 Earnback**

- 7.1 Provider shall have the opportunity to earn back Service Credits as set out in this Section 7.
- 7.2 Where a Service Credit has been accrued in accordance with Section 5.2 above, within fifteen (15) days after each Earnback Period, Provider shall provide a report to Customer that will detail, with respect to each Service Level for which there was a Service Level Default within the original Measurement Period, the performance average for the Earnback Period.
- 7.3 Where, after accruing a Service Credit for a Service Level Default, Provider achieves a performance average for that Service Level greater than or equal to the Service Level Target in effect for that Service Level during the relevant Earnback Period, Provider shall “earn back” such Service Credit and the related accrual shall be adjusted to zero (0).
- 7.4 At the end of the Earnback Period, where the Service Credit has not been earned back in accordance with Section 7.3 above, Provider must pay Customer the amount originally accrued in accordance with Section 5.2 above by way of a credit to the following monthly invoice.
- 7.5 If any Service Credit remains accrued in respect of an SOW on the expiration or termination of such SOW, the Earnback Period will be the period between the end of the Measurement Period and such expiration or termination, and Provider must, within thirty (30) days after such expiration or termination, pay Customer the amount of any accrued Service Credits which are not earned back.
- 7.6 If, during a Measurement Period, a Service Level is removed from the SOW, Provider shall earn back any Service Credits assessed during the preceding six (6) months for Service Level Defaults for that Service Level, provided that Provider's performance for the duration of the last-measured Measurement Period was greater than or equal to the Service Level Target in effect at the time such Service Level was deleted.

---

## **8 Key Performance Indicators**

- 8.1 Key Performance Indicators are measurements of Service against metrics that Provider will strive to achieve; however, no Service Credits apply if Provider does not achieve the relevant metric for any KPI as set out in an SOW.
- 8.2 If Provider fails to achieve a KPI, Provider will carry out reasonable corrective actions in order to meet the KPI, and the parties will discuss corrective actions as part of the governance process outlined in Appendix 4 (Governance Model).

---

## **9 New Service Levels**

- 9.1 Customer may provide written request to Provider for a new Service Level or KPI. Such request shall be considered through the Change Control Process.
- 9.2 Where Customer so requests a new Service Level or KPI, the parties will negotiate in good faith to agree on the Service Level Target or KPI metric, including where applicable having regard to:
  - i) the design specifications for the relevant Service;
  - ii) existing measurements for similar Service Levels; and
  - iii) industry standard measures
- 9.3 If Customer believes that any Service Level Targets or KPI metrics determined in accordance with Section 9.2 above are at a standard that is below the level required by Customer, Provider will prepare a plan detailing alternative solutions, related fees and timeframes to address the requested performance. If Customer wishes to implement any such alternative, Customer will authorize Provider to proceed with one of the proposed alternative solutions and will pay the associated fees. If Customer and Provider cannot, in good faith, resolve the matter then the Escalation Process in Appendix 4 (Governance Model) will apply.

- 9.4 New Service Levels and KPIs for which tracking and reporting can be achieved using existing toolsets, in their then-current configuration, will be added at no additional cost. Where new Service Levels require additional toolsets to be deployed, or require reconfiguration of existing toolsets, any cost associated with such additional toolsets or such reconfiguration shall be borne by Customer.

---

## 10 Excused Events

- 10.1 Provider shall not be responsible for the failure to meet any Service Level to the extent that any such failure is attributable to any of the following causes:
- 10.1.1 Force majeure event;
  - 10.1.2 Customer or Customer Representatives' acts or omissions;
  - 10.1.3 An event which is already the subject of Service Credits against another Service Level;
  - 10.1.4 Deficiencies or failures of assets purchased or used by Customer, with the exception of those Assets that are covered by the Service Levels as explicitly included in an SOW;
  - 10.1.5 Any action taken at the authorized request of the Customer or within an approved Change Window or scheduled maintenance window;
  - 10.1.6 Service or resource reductions requested or approved by Customer and agreed by the parties;
  - 10.1.7 Customer's failure to take corrective actions reasonably requested and identified by Provider in writing to Customer as essential to maintain Service Levels;
  - 10.1.8 Failures to meet Service Levels while operating under a business continuity or disaster recovery plan;
  - 10.1.9 Occurrences outside the In-Scope Environment;
  - 10.1.10 Infringements of third party proprietary rights;
  - 10.1.11 Failure to approve required Change Windows or maintenance windows;
  - 10.1.12 Customer's failure to approve a corrective action plan developed as a result of a previous Service Level Default; and
  - 10.1.13 In addition, with respect to Service Levels where the target is time-based, measurement time shall be suspended during periods when Provider is awaiting performance of functions by any party other than Provider that are necessary for Provider to complete the activities required by such Service Levels.

## Appendix 3 – Security Framework

---

### 1 Information Security Management Program

#### 1.1 Security Management ISO27002: 2005

1.1.1 Provider will maintain an information security management program aligned to the ISO27002:2005 framework, to maintain commercially reasonable administrative, organizational, technical, and physical measures to protect the security, integrity, confidentiality, and availability of Customer information.

#### 1.2 ISO27001:2005 Certification

1.2.1 The following business units, Provider Service Locations and activities are in scope of the ISMS, ISO27001:2005:

- i) Remote systems management
  - a) Ireland – Cork
  - b) India – Bangalore
- ii) Managed services – On-site and remote services
  - a) UK – Brentford, City and Customer Services Locations

---

### 2 Information Security Policies and Standards

#### 2.1 Provider Policies and Standards



2.1.1 Services and solutions will be designed, delivered and maintained in accordance with Provider policies and standards which are aligned to the ISO27002:2005 framework. This includes the following:

- i) Management sponsorship and direction;
- ii) Organization and governance of information security;
- iii) Asset management: inventory and classification of information assets;
- iv) Human resources security: security aspects for employees on-boarding, transferring, and off-boarding;
- v) Physical and environmental security: protection of the computer facilities;
- vi) Communications and operations management: management of technical security controls in systems and networks;
- vii) Access control: restriction of access rights to networks, systems, applications, functions and data;
- viii) Information systems acquisition, development and maintenance: building security into applications;
- ix) Information security incident management: anticipating and responding appropriately to information security breaches;
- x) Business continuity management: protecting, maintaining and recovering business-critical processes and systems; and
- xi) Compliance: ensuring conformance with information security policies and laws applicable to Provider.

---

### **3 Security Incidents**

3.1 Provider will implement and maintain a commercially reasonable and appropriate data security incident management program. In the event Provider becomes aware of a Security Incident, Provider will notify Customer of the Security Incident in accordance with Provider information security policies. In the event a Customer becomes aware of a Security Incident that may impact the Services, the Customer will immediately notify Provider of the Security Incident.

---

### **4 Service Industry Control Reporting**

4.1 Provider will conduct both SSAE 16 and ISAE3402 Type II audit attestations on an annual basis. The audit results, provided in a letter to the Provider management team, may be provided upon Customer request and are subject to when the findings become available to Provider.

---

### **5 Physical Review of Provider Information Security Policies**

5.1 Customer may, from time to time, but not more than once in any calendar year for itself or on behalf of its Affiliates, conduct a physical review of Provider's information policies relating to Provider's performance and this Agreement through its own Personnel or through agents, auditors or advisers and will ensure that such persons are bound by Section 9 of the Agreement and any other applicable provisions therein. All requests for audits shall be written and provided no less than ninety (90) Business Days prior to the commencement of the review. Provider will permit the review of selected samples of Provider's information security policies directly related to the Services during an onsite visit to a Provider executive briefing center ("EBC") during Provider standard business hours. Provider information security policies are classified as Provider Confidential Information.

## Appendix 4 – Governance

---

### 1 Overview

- 1.1 This Appendix 4 sets forth the governance model under which the parties will perform their respective roles and responsibilities under the Agreement.
- 1.2 The principal objective of this governance model is to:
  - 1.2.1 provide the guiding principles of the parties' working relationship; and
  - 1.2.2 assist both parties in managing their relationship in a manner consistent with achieving the underlying objectives of the parties.
- 1.3 Provider, based on the governance model described herein, will develop a governance plan within thirty (30) days of the effective date that defines Provider and Customer:
  - 1.3.1 interactions and boundaries;
  - 1.3.2 governance committee members, roles, and responsibilities (individuals and teams); and
  - 1.3.3 communication plan.
- 1.4 The governance plan will be reviewed no less frequently than once per calendar year. During such review updates will be made to reflect mutually agreed changes to the governance mechanisms, so as to provide flexibility and scalability.

---

### 2 Governance Model

- 2.1 The governance model shall reflect three (3) levels of engagement, as follows:
  - 2.1.1 executive level;
  - 2.1.2 management level; and
  - 2.1.3 delivery level.
- 2.2 Escalations will flow from the delivery level to the management level, and ultimately to the executive level.
- 2.3 Decisions will flow from the executive level to the management level, and ultimately to the delivery level.

---

### 3 Executive Level

- 3.1 The executive level of governance is the highest level in the governance model, responsible for:

- 3.1.1 establishing committees at all levels (executive level, management level, and delivery level) of governance that include representatives of both parties;
  - 3.1.2 organizational cooperation and communication of shared goals and obligations across parties;
  - 3.1.3 managing business decisions and priorities;
  - 3.1.4 escalation management as last point of resolution for disputes or issues;
  - 3.1.5 alignment of strategy and direction;
  - 3.1.6 confirming updates to the governance framework relationship on a periodic basis; and
  - 3.1.7 financial review of the engagement.
- 3.2 The executive level committee(s) will meet to review the performance of the overall Services being delivered under the Agreement and provide guidance to the management level committees in the following areas:
- 3.2.1 strategic objectives;
  - 3.2.2 major risks, issues and escalations;
  - 3.2.3 key service decisions including approval of changes and prioritization; and
  - 3.2.4 emerging Customer and Provider corporate objectives and developments.
- 3.3 Executive level committee meetings will be initiated by Provider within 3 (three) months of the Commencement Date, and thereafter will be held quarterly, or as otherwise agreed by the parties.
- 

#### **4 Management Level**

- 4.1 The management level is in the middle level of the parties' governance structure and includes representatives of both parties that participate in committee(s) responsible for:
- 4.1.1 management of the SOWs;
  - 4.1.2 delivery accomplishments;
  - 4.1.3 service performance;
  - 4.1.4 status of key initiatives and projects;
  - 4.1.5 managing and mitigating risks, issues, escalation and disputes;
  - 4.1.6 managing proposals relating to Changes to any SOW;
  - 4.1.7 providing strategic technical direction and prioritization of projects and Services;
  - 4.1.8 establishing policies, processes, and practices that support priorities; and
  - 4.1.9 maximizing technical investments and resource utilization.
- 4.2 The management level of governance committee(s) will meet to review the performance of each SOW being delivered and provide guidance to executive level and delivery level committees in the following areas:
- 4.2.1 program performance and prioritization;
  - 4.2.2 risks, issues, escalations, decisions and resolutions;
  - 4.2.3 contract and project change reports or requests;
  - 4.2.4 quality management;
  - 4.2.5 compliance;

- 4.2.6 communication management;
  - 4.2.7 delivery management; and
  - 4.2.8 evaluating operational readiness.
- 4.3 Management level committee(s) will meet to review the technical plan and solution of each SOW being delivered and provide guidance to executive level and delivery level committees in the following areas:
- 4.3.1 technical innovation;
  - 4.3.2 technical optimization;
  - 4.3.3 technical prioritization;
  - 4.3.4 technical roadmaps; and
  - 4.3.5 technical approvals.
- 4.4 Committee meetings will be initiated within 2 (two) weeks of the effective date of the Agreement and thereafter held monthly or at a frequency agreed by the parties and documented in the governance plan, as updated from time to time.
- 

## **5 Delivery Level**

- 5.1 The delivery level is in the lowest level of the parties' governance structure and includes representatives of both parties that participate in committee(s) responsible for:
- 5.1.1 Planning:
    - i) scope definition and clarification;
    - ii) project plan and schedule; and
    - iii) policies and procedures supporting the achievement of the objectives;
  - 5.1.2 Organizing:
    - i) establishing the team structure;
    - ii) implementing roles and responsibilities; and
    - iii) ensuring each party's compliance with the relevant obligations;
  - 5.1.3 Leading:
    - i) directing performance of the Services consistent with SOW;
    - ii) setting priorities and directions;
    - iii) coordinating activities across different organizational functions;
    - iv) assigning work;
    - v) ensuring quality; and
    - vi) managing risks, issues and escalations.
  - 5.1.4 Controlling:
    - i) tracking, measuring and checking progress against scope and objectives;
    - ii) status reporting and dashboards;
    - iii) evaluating delivery deviations and cause;
    - iv) taking corrective actions to resolve deviations to plan; and

- v) defining project baselines.
- 5.2 Delivery level committee(s) will meet to review each SOW being delivered and provide input to the management level committee(s) reporting and reviewing the following areas:
- 5.2.1 key decisions;
  - 5.2.2 action items;
  - 5.2.3 risks, issues and escalations;
  - 5.2.4 status reports and dashboard;
  - 5.2.5 policies, processes and practices;
  - 5.2.6 technical quality and compliance;
  - 5.2.7 technical performance;
  - 5.2.8 interoperability;
  - 5.2.9 operational readiness; and
  - 5.2.10 required coordination across different organizational functions.
- 5.3 Committee meetings will be initiated within 2 (two) weeks of the effective date of the Agreement and thereafter held at a frequency agreed by the parties and documented in the governance plan, as updated from time to time.

---

## **6 Escalation Process**

- 6.1 Subject to the terms of the Agreement, the parties shall comply with the following Escalation Process:
- 6.1.1 In the event that a dispute arises between the parties relating to the Agreement, the party claiming dispute shall deliver to the other party a notice containing the information regarding the dispute. Within ten (10) days of delivery of such notice, the parties shall escalate the dispute to the relevant delivery level committee in order to seek to resolve the dispute by discussion and/or negotiation.
  - 6.1.2 In the event that the parties cannot resolve the dispute in this initial period, the parties shall refer the dispute to the relevant management level committee, which shall meet within three (3) Business Days after a matter is referred to it and shall use reasonable endeavors and act in good faith to resolve the dispute within five (5) Business Days after the matter is referred to it.
  - 6.1.3 If the dispute cannot be resolved at the management level, the parties shall refer the dispute to the executive level. Executive representatives of each party shall meet within three (3) Business Days after the matter is referred and shall use reasonable endeavors to resolve the matter within five (5) Business Days after such referral.
  - 6.1.4 If the dispute cannot be resolved at the executive level, each party may exercise its rights under the Agreement. Notwithstanding anything contained herein, a dispute relating to either party's proprietary rights or Confidential Information shall not be subject to this section and Provider shall retain the right to pursue all rights and remedies in law and equity pursuant to the Agreement.

---

## **7 Changes to the Services**

- 7.1 General
- 7.1.1 The purpose of this Change Control Process is to provide the parties with a robust and manageable process which can be followed when proposing, reviewing, agreeing and/or implementing Changes to the scope of the Services, Service Levels and other areas supporting the business, but not related to IT operational Changes.

7.1.2 Any notification required to be given in writing by a party under this process may be given by email to the relevant representative of the other party. Each party must authorize a Change Order prior to its implementation or deployment.

## 7.2 Requesting Changes

7.2.1 Either party may, at any time, request a Change.

7.2.2 The parties shall hold discussions in respect of such request within 5 (five) Business Days of receipt (or such other period as may be agreed by the parties in writing), and shall attempt to reach agreement with regards to the proposed content of the request.

7.2.3 If such agreement cannot be reached, or if either party does not consent to the request, a Change Order shall not be prepared. The requesting party may escalate their request through the Escalation Process identified above.

## 7.3 Implementing Changes

7.3.1 Where the parties have reached in principle agreement to a Change, the requesting party shall within ten (10) Business Days prepare a draft Change Order in the form indicated in Appendix.

7.3.2 The receiving party shall review the draft Change Order and shall respond to the requesting party within 10 (ten) Business Days. The receiving party may request further details, information or costings in relation to any aspect of the draft Change Order, which the requesting party shall provide within 10 (ten) business days of such request, or as soon as reasonably practicable thereafter.

7.3.3 When the parties agree the format and content of the Change Order, both parties shall cause such Change Order to be signed by their authorized representatives.

7.3.4 Any discussions which may take place between Customer and Provider in connection with a draft Change Order prior to the signature of such Change Order shall be without prejudice to the rights of either party.

7.3.5 Both parties shall use reasonable endeavors to review proposed Change Orders promptly.

## Appendix 5 – Assets

---

### 1 Title to Provider Assets.

Title to all Provider Assets provided by Provider pursuant to this Agreement shall remain with Provider at all times until such time as Provider transfers title if mutually agreed to by the Parties. All Assets shall be and remain personal property notwithstanding the manner in which the Assets may be attached or affixed to realty. Customer shall have no right or interest in the Assets except as provided in the Agreement.

---

### 2 Treatment of Provider Assets.

Customer shall keep the Provider Assets (including Provider Software) free from any liens, attachments or third party claims. Additionally, Customer shall not move the Provider Assets from the Customer Service Location without prior written approval of Provider or remove or permit another to remove the original identification marks or move or use Provider Software on any equipment except as permitted in writing by Provider. Customer shall not remove any other Assets as needed by Provider to perform the Services.

---

### 3 Risk of Loss.

In the event that there are Assets at a Customer Service Location, Customer shall bear the entire risk of loss, theft, damage or destruction with respect to such Assets from any cause other than Provider's acts or omissions from the date of delivery of the Provider Assets to the site(s) until the Provider Assets are removed from the site(s). In the event Customer's acts or omissions result in any loss, theft, damage or destruction to the Provider Assets, Customer shall promptly repair or replace (at Provider's discretion) the Asset with an asset of the same manufacturer, model, capacity, configuration and condition, free and clear of any liens. Provider shall be relieved of its Services obligations to the extent any such loss, theft, damage or destruction to the Provider Assets impacts Provider's ability to provide such Services until such time as Customer replaces or repairs the Provider Assets. Upon replacement of any Asset, the replacement units shall be the property of Provider and, for purposes of this Section, shall be deemed to be the Asset which it replaced, and thereupon shall be subject to the terms of this Agreement.

---

### 4 Customer Insurance.

Customer shall obtain and maintain, at its own expense, Commercial General Liability insurance and insurance against all risk of loss or damage to the Assets. Such insurance shall be (i) initially in the amount equal to the replacement cost of such Assets; (ii) increased or decreased upon notice from Provider to reflect changes in the delivered capacity; and (iii) with such insurers having an A VIII or better BEST rating. The Commercial General Liability insurance policy shall name Provider as additional insured and the Property policy shall name Provider as loss payee thereof, as

Provider's interests may appear; and shall provide at least thirty (30) days' written notice of cancellation or non-renewal to Provider or its successors and assigns. Upon request, Customer shall provide to Provider a certificate of insurance as evidence of insurance coverage.

---

## **5 Tracking of Usage Levels.**

Provider shall monitor and/or audit the usage in order to calculate the applicable fees. Provider shall conduct such activity through the use of electronic means, remote access and/or on-site inspection by Provider Personnel in order to authenticate Customer as the user of the Services and verify the Customer's usage levels. Customer will take any actions required by Provider to permit such tracking of usage and provide all necessary equipment. If Provider is unable to monitor usage for any reason, Customer shall pay an amount for the affected Service period based on Customer's average usage during the previous three (3) months. Provider shall promptly notify Customer of an inability to electronically and or physically access the Assets, as applicable, and work cooperatively to reestablish access. Once access is reestablished, then Provider shall compute the unavailable metrics by calculating the capacity change between next successful measurement and the preceding successful measurement, plotting a straight distribution over the number of missing monitoring events, and will provide a corrected invoice for the affected Service Period in accordance with that calculation.

---

## **6 Technology Refresh.**

Provider is responsible for the implementation of technology refresh in the ordinary course of the technology lifecycle as detailed in each SOW. Notwithstanding the foregoing, (i) Provider shall comply with any direction by Customer not to implement technology or refresh Products, provided that in such an event, Provider retains the right to modify the applicable fees and (ii) Provider shall have no obligation to refresh Provider Assets within the twelve (12) months prior to expiration of the Term. On the occasion that (i) or (ii) above occurs, Provider shall have no liability with respect to the Services provided under the applicable SOW where the root cause of such failure is determined to be lack of refresh or implementation of new technology, including without limitation, failure to achieve any Service Levels.

---

## **7 Termination or Expiry.**

### **7.1 Purchase of Assets.**

Upon the cancellation, expiration or termination of the Agreement or an SOW, Provider will advise Customer which Provider Assets are available for purchase. Customer has the option to purchase such Provider Assets according to the provisions herein. Customer shall notify Provider in writing of those Provider Assets that it wishes to purchase, such notice to be received no less than thirty (30) days prior to the termination or expiry of the Agreement or applicable SOW. In the event Customer does not exercise the option to purchase an Asset and with respect to Provider's Assets which have not been made available for purchase, Provider and Customer shall promptly develop a plan for (i) migrating Customer's data from Provider's Assets; and (ii) enabling Provider to promptly recover possession of such Asset or any part thereof in accordance with 7.2 below. Where Customer elects to purchase any Asset, such Assets shall be purchased for a Residual Value, which shall be calculated for each individual asset according to the following approach:

$$\text{Residual Value} = \text{List Value} \times (1 - \text{Contract Discount}) \times ((\text{Asset Life} - \text{Deployed Months}) / \text{Asset Life})$$

In addition to the Residual Value, Customer shall pay any transfer fees or taxes associated with the transfer of ownership of the Assets. For the avoidance of doubt, title to any Assets transferred pursuant to these provisions shall be subject to Customer payment in full of the applicable fees, and any other fees associated with transfer; and the fees calculated herein shall include prepaid maintenance (hardware or software) solely to the extent advised by Provider. Customer shall be responsible for procuring maintenance post transfer. Any Assets purchased under this Section shall be purchased "as is". Provider shall have no further liability with regards to the Assets, with the exception of any liability that is created through the separate purchase of ongoing support and maintenance for the Assets under a separate agreement.

### **7.2 Migration and Ongoing fees.**



In the event that Provider Assets are included in one or more SOWs and located at a Customer Service Location, on or before the end of the termination assistance period, Customer shall permanently remove all data from the Provider Assets, at Customer's sole cost and expense. Customer shall be solely liable for (a) any and all damages to the Provider Assets and (b) any loss or damage to Customer's data, in each case arising out of or relating to the removal of such data. At the conclusion of the termination assistance period, Provider may terminate Customer's access to the Services and/or immediately enter upon any Customer Service Locations where any of the Provider Assets are located, free from all claims, and recover the Provider Assets. Customer shall be responsible for the payment of the actual documented costs and reasonable attorneys' fees incurred by Provider in retaking possession of the Provider Assets and/or seeking to recover amounts due.



## **TERMS AND CONDITIONS FOR PEGASYSTEMS PRODUCTS AND SERVICES**

### **MASTER SOFTWARE LICENSE, MAINTENANCE & PROFESSIONAL SERVICES AGREEMENT**

This Agreement (“Agreement”) describes the terms and conditions that will apply to licenses for Pegasystems’ products that Customer purchases from time to time, and maintenance services and professional services and training from Pegasystems relating to those licensed products. This Agreement consists of specific terms and conditions relating to Licenses, Maintenance and Professional Services and Training, general terms and conditions relating to the relationship between the parties, the defined terms specified on Exhibit A, and the terms and conditions in any License Schedule.

Pegasystems’ products include the Pega Platform for CRM and BPM applications, Artificial Intelligence for adaptive real-time decisioning, Robotic Automation for assisting workforces, and strategic applications and components. Pega Platform products are composed of Pegasystems’ RuleSets to develop specific Customer Applications. Customer Applications may be deployed on the Pega Cloud, a Customer Managed Cloud, or a partner-managed cloud, each as described in a Schedule to this Agreement. Professional services and training may be obtained under a Statement of Work to this Agreement. Definitions are stated on Exhibit A.

#### **Subscription Services and License Terms**

1. Subscription Services: Software License
  - (a) If designated in an applicable Schedule, Pegasystems will provide Customer with the Subscription Services and/or Pega Cloud Collaboration Services in accordance with the Documentation to develop, test and/or deploy Customer Applications within the Scope of Use. Customer will be responsible for any Customer managed or installed third-party products that are not included as part of the Subscription Services.
  - (b) If designated in an applicable Schedule, Pegasystems will grant Customer a non-transferable, non-exclusive license to install the Software in a Customer Managed Cloud in accordance with the Documentation to develop, test and/or deploy Customer Applications within the Scope of Use. Software licensed for use in a Customer Managed Cloud will not include the Subscription Services.
  - (c) Customer is responsible for the performance of any Customer Application(s) and for configuring Guardrail Compliant Customer Application(s) in the Pega Cloud.
  - (d) Customer will receive support, upgrades, and updates during the Term in accordance with the terms of the applicable Schedule and the Customer Support Handbook.
  - (e) Pegasystems will email to Customer a URL to allow Customer access to the Software and/or Subscription Services. The Software and/or Subscription Services will be accepted upon delivery (“**Acceptance**”). This Acceptance is not dependent on any remaining services, conditions or contingencies, and there are no other written or verbal agreements with respect to Acceptance.
  - (f) Pegasystems may host, copy, use, transmit and display Customer’s data, Customer Applications, and any third-party products, only as necessary to provide the Subscription Services. Customer agrees to allow Pegasystems to use anonymized information about Customer’s use of the Subscription Services and Software to improve the Pega services generally. Pegasystems will not acquire any title or interest from Customer in or to Customer’s data or third-party products.
2. Restrictions.
  - (a) Customer’s use of the Subscription Services and/or Software will comply with the terms of this Agreement. Customer’s use of the Subscription Services will comply with the Documentation, Customer Data Rights and Responsibilities, and Acceptable Use Policy. Customer agrees not to sell, resell, rent, outsource, timeshare, lease or sublicense the Subscription Services and/or Software to any third party or otherwise use it except as permitted under this Agreement and the applicable Schedule. Customer will not use shared User IDs to avoid or reduce the counting of individuals that use the Subscription Services and/or Software.
  - (b) Customer’s use of the Subscription Services and/or Software will be in object code and/or RuleSet form. Unless specifically authorized by law, Customer may not reverse engineer, decompile, disassemble or otherwise attempt to determine source code or protocols from the Subscription Services and/or Software.
  - (c) Pegasystems retains all right, title and interest to the Subscription Services, Software and Background Materials. The Software will contain Pegasystems’ copyright notice and Customer will reproduce such notice in any permitted copy made by Customer.



### Professional Services Terms

3. Performance of Professional Services; Deliverables.
  - (a) Pegasystems may provide Professional Services to Customer under a Statement of Work.
  - (b) All Deliverables that Pegasystems creates when providing Professional Services for Customer under this Agreement will be a “work made for hire” and will become, effective upon payment by Customer in full, the exclusive property of Customer. Customer will also retain all right, title and interest in any new RuleSets that Customer develops for itself using the Software. So long as Pegasystems has not used any Customer Confidential Information, Customer agrees not to challenge or make claims against Pegasystems’ ability to provide its products and services to other customers.
  - (c) Pegasystems may use its Background Materials when providing Professional Services to the Customer. Background Materials are the property of Pegasystems, and if Pegasystems incorporates any Background Materials in a Deliverable that is provided to Customer under a Statement of Work, Customer will receive a non-exclusive, non-transferable, fully paid-up license to use those Background Materials solely in connection with the Deliverables in which they were incorporated under the terms of the applicable Schedule.

### General Terms and Conditions

4. Reserved.
5. Reserved.
6. Representations and Warranties.
  - (a) Each party represents and warrants the following: (i) entering into and carrying out the terms and conditions of this Agreement will not violate any obligation binding upon it; (ii) each party will comply with all applicable laws in connection with its performance under this Agreement; and (iii) the executing persons have the authority to bind their respective parties.
  - (b) Pegasystems warrants that (i) the Subscription Services and/or Software will operate substantially in accordance with its Documentation for a period of 90 days from initial delivery, (ii) no disruptive or corrupting software that would damage, disable or compromise the security of a Customer Application will be intentionally or knowingly introduced into the Subscription Services and/or Software by Pegasystems or its employees, and (iii) all Professional Services provided under this Agreement will be performed in a good and workmanlike manner, consistent with applicable industry standards. Pegasystems will, at its election, promptly repair the Software or Subscription Services to resolve any failure of the warranties described in (i) and (ii) above, which can be replicated or verified, or replace the Software or Subscription Services with alternative software that provides substantially the same functionality. These remedies will be Customer’s exclusive remedy for any failures of these warranties. To invoke these remedies, Customer must provide written notice to Pegasystems within the warranty period, expressly outlining the nature of the alleged failure or breach.
  - (c) The foregoing warranties will be void to the extent that any failure of such warranties is caused by (i) anyone other than a Pegasystems employee modifying the Subscription Services or Software (unless Pegasystems authorizes the specific change in writing), or (ii) non-Pegasystems’ service, software, or hardware, or (iii) non-Guardrail Compliant Customer Applications.
  - (d) EXCEPT AS EXPRESSLY STATED IN THIS SECTION 6, PEGASYSTEMS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT.
7. Confidentiality.
  - (a) “**Confidential Information**” means all non-public information provided by or on behalf of a party to the other party unique to the disclosing party’s business, including but not limited to Subscription Services, Software, and Documentation.
  - (b) Each party agrees that any Confidential Information is the exclusive proprietary property of the disclosing party or its licensors and may include trade secrets and other highly confidential information.
  - (c) Each party agrees to receive and hold any Confidential Information supplied by the other party in confidence



and agrees:

- (i) not to disclose or publish any such Confidential Information to third parties;
  - (ii) not to use any such Confidential Information except for those purposes specifically authorized by the disclosing party;
  - (iii) to disclose such Confidential Information only to those of its officers, directors, agents and employees who have a need to know, have been advised of the confidential nature of the Confidential Information, and who are under obligations of confidentiality to the receiving party; and
  - (iv) to follow the other party's reasonable on-site security procedures.
- (d) The above confidentiality provisions will not apply to information that:
- (i) is in the public domain at the time of its disclosure;
  - (ii) is disclosed to a third party who is under no obligation to maintain the confidentiality of the information with the prior written consent of the disclosing party;
  - (iii) becomes known to the receiving party from a source other than the disclosing party, provided such source is legally entitled to have and disclose the information; or
  - (iv) is independently developed by a receiving party without use of the Confidential Information of the disclosing party, as demonstrated by written records of such receiving party.
- (e) In the event that a receiving party is required by a court of law or by a governmental, regulatory or administrative agency, body or tribunal to disclose any of the Confidential Information of a disclosing party, the receiving party shall (i) provide the disclosing party with prompt prior written notice of such requirement so that the disclosing party may seek appropriate relief to prevent or limit such disclosure, and (ii) furnish only that portion of the Confidential Information which is legally required to be furnished or disclosed.
- (f) If, in connection with the Subscription Services and/or Software, Customer communicates suggestions for improvements to the Subscription Services and/or Software, Customer assigns to Pegasystems all of its right, title and interest (including all intellectual property rights) in such suggestions for improvements and Pegasystems will own all right, title, and interest in and to the same and shall be entitled use the same without restriction.

8. Indemnification.

- (a) Pegasystems will indemnify and defend Customer against any third-party claim that the Subscription Services, Software, or a Deliverable infringe upon a United States, Australian, Canadian or European Union trademark, copyright, trade secret or patent ("IPR"). If the Subscription Services, Software, or a Deliverable is found to be infringing or if Pegasystems deems it advisable as the result of a claim or threatened claim, Pegasystems will, in its reasonable discretion:
- (i) procure for Customer the right to continue using the Subscription Services, Software, or applicable Deliverable;
  - (ii) replace or modify the Subscription Services, Software or applicable Deliverable so that it becomes non-infringing; or
  - (iii) if Pegasystems cannot reasonably do either of the foregoing in its discretion, terminate the Schedule to which the IPR infringement claim relates.
- These remedies will be Customer's sole remedy for any IPR infringement claim.
- (b) Pegasystems will not indemnify Customer when the alleged infringement results from (i) content provided by Customer or developed for Customer as a Deliverable pursuant to written specifications or instructions provided by Customer; (ii) modifications made to the Subscription Services, Software, or applicable Deliverable by Customer or a third party; or (iii) any Customer Application (excluding unmodified Pegasystems provided RuleSets) or any other RuleSets created by Customer or a third party.
- (c) Pegasystems shall indemnify and defend Customer against any third-party claim to the extent that it is attributable to bodily injury or to death of any person or to damage to or destruction of any property, resulting from the willful or grossly negligent acts of Pegasystems, its agents, or employees.
- (d) Customer will indemnify and defend Pegasystems from and against any third-party claim that (i) arises from any use of the Software by Customer that is not in compliance with the terms of this Agreement or the applicable Schedule (other than an IPR claim that is subject to indemnification by Pegasystems pursuant to clause (a) above), or (ii) alleges that any of the Customer Applications (excluding unmodified Pegasystems provided RuleSets) or any Customer RuleSets infringe or misappropriate any third-party intellectual property rights. During the term of this Agreement and for three years thereafter, Customer will not assert against Pegasystems or its affiliates any patent infringement claim relating to its use of the Software or Subscription Services.
- (e) In asserting any claim for indemnification, the relevant party must provide prompt written notice describing the



claim and cooperate fully with the indemnifying party. The indemnifying party will be entitled to control any proceedings or litigation for which it is indemnifying the other party, except that the indemnifying party will not, without the other party's prior written consent (not to be unreasonably withheld), enter into any settlement that would require the other party to take any action, or refrain from taking any action, other than permitting the indemnifying party to pay money damages on its behalf.

9. Limitation of Liability. Each party will have unlimited liability to the other party for the following types of actual, direct damages arising under, or related to, this Agreement:

- (a) damages, and related reasonable legal costs and attorneys' fees, for which the other party has agreed to provide indemnification under Section 8 of this Agreement; or
- (b) damages resulting from a breach of a party's confidentiality obligations under Section 7 of this Agreement or from the infringement or misappropriation of the other party's intellectual property rights.

Each party's liability for all other damages arising under, or related to, this Agreement (regardless of the type of damages, and whether for breach of contract, breach of warranty, tort or otherwise) will be limited to the amount of fees received by Pegasystems from Customer in connection with the Schedule(s) under which such damages arose, or to which such damages relate (except any claim by Pegasystems for payments owed by Customer will be limited to the amount owed plus any additional amounts owed for use that exceeds the Scope of Use). However, Pegasystems' liability for any damages resulting from a material, uncured breach of Pegasystems' Data Security Obligations under this Agreement shall be limited to two times the amount of fees received by Pegasystems from Customer in connection with the Schedule(s) under which such damages arose, or to which such damages relate.

10. Reserved.

11. Insurance. During the Term of any applicable Schedule, Pegasystems will maintain insurance from a company rated at least A- by A.M. Best's Rating Service or equivalent with limits no less than those set forth in the Certificate of Insurance that Customer may obtain directly from:

<https://online.marsh.com/marshconnectpublic/marsh2/public/moi?client=D133>

12. Additional Terms and Conditions.

- (a) Cooperation. In the event of any dispute, which cannot be readily resolved within 30 days, the parties will each escalate the matter to senior management who will meet in person or by telephone within 15 days of receipt of notice of the dispute, to attempt to resolve the open issues.
- (b) Assignment or Delegation. Neither party may assign or delegate any rights or obligations under this Agreement or any Schedule without the other party's prior written consent, except that, subject to Section 12(c), either party may assign the entirety of its rights and obligations under this Agreement (i) to its parent company or an Affiliate, or (ii) in connection with a merger or sale of a business unit or majority stock ownership provided that the successor party assumes the rights and obligations in writing and has adequate resources to meet its obligations and Customer notifies Pegasystems in writing prior to the assignment. Customer will not assign or delegate any rights or obligations under this Agreement or any Schedule to a Pegasystems competitor. Any assignment is subject to the terms and conditions of this Agreement.
- (c) Customer Combinations. In the event that Customer should merge with, acquire, or be acquired by another entity (collectively, a "**Combination**"), the resulting combined entity may only use the Subscription Services and the Software within the scope of the Customer's operations at the time immediately prior to the Combination. In addition, the parties will negotiate in good faith a proportionate adjustment to the scope of use and the fees due under the applicable Schedule as a result of the Combination.
- (d) Non-Solicitation. Neither party will hire or contract with, either as an employee or an independent contractor (either directly or through a third party), any Covered Personnel of the other party. The term "Covered Personnel" of a party will mean that party's employees or any contractors retained by that party who are professional services personnel or who were involved in the performance of this Agreement within the preceding six-month period, or any person who would have been considered Covered Personnel but for having terminated employment or contractual relationship within the past six months. Breach of this Section 12(d) will constitute a material breach of this Agreement.
- (e) Export Compliance. The export and re-export of the Software and any Pegasystems technology is subject to export controls under the laws and regulations of the United States, including but not limited to the Export Administration Regulations, 15 C.F.R. Parts 730-774, and the Foreign Assets Control Regulations, 31 C.F.R. Parts 500-598. The export and re-export of the Software and any Pegasystems technology may also be subject





to export and import controls under the laws and regulations of other countries. Customer agrees, at all times, to comply fully with these controls, laws and regulations. Customer also agrees not to export, re-export, transport or otherwise make available the Software and any Pegasystems technology to any party, country or territory that is the target of United States sanctions, including Cuba, Iran, Syria, North Korea, and the Crimea region.

- (f) U.S. Government Contracts. *This subsection applies when any Software is acquired directly or indirectly by or on behalf of the United States Government:* The Software is a commercial product, licensed on the open market; developed entirely at private expense; and without the use of any U.S. Government funds. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19. Use, duplication and disclosure by DOD agencies is subject solely to the terms of this Agreement as stated in DFARS 227.7202.
- (g) Anti-Corruption. Pegasystems and Customer each represent and warrant to the other: (i) that it is aware of all anti-corruption legislation that applies to this Agreement and in particular the US Foreign Corrupt Practices Act 1977 and the U.K. Bribery Act 2010; (ii) it has implemented rules and procedures that enable it to comply with this legislation and adapt to any future amendments thereto; (iii) it has implemented appropriate rules, systems, procedures and controls for preventing the commission of Corrupt Acts, either by itself or its staff, and for ensuring that any evidence or suspicion of the commission of a Corrupt Act will be thoroughly investigated and unless prohibited by confidentiality or law, reported to the other party; (iv) its records relating to its business, including accounting documents, are maintained and kept so as to ensure their accuracy and integrity; and (v) it has not made or offered or received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of the other party's employees or agents in connection with this Agreement (reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction). If a party learns of any violation of the above restriction, it will use reasonable efforts to promptly notify the other party at the address for notices above.
- (h) Reserved.
- (i) Cooperation; Usage Validation. Pegasystems and Customer agree that each will execute and deliver documents, including confirmations to Pegasystems auditors, and take such other actions as may reasonably be requested to effect the transactions contemplated by this Agreement. Pegasystems reserves the right to validate Customer's usage of the Software and/or Subscription Services and its compliance under this Agreement. Customer will provide usage logs generated by the Software in connection with this usage validation. Upon request and not more than once annually, deliver to Customer (i) the current SSAE 16 SOC II Type 2 report, (ii) the current HIPAA compliance opinion letter, (iii) the current PCI-DSS Attestation of Compliance, (iv) the current penetration testing report, (v) an executive summary of Pegasystems' Written Information Security Program and (vi) executive summaries of the security, data backup, and monitoring events for the Customer's Environment(s) that are currently available.
- (j) Force Majeure. Neither party will be responsible for performance delays caused by circumstances outside its reasonable control.
- (k) No Waiver. Neither a failure of a party to exercise any power or right under this Agreement, nor a custom or practice of the parties with regard to the terms or performance under this Agreement, will constitute a waiver of the rights of such party to demand full compliance with the terms of the Agreement.
- (l) Counterparts. This Agreement may be signed in counterparts, including facsimile or PDF counterparts or electronic signatures, each of which will be a legally binding method of execution of the Agreement.
- (m) Entire Understanding. This Agreement and its Schedules constitute the entire understanding of the parties with respect to the Software and supersedes all previous agreements, statements and understandings from or between the parties regarding the subject matter of this Agreement. This Agreement also supersedes any conflicting language contained in any applicable past or future purchase order regarding the subject matter of this Agreement. In the event of any conflict between the terms of this Agreement and the terms of any Schedule, the terms of the applicable Schedule will control. This Agreement will not be modified except in a writing signed by an authorized representative of each party.
- (n) Enforceability. If any portion of this Agreement is declared by a court of competent jurisdiction to be overbroad or unenforceable, the remainder of this Agreement will be valid and enforceable to the fullest extent permitted.



## EXHIBIT A

### DEFINITIONS

- “Acceptable Use Policy”** means the then current policy as published from time to time at [www.pega.com/cloud-aup](http://www.pega.com/cloud-aup).
- “Affiliates”** are those entities that control, are controlled by, or are under common control with a party to the Agreement. Affiliates may be entitled, subject to the terms of this Agreement and the applicable Schedule, to use the Subscription Services, Software, or purchase maintenance services or Professional Services. For any Schedule to which an Affiliate is a party, the Affiliate will be additionally considered the Customer for purposes of the Agreement and such Schedule.
- “Background Materials”** means processes, methods, software (including but not limited to the Software), related documentation, designs and know-how which Pegasystems creates independently of the services for Customer. Background Materials also include all tangible and intangible materials created by Pegasystems that generally apply to other Pegasystems customers, products or services and which do not include any Customer Confidential Information.
- “Cloud Data Storage”** means the storage of business data and rules data in the Pegasystems database that is available for the Production Environment only.
- “Cloud File Storage”** means the storage of files associated with features such as archive/purge, large attachment handling and file transfer services that is available across all Environments.
- “Connector”** means an integration facility that permits the Software to call applications for data or processing.
- “Corrupt Act”** means any act of seeking, authorizing, offering, promising or granting a financial or other benefit (including a payment, loan, gift or transfer of anything of value) for the purpose of inducing a private person or public official to perform his or her duties dishonestly or in breach of his or her professional, legal or contractual obligations and/or to obtain or retain business for Pegasystems and or Customer in an undue or dishonest manner.
- “Customer Application”** means a unique collection of rules and processes as part of one or more new RuleSets that are created using the Software and that provide specific business function for the Customer.
- “Customer Data”** means any information received by or on behalf of Customer from its end customers or any personally identifiable information about Customer’s employees or agents that is stored, transferred, or processed by the Subscription Services.
- “Customer Data Rights and Responsibilities”** means the additional rights and obligations related to Customer data as published at: <https://community.pega.com/knowledgebase/articles/customer-data-rights-and-responsibilities>
- “Customer Managed Cloud”** means use of the Software in Customer or third party owned and controlled environments that are run and managed within private clouds or on infrastructure-as-a-service (IaaS) offerings delivered by third party providers.
- “Customer Support Handbook”** means the terms for Pegasystems’ provided support, upgrades, and updates located at: <https://community.pega.com/knowledgebase/documents/support-pega>, as may be periodically updated.
- “Data Security Obligations”** means Pegasystems’ obligations regarding the security of Customer Data available at: <https://community.pega.com/knowledgebase/articles/pega-cloud-security-standards>
- “Deliverable”** means RuleSets, documents and other tangible work product that are produced by Pegasystems for Customer during the course of the performance of Professional Services under a Statement of Work, excluding any Background Materials.
- “Documentation”** means, as applicable, the Subscription Documentation or Software Documentation.
- “Environment”** means one of the following Pega Cloud deployments provided by Pegasystems:
- **“Standard Sandbox”** means a service that is intended to be used for development, functional/unit testing, UAT testing of Customer Applications and training. A Standard Sandbox is scaled to support up to 15 developers/users with a storage limit of 50GB of Cloud Data Storage.
  - **“Large Sandbox”** means a service that is intended to support development, functional/unit testing, UAT testing, pre-production, staging, and/or training of the Customer Applications. A Large Sandbox is scaled to support up to 45 developers/users with a storage limit of 100GB of Cloud Data Storage.
  - **“Production Environment”** means a service that is designed, built and scaled to accommodate Customer Applications to process live and/or real-time data in connection with Customer’s ongoing business operations and is deployed within a single geographic region. The Production Environment is scaled to support up to the licensed metrics defined in the Schedule.
  - **“Production Mirror Sandbox”** means a replica of the scaled Production Environment that can be used for



staging, scaled benchmark testing, and/or load performance testing or as defined in the applicable Schedule.

**“Guardrail Compliant”** means a Customer Application with no severe warnings flagged by the Software and with a guardrail weighted score generated by the Software of ninety (90) or above as specified in the Subscription Documentation.

**“Pega Cloud”** means a Pegasystems’ managed, single-tenant, virtual private cloud (VPC) deployment of the Customer Application.

**“Pega Cloud Collaboration Services”** means multi-tenant, cloud hosting services for Pega Chat and Pega Co-Browse.

**“Pega Cloud HIPAA Edition”** means that the Customer’s VPC will be serviced and deployed with HIPAA-eligible controls and infrastructure. The Pega Cloud HIPAA Edition supports the Customer in deploying a HIPAA-compliant Customer Application to store and process PHI within their Production Environment. Under the Pega Cloud shared responsibility and security model, the Customer is responsible for ensuring that the Customer Application adheres to all HIPAA controls.

**“Professional Services”** means professional services provided by Pegasystems pursuant to a Statement of Work for consulting, installation support, and access to training courses.

**“RuleSet”** is a named collection of configuration records created using the Software. For Pegasystems’ provided RuleSets, the RuleSet names usually begin with “Pega” or the “&,” “@” or “)” symbol.

**“Scope of Use”** means the purpose, metric and volume of use for the Subscription Services and the Software, in each case, as specified in the applicable Schedule.

**“Service”** means an integration facility that permits applications to call the Software for data or processing.

**“Schedule”** or **“Statement of Work”** means, respectively, an agreement signed by both parties for Customer to receive Subscription Services, Software, or purchase professional services from Pegasystems. Schedules and Statement of Works are referred to collectively as **“Schedules”**. Each Schedule will be non-cancelable and non-refundable, except to the extent expressly provided in this Agreement or such Schedule or under applicable law.

**“Software”** means the software listed in the applicable Schedule, including any enhancements, updates, upgrades, modifications or other releases provided to Customer. Software may be managed by Pegasystems as part of the Subscription Services or deployed in a Customer Managed Cloud pursuant to the applicable Schedule. The Software includes Pegasystems’ provided RuleSets.

**“Software Documentation”** consists of user manuals for the Software, which are provided to Customer in electronic form at the time of delivery of the Software.

**“Subscription Documentation”** means the service catalog, product help files, operating guides, support services, service level agreement and security policies associated with the Pega Cloud as published from time to time on Pegasystems’ web site at <https://community.pega.com/knowledgebase/pega-cloud>.

**“Subscription Services”** means the Pegasystems Software which is made available to Customer for use on the Pega Cloud within the Scope of Use, including any enhancements, updates, upgrades, modifications, releases, Environments, data storage, or other services pursuant to an applicable Schedule.

**“Term”** is as defined in the applicable Schedule.

**“User”** is a person who uses the Software in a particular month.

1. A **“Sporadic User”** is a person that uses the Software less than 10 hourly periods in a calendar month.
2. An **“Occasional User”** is a person that uses the Software during between 10 and 50 hourly periods in a calendar month.
3. Any person other than a Sporadic User or Occasional User that uses the Software in a calendar month, or that has the privilege to modify rules or processes, is a **“Regular User”**.

Regular Users, Occasional Users and Sporadic Users will be the unit of measurement for work done by customer staff. The number of Regular Users, Occasional Users and Sporadic Users will be measured each calendar month based on their actual usage of the Software in that month. The Software tracks only actual use, so a person who has a User ID but does not use the Software in a month will not be counted as a User for that month. Also, for the avoidance of doubt, merely being “logged in” is not counted as actual use during inactive hours.

**NEW SUBSCRIPTION SERVICES CLIENTS:** To access the Subscription Documentation URLs, first create an account by clicking this URL or pasting it into your browser: <https://accounts.pega.com/register>





## EXHIBIT A-1

### PEGA DECISIONING DEFINITIONS

For the purposes of the Agreement and any Schedule where Customer is licensed for Pegasystems' decisioning Software, such as Pega Marketing or Customer Decision Hub, the following definitions will apply:

- "Batch/Bulk Decisions"** means a unit of work (measured in blocks of 500,000 records per 4-hour segment) to reach a judgment (for example, determining the best offer to include in an email campaign to be sent to a segment of customers). The processing time is counted from the time the decision batch process starts to the time it takes to complete processing, excluding the time to pre-process data before the batch run and the time to post process the output records and send/ship them to a fulfillment system. All batch/bulk processing must be configured by the customer to complete in a time window under 4 hours.
- "Cloud Data Storage"** means the storage of business data and rules data in any Pega-managed database. For the Pega Marketing and/or Pega Customer Decision Hub applications this is the storage location for Interaction History or the Pega Customer Movie store.
- "Cloud File Storage"** means the storage of files associated with features such as archive/purge, large attachment handling and file transfer services.
- "Decision Data Storage"** means the storage used for the Pega Marketing and/or Pega Customer Decision Hub applications for recoding decisions that are leveraged through the Adaptive Decision Manager (ADM) module.
- "Real-time Decision"** means a unit of work processed to reach a judgment (for example, determining the top five recommended offers for a customer/prospect). Each unit of work processed is known as a "decision" and the number of decisions that can be handled is measured in decisions per second ("**DPS**"). A unit of work must be configured by the customer to complete in a time window under 200 milliseconds. The time window is counted from start of the service call to when the service call completes, excluding the time for the called system to receive the start request and the time to return the results to the calling system.
- "Streaming Events"** is defined as ingesting and buffering data records, performing pattern detection, and writing or updating one summary record per event. Each data record is known as an "event" and the number of events that can be handled is measured in events per second ("**EPS**"). An event must be configured by the customer to complete in a time window under 0.4 milliseconds. The time window is counted from start of the ingesting of the data records to the writing of the summary record, excluding the time for the called system to receive the start request and the time to return the results to a calling system.