MetricStream , Confidential

METRICSTREAM

CLOUD SERVICES AGREEMENT

This CLOUD SERVICES AGREEMENT (the “Agreement”) is effective as of January 31, 2020

(“Effective Date”) and is entered into by and between MetricStream, Inc., a Delaware corporation with its

principal place of business at 2479 East Bayshore Rd, Suite 260, Palo Alto, California 94303

(“MetricStream” or “Company”), and State Street Bank and Trust Company, A Massachusetts trust

company whose principal place of business is Once Lincoln Street, Boston, MA 02111 (‘State Street” or

“Customer”) (each a “Party” and collectively the “Parties”) as of the “Agreement Effective Date” (both as

defined below):

State Street Bank and Trust Company

One Lincoln Street

Boston, Massachusetts 02111-2900

with notices to be delivered to:

Attention: General Counsel

With Copy to: Chief Procurement Officer

Annual subscription terms set forth in Section 3 of Exhibit

“Term” : ,

A, MetricStream Terms and Conditions.

Metmesiream | Pens \_~“ane Attached hereto as Exhibit A

Conditions

Service Levels Attached hereto as Exhibit B,

| “Acceptable Use Policy” Attached hereto as Exhibit C

“Security Schedule” Attached as Exhibit D

| “Data Privacy Addendum” | Attached as Exhibit E

“List of Subcontractors” | Attached as Exhibit F

“Open Source Component” | Attached as Exhibit G -

“Human Trafficking” Attached as Exhibit H

“List of 3 Party Products” Attached as Exhibit I as applicable.

Order Form - | AttachedasExhibit} = = = |

Audit Methodology Attached as Exhibit K

"Master Services Agreement Attached as Exhibit L

Information Classification: Limited Access

GPS# 180319755629459 4

MetricStream Confidential

Agreement Terms. This Agreement shall consist of the MetricStream Terms and Conditions, Service

Level Agreement, Acceptable Use Policy, Security Schedule, Data Privacy Addendum, Human

Trafficking Exhibit, the Non-Disclosure Agreement and all applicable Purchase Orders, MetricStream

Order Forms and all other attachments, addenda, and amendments which reference this Agreement and

are signed by both Parties. This Agreement constitute the entire agreement between the Parties with

respect to its subject matter, and supersedes all prior or contemporaneous agreements, understandings,

representations, warranties, promises, and discussions, whether written or oral, between the Parties

regarding the same. In the event of a conflict between the terms of this Agreement and an applicable

MetricStream Order Form, this Agreement shall govern unless specifically provided for otherwise in the

MetricStream Order Form.

IN WITNESS WHEREOF, the Parties have executed this Agreement through their authorized

representatives.

STATE STREET BANK AND TRUST METRICSTREAM, INC.

COMP

By: / By: all

Name: c L Fic S Name: SEES IC Qa 4 Ot

Title: Chiat re gal OFFICE

Date: i/o! {| Zet

Title:

Date:

Information Classification: Limited Access

GPS# 180319755629459 2

MetricStream Confidential

EXHIBIT A

METRICSTREAM TERMS AND CONDITIONS

1.0 DEFINITIONS

1.1 “Affiliates” “Affiliate(s)” whether capitalized or not, means, with respect to a specified person,

any person that directly or indirectly controls, is controlled by, or is under common control with the

specified person, for as long as such relationship remains in effect where “control” means possessing,

directly or indirectly, the power to direct or cause the direction of the management, policies and

operations of such Person, whether through ownership of at least fifty percent (50%) of the voting

securities, by contract or otherwise. For the avoidance of doubt, with respect to State Street, any

Affiliates shall include Affiliates of State Street Bank and Trust Company and, its parent, State Street

Corporation.

1.2 “Cloud Services” means the Software, access to the Cloud Application, network access,

monitoring and maintenance of the Software and related services, as described in the applicable Order and

Service Level Agreement attached hereto as an Exhibit B and incorporated herein.

13 “Cloud Applications” means the MetricStream Software applications to be made available to

Customer as part of the Cloud Services.

1.4 “Confidential Information” as defined in Section 7.

1.5 “Customer Content” means all data and information that Customer uploads into the Cloud

Services.

1.6 “Documentation” means MetricStream’s documentation for the Cloud Services, in any medium,

electronic or written, including that which is currently published and delivered (whether physically with

the Software or on a MetricStream web site) to Customer by MetricStream under this Agreement, which

describes the content and functionality of the Cloud Services and how to use the Cloud Services including

details regarding the performance and operational characteristics of the Cloud Services and all technical,

systems and user manuals, drawing, diagrams or other materials.

1.7 “{ntellectual Property Rights” means all of the following in any jurisdiction throughout the world

and whether existing now or in the future: (a) patents and patent disclosures; (b) copyrights and

copyrightable works; (c) trademarks, service marks, trade dress, trade name, logos, and other designations

a party uses in connection with its business (whether registered or unregistered); (d) trade secrets and

know-how; (e) any other proprietary or intellectual property rights.

1.8 “Purchase Order” means a written order issued in electronic form by the Customer confirming

payment obligations as applicable under the MetricStream Order Form or SOW (as this term is defined in

the Master Services Agreement, attached hereto as Exhibit L).

1.9 “MetricStream Order Form” means MetricStream’s ordering document for Cloud Applications

and Services in the form of the Order Form attached to this Agreement Each Order Form shall be

consecutively numbered and shall reference the MetricStream Agreement number above and the Effective

Date of this Agreement. Customer’s initial purchase of Cloud Applications and Services is reflected in

Order Form No. 1, attached hereto as Exhibit to the Agreement.

1.10 “Master Services Agreement” means agreement for professional consulting services Master

Services Agreement between MetricStream and Customer, which attached hereto as Exhibit L and is

hereby incorporated by reference and Company dated of December 30, 2011.

Information Classification: Limited Access

GPS# 180319755629459 3

MetricStream Confidential

1.11 “Non-Disclosure Agreement” means that certain agreement concerning confidentiality entered

into by and between Customer and MetricStream, dated November 6, 2019.

1.12 “Security Incident” means any loss, destruction, theft, or unauthorized access, use or disclosure

of State Street Data (as defined in the Security Schedule D), which includes Customer’s Confidential

Information.

1.13 “Security Schedule” means that certain Security and Data Privacy Schedule, dated as of the date

of this Agreement, between MetricStream and Customer, which attached hereto as Exhibit D and is

hereby incorporated by reference.

1.14 “Services” means any services related to the Cloud Services, Service Level Agreement or any

other professional services provided by MetricStream to Customer (and set forth in an applicable SOW).

1.15 “Software” means the computer programs and applications, in machine readable (object code)

form as described in the, related Documentation and any supporting materials in either machine readable

or hard copy form.

1.16 “Subscription Term” shall mean the term as set forth in the applicable MetricStream Order Form.

2.0 CLOUD SERVICES

2.1 Cloud Services. MetricStream will provide Cloud Services in accordance with this Agreement

and an applicable MetricStream Order Form and a Purchase Order issued by Customer.

2.2 Access to the Cloud Applications. MetricStream hereby permits Customer access to and use of

the Cloud Applications as described in the applicable MetricStream Order Form. Customer may not use

the Cloud Applications to process information owned by or for the benefit of any third party unless such

use is specifically in connection with Customer’s authorized use of the Cloud Applications as specified in

the applicable MetricStream Order Form. In consideration of the access and permissions granted herein,

Customer shall pay the fees in the amount and in accordance with the payment terms set forth in the

applicable Metric Stream Order Form. Affiliates, regulators, consultants, and authorized contractors of

Customer are hereby authorized to access to and use of the Cloud Services and/or Cloud Applications.

Customer represents that its consultants and authorized contractors, who have access to the Cloud

Application, are or will be bound by confidentiality provisions which are, at the Jeast as stringent as the

provisions contained in the Non-Disclosure Agreement.

Customer shall have no obligation to order any products or services by virtue of this Agreement alone.

Whenever Customer does order products or services hereunder, Customer shall issue a written or

electronically transmitted Purchase Order to MetricStream prior to delivery. No product or service shall

be delivered prior to receipt of such Order by MetricStream. Customer shall not be obligated to pay for

any product or service for which it has not issued a Purchase Order to MetricStream. MetricStream shall

not be obligated to provide any product or service to Customer until it receives a MetricStream Order

Form. The terms and conditions of this Agreement shall prevail over any additional or conflicting terms

included on such Purchase Orders or on MetricStream’s acknowledgments, quotes or invoices.

Orders placed and acknowledgments sent under this Agreement may be sent in writing or by electronic

means. The Parties agree that: (i) these electronic transmissions shall be deemed to satisfy any legal

formalities requiring that agreements be in writing, (ii) neither party shall contest the validity or

enforceability of any such electronic transmission under any applicable statute of frauds, and (iii)

Information Classification: Limited Access

GPS# 180319755629459 4

MetricStream Confidential

computer maintained records when produced in hard copy form shall constitute business records and shall

have the same validity as any other generally recognized business records.

MetricStream shall deliver the products or services on the dates indicated. Payment for invoices that do

not conform to MetricStream Order Form, Customer Order and/or this Agreement may be delayed.

All products or services furnished by MetricStream under the terms of this Agreement shall be subject to

inspection and acceptance by Customer.

Customer’s acceptance of a MetricStream Order Form shall not be unreasonably withheld.

2.3 Acceptance of the Cloud Services. Customer shall test the Cloud Services to ensure that it

performs in accordance with the applicable Documentation to the reasonable satisfaction of Customer.

Customer shall have thirty (30) days from the completion of Cloud Services (“Acceptance Period”) to test

and accept or reject such Cloud Services as being in compliance with applicable Documentation and will

provide written notice thereof to MetricStream. If the Cloud Services is substantially in conformity with

the applicable documentation, then on or prior to expiration of the Acceptance Period, Customer shall

provide MetricStream with written notice of acceptance (“Acceptance”). In the event Customer provides

notice that the testing results do not meet applicable Documentation, MetricStream shall remedy any

deficiency promptly, but no greater than fifteen (15) business days and notify Customer that the

deliverable is available for testing as provided above. In the event MetricStream is not able to remedy the

defect, Customer may terminate this Agreement with respect to the applicable deliverable, and

MetricStream shall refund the fees prepaid by Customer with respect to such deliverable, In the event

Customer does not provide the response indicating its Acceptance or listing deficiencies within the

Acceptance Period defined above MetricStream shall notify Customer of such failure (“Final

Notification”) in writing (for that purpose notice may be in an email) and Customer shall promptly

provide the response within ten (10) days of receipt of Final Notification.

2.4 Affiliates may submit a MetricStream Order Form to MetricStream under this Agreement.

Customer’s Affiliates may receive services or procure the software or services from MetricStream under

this Agreement, In such event, each Customer Affiliate that signs a MetricStream Order Form confirmed

by a Purchase Order or Statement of Work shall be deemed to be Customer as such term is used herein

and shall be subject to the terms and conditions of this Agreement and beneficiary of all rights hereunder.

Each Customer Affiliate shall be solely responsible for its obligations under each applicable

MetricStream Order Form, Purchase Order or the Statement of Work signed by such Customer Affiliate

including compliance with this Agreement in relation to any such Orders and Statements of Work. Each

Customer Affiliate shall be entitled to enforce its rights under this Agreement directly against Metric

Stream, independent of Customer, in relation to Orders and Statements of Work that the State Street

Affiliate is signatory to. Subject to a Customer Affiliate complying with the terms and conditions of this

Agreement, no breach or termination of this Agreement by Customer or any other Customer Affiliate in

relation to the MetricStream Order Form, Purchase Orders or Statements of Work that Customer or such

other Customer Affiliate are signatories to will have any impact on the rights of the Customer Affiliate to

enforce this Agreement in relation to Orders and Statements of Work that such Customer Affiliate is

signatory to, which rights will continue notwithstanding any such breach or termination. For avoidance

of doubt, MetricStream is under no obligation to provide products or services to new Customer Affiliates

until there remain unpaid undisputed invoices by those new Customer Affiliates, provided that Metric

Stream has notified new Customer Affiliates of undisputed invoices according to the terms of this

Agreement.

Information Classification: Limited Access

GPS# 180319755629459 5

MetricStream Confidential

2.6 Limitation of Rights. Customer acknowledges that Customer’s rights in and to the Cloud

Applications are solely as set forth in Section 2.2 hereto and do not include any rights of ownership.

Customer agrees that MetricStream owns all right, title and interest, including but not limited to

copyright, patent, trade secret and all other Intellectual Property Rights, in and to the Cloud Applications,

and any changes, modifications or corrections thereof. All Customer Content is owned solely by

Customer and is the Confidential Information of Customer. Subject to the terms and conditions of this

Agreement State Street grants to MetricStream a worldwide, royalty-free, non-exclusive and non-

transferable license to store, manage the Customer Content, all solely in connection with and for the

purposes of providing the Cloud Services to Customer hereunder. Such license shall terminate

immediately upon the termination of this Agreement.

2.7 Professional Services. The Parties acknowledge and agree that if Customer requires professional

services such professional services will be provided under a statement of work governed by the Master

Services Agreement.

3.0 TERM AND TERMINATION

3.1 Term. The Term of this Agreement shall begin upon the Effective Date and shall remain in effect

until terminated pursuant to this Agreement.

3.2 Term of MetricStream Order Form. Each MetricStream Order Form shall last for the duration of

the initial term set forth on that MetricStream Order Form (“Initial Term”). Each MetricStream Order

Form may be renewed for additional terms (each a “Renewal Term”) as set forth herein. The Initial Term

of a MetricStream Order Form together with all Renewal Terms are herein referred to the Term (“Term”).

MetricStream shall issue a renewal notice to Customer at least ninety (90) days prior to the expiration of

the then current Term for an applicable Metric Stream Order Form. Customer shall have no more than

sixty days (60) prior to the expiration of the then current Term to reject the renewal notice issued

Customer. For avoidance of doubt, should Customer fail to reject the renewal notice sixty (60) days prior

to the expiration of the then current Term, the MetricStream Order Form shall automatically renew for

another one (1) year Renewal Term. The Parties may agree to renew an applicable MetricStream Order

Form by MetricStream’s issuance of an applicable MetricStream Order Form and Customer’s acceptance

of the MetricStream Order Form by its issuance of a Purchase Order for each Renewal Term. The Fees

for each subsequent Renewal Term shall be agreed between the Parties and shall not exceed 2.5 % of the

fee applicable in the prior Term.

3.3. Additional Customer Orders. In the event Customer wishes to purchase additional products or

services, the Parties shall execute an additional MetricStream Order Form and confirm it by means of a

Purchase Order.

3.4 Termination.

3.4.1 For Breach. Either Party may terminate this Agreement or the MetricStream Order Form upon

written notice to the other Party if a Party materially defaults in the performance of any material provision

hereunder, and if such default continues and is not cured by the breaching Party within thirty (30) days

after written notice thereof. Such termination right is in addition to, and not in limitation of, any other

remedies available to a Party.

3.4.2 Customer may terminate this Agreement or any MetricStream Order Form, without cause and

without liability or penalty, at any time upon thirty (30) days’ prior written notice to MetricStream.

Customer shall not be liable for any obligation, liability or penalty with respect to exercising its

Information Classification: Limited Access

GPS# 180319755629459 6

MetricStream Confidential

termination rights provided for in this Agreement. For the avoidance of doubt, Customer shall not be

entitled to a refund of pre-paid fees in the event of such termination for convenience.

3.4.3 Should Customer terminate this Agreement or the MetricStream Order Form for cause, Customer

shall be entitled to a pro-rated refund of the fees for the remaining Term as defined under the applicable

Order.

3.5 Effects of Termination. Upon expiration or termination of this Agreement; (a) Customer shall: (i)

cease using the Cloud Services; and (ii) certify, by email being sufficient, to MetricStream, upon request,

within one (1) month after expiration or termination that Customer has destroyed or has returned to

MetricStream all related documentation and copies thereof; and (b) MetricStream shall return to

Customer all data furnished by Customer in connection with this Agreement, however if any

MetricStream Services are required to migrate Customer’s data to other systems, the Parties shall

mutually agree to a transition plan more fully defined in an executable SOW issued pursuant to the

Master Services Agreement and any applicable provisions of this Agreement. Termination of this

Agreement shall not relieve Customer’s obligation to pay all fees that have accrued or are otherwise owed

by Customer under this Agreement for Services performed by MetricStream prior to termination.

Termination of this Agreement shall not relieve Customer’s obligation to pay all fees that have accrued or

ate otherwise owed by Customer under this Agreement for Services performed by MetricStream prior to

termination. All such payments shall be made by Customer within thirty (3 0) days of any termination of

this Agreement. In the event of termination, within twenty (20) business days of Customer’s delivery of a

hard drive (or other backup medium) to MetricStream, MetricStream shall provide a backup copy of

Customer’s production data and application files in a machine-readable format and should be able to load.

and print. —

3.6 Termination Assistance.

Upon any termination of the Agreement, Metric Stream shall, upon Customer’s request, continue to

provide the Cloud Application to Customer pursuant to the terms of this Agreement for a transitional

period of up to twelve (12) months (the “Transition Period”). Access to the Cloud Application during the

Transition Period will be subject to the fees set out in the applicable MetricStream Order Form or

Statement of Work, prorated on a monthly basis, based on the fees charged to Metric Stream for the

Cloud Application during the twelve (12) month period immediately preceding the termination date.

During the Transition Period, MetricStream will provide cooperation and assistance as Customer may

reasonably request to support an orderly transition to another provider of similar Cloud Application or to

Customer’s internal operations.

4.0 INDEMNITY

4.1. By MetricStream. MetricStream shall defend at its sole cost and expense or, at its option, settle,

any claim or proceeding brought against Customer or Customer Affiliate to the extent that it is based on

an assertion that the Cloud Application constitute infringement of any Intellectual Property Rights, and

shall indemnify and hold Customer harmless from and against all costs, damages and expenses, including

reasonable attorney's fees, asserted against Customer or Customer Affiliate which result from any such

claim. Without limiting the generality of the foregoing, should Cloud Application or any portion thereof

become, or in MetricStream’s opinion be likely to become, the subject of a claim of infringement or the

like under applicable patent or copyright or trade secret laws, MetricStream’s shall either procure for

Customer the right to continue using the Cloud Application, or to replace or modify the Cloud

Application, without changing their functional capabilities, so that the Cloud Application becomes non-

infringing. If Customer is unable to do either of the foregoing within thirty (30) days, upon request,

Information Classification: Limited Access

GPS# 180319755629459 7

MetricStream Confidential

Metric Stream shall refund the entire fees paid to Service Provider by Customer prorated to reflect use of

the Cloud Application by Customer or any Customer Affiliate prior to commencement of the Claim or

proceeding described herein.

MetricStream assumes no liability hereunder for, and shall have no obligation to indemnify, defend, hold

Customer harmless or pay costs, damages or attorney's fees for any claim based upon: (a) the

combination, operation or use of the Cloud Services furnished under this Agreement with software,

hardware or other materials or services not provided by MetricStream if such infringement would have

been avoided in the absence of such combination, operation, or use; or (b) use of altered Services or

services not authorized by MetricStream, (i.e., alterations to the Services by a party other than

MetricStream or not authorized by MetricStream), if the infringement would have been avoided by the

use of unaltered Services that MetricStream provides to Customer; (c) use or incorporation in the Services

of any design, technique or specification furnished by Customer, if the infringement would not have

occurred but for such incorporation or use; or (d) alteration of the Services by a party other than

MetricStream; or (e) Customer’s use of the Services other than as authorized under this Agreement.

4.2 By Customer. Customer shall defend at its sole cost and expense or, at its option, settle, any

claim or proceeding brought against MetricStream to the extent that it is based on an assertion that the

SSBT Content constitutes infringement of any Intellectual Property Rights, and shall indemnify and hold

MetricStream harmless from and against all costs, damages and expenses, including reasonable attorney's

fees, asserted against MetricStream which result from any such claim, provided that MetricStream

notifies Customer promptly in writing of any such claim or proceeding. This subsection shall constitute

Service Provider's sole remedy as to matters covered in this subsection.

43 Indemnification Procedures. Promptly after the receipt by a Party (the "Indemnified Party") of

notice of any claim, determination, suit or cause of action with respect to which the other Party is

obligated to provide indemnification (the "Indemnifying Party") pursuant to this provided, however, that

any delay by the Indemnified Patty to so notify the indemnifying Patty shall relieve the Indemnifying

Party of its indemnification obligations only to the extent that such delay materially prejudices the

Indemnifying Patty's defense. The Indemnifying Patty shall be entitled to assume control of the defense

and the negotiations, if any, regarding settlement of this matter. If the Indemnifying Patty assumes such

control, the Indemnified Patty shall be entitled to participate in the defense and negotiations of such

matter at its own expense; if the Indemnifying Patty does not assume control of the defense and

negotiations, the Indemnified Party may conduct such defense and negotiations and its reasonable costs

and expenses shall be subject to indemnification. The Patties agree, at the Indemnifying Party's expense,

to reasonably cooperate in such negotiations, defense or settlement and to give each other full access to

any information relevant thereto. The Indemnified Patty shall not enter into any settlement of such matter

without the written consent of the Indemnifying Party, and the Indemnifying Party shall not be obligated

to indemnify the Indemnified Party for any settlement entered into without the written consent of the

Indemnifying Party. If the consent of the Indemnified Party is required to effectuate any settlement

negotiated by the Indemnifying Party, then such consent shall not be unreasonably withheld.

5.0 LIMITED WARRANTY

5.1 Services. For the term of the Agreement, MetricStream warrants that the Cloud Services will

conform to the specifications and Documentation under this Agreement, applicable MetricStream Order

Form or SOW and shall be performed in a good and workmanlike manner, according to time frames and

in all material respects in accordance with the applicable and accepted MetricStream Order Form or

SOW. Customer’s sole and exclusive remedy (excluding Customer’s right to terminate this Agreement),

and MetricStream’s entire liability for any breach of this warranty shall be the service credits set forth in

Information Classification: Limited Access

GPS# 180319755629459 8

MetricStream Confidential

the Service Level Agreement of the applicable MetricStream Order Form. MetricStream further warrants

that the Cloud Services and any updates thereof do not contain any malicious code, program, or other

internal component (e.g. computer virus, computer worm, computer time bomb, or similar component)

(“Malicious Code”), which could damage, destroy, or alter the Cloud Service, or which could reveal,

damage, destroy, or alter any data or other information accessed through or processed by the Cloud

Services in any manner or which could permit unauthorized access, modification or other interference

with, or otherwise harm, any computer, systems or software used by the Customer; unless, and to the

extent MetricStream is able to prove relevant facts, such Malicious Code was provided by the Customer

or a third party under Customer’s direction. This warranty will be considered part of and covered under

the provisions of this Agreement. Customer must notify MetricStream promptly in writing of any

nonconformance under this warranty after it becomes aware of such nonconformance. Customer might at

its sole discretion: (i) provide MetricStream with reasonable opportunity to remedy any nonconformance

under the provisions of this Agreement and (ii) provide reasonable assistance in identifying and

remedying any nonconformance. MetricStream complies and shall continue to comply with all applicable

laws and regulations; and shall develop and implement, at its sole expense, an adequate disaster recovery

plan to ensure disaster recovery/business continuity and back-up capabilities for the Cloud Services.

5.2 Disclaimers. EXCEPT AS SET FORTH IN THIS AGREEMENT, NO OTHER WARRANTY,

EXPRESS OR IMPLIED, IS MADE WITH RESPECT TO ANY SERVICES TO BE SUPPLIED

HEREUNDER, AND METRICSTREAM EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES

OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, NON-

INFRINGEMENT OF THIRD-PARTY RIGHTS AND THOSE ARISING FROM A COURSE OF

DEALING OR USAGE OF TRADE.

6.0 PAYMENT AND TAXES; REPORTING

6.1 Fees. MetricStream will invoice Customer the fees set forth in the applicable MetricStream Order

Form, or SOW. MetricStream will send invoices to the address set forth in the applicable MetricStream

Order Form or SOW. Customer will pay MetricStream in U.S. dollars unless agreed to otherwise in

writing by the Parties, within forty-five days (net 45 terms) of receipt of a correct and undisputed invoice.

Customer shall notify MetricStream in writing, email being sufficient, of any bona fide disputed amount.

To the extent reasonably possible, MetricStream shall supply Customer with documentation to support

the validity of any disputed charge.

6.2 Taxes. Any charges and fees due hereunder are exclusive of any sales, use, or value added taxes

and any other similar taxes and governmental charges, however designated, arising out of this Agreement

(except taxes based on MetricStream’s income), and Customer shall pay. all such taxes and charges.

6.3 Reporting, From time to time but not more frequently than once per year, MetricStream may

request verification from Customer, by email being sufficient, which verifies that Customer’s use of the

Cloud Services, including the number of authorized end users, conforms with the terms and conditions of

this Agreement. Customer will deliver such verification to MetricStream within thirty (30) days of such

request by MetricStream.

7.0 CONFIDENTIAL INFORMATION

In conjunction with this Agreement, either Party may provide to the other Party and/or may generate

confidential and proprietary information. Each Party agrees that all confidential and proprietary

information disclosed or otherwise made available to the other Party in connection with this Agreement,

and any amendments thereto, including, without limitation, the existence of and the terms set forth in this

Information Classification: Limited Access

GPS# 180319755629459 9

MetricStream Confidential

Agreement, is “Confidential Information” as such term is defined in the Non-Disclosure Agreement dated

November 6. 2019 and executed by the Parties hereto and shall be treated as Confidential Information in

accordance therewith. The Non-Disclosure Agreement is incorporated herein by reference.

8.0 LIMITATION OF LIABILITY

8.1 Cap on Liability. Except for a Party’s (i) breach of its confidentiality obligations, (ii) liability for

Security Incidents, subject to Section 8.2., (iii) indemnification obligations, or (iv) for gross negligence,

willful misconduct or fraud, the Parties agree that the total liability of each of the Parties for any breach of

its obligations under this Agreement shall not exceed the total of fees paid by Customer under this

Agreement in the preceding twelve (months).

8.2 Liability Related to Security Incidents. Notwithstanding the terms of Section 8.1, the Parties

acknowledge and agree that, with respect to any claims arising from an alleged Security Incident where

such claim concerns State Street Personal Data, as defined in Exhibit E, to the extent that the Customer

incurs damages, MetricStream’s liability shall be determined as follows:

a. to the extent such Security Incident occurred despite MetricStream’s (and its Affiliates and

subcontractors) material compliance with the obligations under Section 9, the Security Schedule

and Data Processing Addendum, as applicable, MetricStream’s total liability shall be limited to

one million US dollars ($1.000.000), provided. that MetricStream shall not be liable for

consequential damages constituting lost profits, drop in share price, reputational harm, or

diminution to value;

b. to the extent such Security Incident occurred and MetricStream (and its Affiliates and

subcontractors) was not in material compliance with its obligations under Section 9, the Security

Schedule and Data Processing Addendum, as applicable, there shall be no limitation on

MetricStream’s liability for damages, provided that (i) MetricStream shall not be liable for

consequential damages constituting lost profits, drop in share price, reputational harm, or

diminution to value, and (ii) Customer materially complied with its own internal policy with

respect to the use and redaction of State Street Data on the Cloud Services, the policy being

attached hereto as Exhibit K;

c. for avoidance of doubt, a claim arising from a Security Incident concerning State Street Personal

Data shall not be considered to as an additional claim for breach of confidentiality under this

Agreement, provided that such Security Incident involved solely State Street Personal Data and

did not involve any other Confidential Information. Where a Security Incident involved other

State Street Data than State Street Personal Data, State Street shall not be prevented from

bringing any such additional claim, which shall not be subject to limitations under Section 8.2.

For clarification, this Section 8.2 shall not be interpreted to limit MetricStream’s liability in the event of

MetricStream’s (i) indemnification obligations under Section 4 or (ii) gross negligence, willful

misconduct or fraud.

8.3. EXCLUSION OF DAMAGES. EXCEPT FOR CLAIMS UNDER SECTIONS 4, 7, and 9 IN NO

EVENT SHALL EITHER PARTY BE LIABLE TO HE OTHER PARTY OR TO ANY THIRD PARTY

FOR LOSS OF PROFITS, OR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL OR

CONSEQUENTIAL DAMAGES (INCLUDING. BUT NOT LIMITED TO SUCH DAMAGES

ARISING FROM BREACH OF CONTRACT OR WARRANTY OR FROM NEGLIGENCE OR

STRICT LIABILITY), IN CONNECTION WITH THIS AGREEMENT, EVEN IF SUCH PARTY HAS

BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE

Information Classification: Limited Access

GPS# 180319755629459 10

MetricStream Confidential

LEGAL OR EQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH THE

CLAIM IS BASED.

9, DATA SECURITY AND DATA PROTECTION.

MetricStream shall have implemented as of the date of this Agreement, and shall thereafter continue to

maintain current, a comprehensive security and data privacy policy or policies that satisfies the

requirements set out in Exhibit D and Exhibit E.

10. GENERAL TERMS

10.1 Modification of the Agreement. Neither Party may modify or amend this Agreement except on

upon written agreement by the Parties. Subject to the requirements of applicable law, any such

modifications will become effective at the time stated in such notice. Neither Party has the right to

unilaterally modify this Agreement. Variance from the terms and conditions of this Agreement in any

Customer purchase order or other written notification sent by Customer will be of no effect.

10.2 Assignment. This Agreement may not be assigned by either Party without the prior written

consent of the other Party, which consent shall not be unreasonably withheld; provided, however, that

such consent shall not be required for the assignment of this Agreement by either Party to a wholly-

owned subsidiary or Affiliate of either Party or to a successor corporation or entity in connection with a

merger, consolidation or transfer of all or substantially all of the assets of either Party by such successor

corporation or entity. In such event, the assigning Party shall provide prior written notice of such

assignment to the other Party.

10.3. Survival. The provisions of Sections 3.4.3, 3.5, 3.6, 4, 5. 7, 8 9 and 10, shall survive any

termination of this Agreement, as will such other terms that by their nature should survive the termination

of this Agreement.

10.4 Governing Law. This Agreement and all acts and transactions pursuant hereto and the rights and

obligations of the Parties hereto shall be governed, construed and interpreted in accordance with the laws

of the State of Massachusetts and the United States of America.

10.5 Notices, Any notice or report required or permitted by this Agreement, except as otherwise set

forth in this Agreement, shall be in writing and shall be deemed sufficient upon receipt, when delivered

personally or by courier, overnight delivery service or confirmed facsimile, or forty-eight (48) hours after

being deposited in the regular mail as certified or registered mail (airmail if sent internationally) with

postage prepaid, if such notice is addressed to the Party to be notified at such Party’s address or facsimile

number as set forth below or as subsequently modified by written notice. It shall also be valid for a Patty

to send any notice to the other Party electronically (e.g., by email or through the Services). Such notice

will be deemed to have been given as of the date it is delivered.

For MetricStream:

MetricStream, Inc.

2479 East Bayshore Road, Suite 260

Palo Alto, California 94303

Atin: Chief Legal Counsel

For Customer:

State Street Bank and Trust Company

One Lincoln Street

Information Classification: Limited Access

GPS# 180319755629459 1

MetricStream Confidential

Boston, MA 02111

Attn: General Counsel

With copy to: Chief Procurement Officer

10.6 Severability; Waiver. If one or more provisions of this Agreement are held to be unenforceable

under applicable law, the Parties agree to renegotiate such provision in good faith, to maintain the

economic position enjoyed by each Party as close as possible to that under the provision rendered

unenforceable. If the Parties cannot reach a mutually agreeable and enforceable replacement for such

provision, then: (a) such provision shall be excluded from this Agreement; (b) the balance of the

Agreement shall be interpreted as if such provision were so excluded; and (c) the balance of the

Agreement shall be enforceable in accordance with its terms. No failure of either Party to exercise or

enforce any of its rights under this Agreement will act as a waiver of such rights or of any other rights

hereunder.

10.7 Relationship of the Parties. Nothing in this Agreement is to be construed as creating an agency,

partnership, or joint venture relationship between the Parties hereto.

10.8 Force Majeure. If either Party is prevented from complying, either totally or in part, with any of

the terms or provisions of this Agreement by reasons of fire, flood, storm, earthquake, strike, lockout or

other labor trouble, riot, war, rebellion, communications or utility failures, accident or other acts of God

(“Force Majeure Event”), then upon written notice to the other Party, the requirements of this Agreement,

or the affected provisions hereof to the extent affected, shall be suspended during the period of such

disability, if such Party shall have used reasonable efforts to avoid such occurrence and minimize its

duration and has given prompt written notice to the other Party. If such period exceeds twenty (20) days,

the other Party may, at its option, terminate this Agreement. If terminated by Customer, MetricStream

shall refund to Customer any and all prepaid fees unused by Customer covering the remainder of any

applicable Term. Notwithstanding foregoing, Customer shall not be delayed with respect to payment

obligations unless the particular Force Majeure Event causes the delay.

10.9 Laws. MetricStream and Customer shall comply with all applicable laws, rules and regulations of

Federal, State, or local governments in connection with this Agreement.

10.10 Marketing Rights. MetricStream may not, except upon Customer’s prior written consent, which

may be withheld for any reason, (a) use Customer’s or an Affiliate of Customer’s name or logo on

MetricStream’s website and customer list nor issue a press release announcing MetricStream’s selection

by Customer; (b) seek Customer’s or an Affiliate of Customer’s participation in additional marketing

activities and engagements from time to time. Examples of such activities and engagements include

reference calls from prospects, media interviews, video testimonials, case studies, webinars, analyst

surveys and presentations.

10.11 Export Restrictions. Customer acknowledges and agrees to comply with all export and re-export

restrictions and regulations of the Department of Commerce or other United States agency or authority.

Without limiting the foregoing or any other provision of this Agreement, Customer agrees not to

download or transfer (or authorize anyone to download or transfer) the Customer Materials: (i) into (or to

a national or resident of) any country to which the U.S. has embargoed goods; or (ii) to anyone on the

U.S. Treasury Department’s list of Specially Designated Nationals or the U.S. Commerce Department’s

Denied Person List.

Information Classification: Limited Access

GPS# 180319755629459 12

MetricStream Confidential

10.12 Entire Agreement: Amendment. These Terms and Conditions, along with the signature page,

including the Service Level Agreement, Acceptable Use Policy, Security Schedule, Data Privacy

Addendum, Human Trafficking Exhibit, the Non-Disclosure Agreement and all applicable Orders, SOWs,

MetricStream Order Forms and all other attachments, addenda, and amendments , constitute the entire

agreement between the Parties with respect to the subject matter contained in this Agreement and

supersede all prior agreements, whether written or oral, with respect to such subject matter. In the event of

any conflict between this Agreement and a MetricStream Order Form, the terms of this Agreement shall

control unless specified by the MetricStream Order Form but only with respect to Services or deliverable

provided pursuant to this Agreement. No “click-through,” “shrink-wrap,” “browse-wrap” or similar terms

that have not been specifically negotiated by the Parties, whether before, on, or after the date of this

agreement, will be effective to add to or modify the terms of this agreement, regardless of any Party’s

“acceptance” of those terms by electronic means. No modification, waiver, or discharge hereof will be

valid unless in writing and signed by an authorized representative of the Party against which such

modification, waiver or discharge is sought to be enforced.

10.13 INSURANCE.

MetricStream represents that it now carries, and agrees that it will continue to carry during this Agreement,

with insurers having an AM Best Rating of A- or higher, insurance in the following amounts:

‘Type of Coverage = P|. Mihimum-Coverage Amounts

Workers:Compensation (including

: Waiver of Subrogation).

"We do-not carry this type of policy

Values at Risk at Full Replacement Cost

Based on project value (no coverage N/A)

: Transi a Values at Risk (no coverage N/A)

Information Classification: Limited Access

GPS# 180319755629459 , 13

MetricStream Confidential

In addition, Customer may require additional insurance coverage depending upon MetricStream’s

business or the services to be performed by MetricStream on behalf of Customer.

Prior to commencing work, and thereafter on the anniversary date of this Agreement and continuing for a

period of three years following the termination of this Agreement, MetricStream shall provide to

Customer certificates of all such insurance evidencing the coverages noted herein and as modified by any

order. In addition, MetricStream shall provide Customer with certificates or endorsements or other

sufficient written confirmation indicating that Customer, its parent, subsidiaries, Affiliates and their

respective officers, agents and employees, have been named as Additional Insured’s under its

Commercial General Liability, Auto Liability, and umbrella Liability policies: MetricStream shall

provide Customer thirty (30) days’ advance written notice (in accordance with the notice procedures

hereunder) of any cancellation, in any insurance coverage hereunder. To the extent that MetricStream is

based outside of the United States and/or will be providing any services from outside of the United States,

MetricStream shall ensure that its insurance coverage applies to losses occurring outside of the United

States. MéetricStream’s policy will be considered primary coverage for claims arising out of the

contractual relationship.

10.14 Divestment. If Customer or any of its Affiliates is required by applicable law, rule or regulation

or at the direction of its regulators to separate some or all of its Affiliates, divisions, departments, business

unites and/or certain of its assets or otherwise divests any Affiliate, division, department, business unit or

asset so that such Affiliate, division, department, business unit or asset (the “Divestee”) is no longer under

the control of Customer or any of its Affiliates, then Customer or any of its Affiliates may, upon written

notice to MetricStream, continue to use the Cloud Services for the benefit of the Divestee for a period not

to exceed twelve (12) months after the effective date of the divestiture or until the end of the Term

(whichever is earlier). During such period, Customer will continue to pay the fees for the Cloud Services

as if the Divestee continued to be an Affiliate of Customer, however, in no event may use of the Cloud

Services for the benefit of the Divestee expand beyond the scope of use related to the divested assets prior

to the divestiture. During such period, Customer shall be liable for the acts and omissions of Divestee

relating to this Agreement.

10.15 MetricStream Third Party Risk Management Program. MetricStream agrees to participate in

Customer’s MetricStream third party management program including completing Customer’s

MetricStream risk assessment questionnaire(s) when requested by Customer. Requests by Customer will

be no more frequent than once in any twelve (12) month period for any services provided to Customer.

MetricStream also agrees to make appropriate resources available for follow-up phone review(s) of the

questionnaire or, if requested by Customer, for an onsite visit.

Information Classification: Limited Access

GPS# 180319755629459 14

MetricStream

EXHIBIT B

Confidential

Service Level Agreement

Business Hours: 8:00 am hours to 5:00pm EST (Customer requested time zone) for 8X5 Support

Customer Support:

Telephone Support a

Self-Service Portal

Version Level Support

Ability to contact support

between 8:00 a.m. to

5:00 p.m. Monday through

Friday, excluding holidays

scheduled by MetricStream

(“Normal Business Hours”)

Ability to contact Support

through e-mail

Online access to ticketing

system to report an incident.

Support for Previous version

release of the Cloud

“Support Email Address:

1-800-858-

Support Telephone Number:

5658

support@metricstream.com

Response will be end of current Business

Day

Support Online:

support.metricstream.com

Response will be as per the Response Time

mentioned below

Support available for up to twenty-four (24)

months following the release of a new

Applications version of the Cloud Applications

Proactive Support:

“Support Type ‘| Support Description ..

| Self-Service Online access to ticketing system to monitor status of outstanding 24x7x365

Portal tickets

“System | Regular scheduled System Monitoring ofthe environment ‘| Continuous \_|

Monitoring Monitoring for

Frequency Cloud Services

“Account ‘| | Regular meeting with Account Management Team to review overall | Quarterly

Review status including outstanding tickets and usage reports.

Information Classification: Limited Access

GPS# 180319755629459

15

MetricStream

Functionality:

(sevaiien

| Classification |

Critical

Severity 2

Major |

'Severity3

| |

Minor

Severity Description .

down

“Severity | Critical service functionality

is

| Major impact to Customer's

| business, part or all of the

application is unavailable for

25% of the Users,

exists

Cyber security issue that

\

| No reasonable worka round(s)

\_ Malfunction causes response

| time for the system to be

substantially downgraded

: Re

! 2hours | Every 2 hours during

involves personally identified or

or degraded

| personal health information

| There are time-sensitive issues

t

{

$

that impact ongoing production

temporary

Malfunction that causes

| Workaround exists, but it is only

response time to be materially

downgraded

down or impaired

Does not have significant

current production impact

Performance is degraded

/ Non-critical functionality is

A short to medium term work-

Information Classification: Limited Access

GPS# 180319755629459

tesponse

Time .

| Critical functionality is impaired 4 Hours .

Next

Business

day

Confidential

Follow-up Frequency | Resolution Goal

| Business Hours.

| After Business Hours,

| update frequency

| will be mutually

agreed upon.

Self-service portal

| will be updated daily

NA

Within 8 Hours

the issue will be

contained.

Permanent

| resolution will be

in “Next Patch

Delivery OR ona

mutually agreed

upon date”

Work will

continue during

normal business

hours until the

issue is contained

Permanent

resolution will be |

in “Next Patch

Delivery OR ona

mutually agreed

upon date”

Permanent

resolution will be

in “Next Patch

Delivery OR ona

mutually agreed

upon date”

16

MetricStream Confidential

| around is available |

|

| }

Severity4 | Non-critical functionality is | NA |

| impaired |

Low Impact Next Permanent

| No business impact | Business — resolution will be

Da in “Next Patch

A medium to long term work- y .

; . Delivery OR ona

around is available

mutually agreed

Patch, service pack or upgrade | upon date”

is available |

Se A Se po En

Maintenance Windows:

‘Standard Maintenance Window : Pacific ic Time: Friday 11:00 pm — Saturday 5:00 am |

Extended Maintenance Window Pacific Time: Friday 9:00 pm — Saturday 12:00 pm |

Disaster Recovery:

; Recovery Declaration 12 hours | ~ | 8 hours 4 hours

6 hours

24 hours 24 hours 1 hours

Cloud Environment:

Annual Vulnerability Scans and review of cloud and applications .

Intrusion Detection System Active24/7/365. 22° «°° © CCC ee

secrereenye-e-eeee nse estimeteenmeervintpinan titan tt seems tener bt mentee nerve nr Ate me rr ro rm nme tt

“Security Event Notifications Within 24 hours of identification of breach

Annual ‘Penetration testing performed by trusted independent

Penetration Testing third party

Information Classification: Limited Access

GPS# 180319755629459 17

MetricStream Confidential

Uptime/Availability

99.5% of the time, each calendar month, measured ona

24x7x365 basis, excluding scheduled maintenance

{Total Minutes} — {Scheduled Down Minutes) — {Unscheduled

Uptime/Availability % Calculati

ptime/Availability % Calculation Down Minutes} / {Total Minutes} — {Scheduled Down Minutes}

Logging and Monitoring 3ax7x865

Maintain disaster recovery infrastructure for production

Redundanc

un y environment based on Cloud tier

Maintain Service Organization Control reports like SSAE16 SOC2

Control Audit or ISAE 3402. Also, industry accepted security certifications and

standards like ISO 27001, PCI-DSS, NIST

Security:

~ |

‘Objective: | oF Metric

; The Provider application data will be encrypted at rest and in

Data security PP "ve |

transit.

All end user network traffic shall be encrypted via TLS over

HTTPS or via VPN.

ees meme imneteeeieetni ert Metter ee erect vrhs ht pent a At

Network security

critical OS/System patches must be performed regularly and

System Patching should coincide with regularly scheduled maintenance windows

(“Scheduled Downtime” as defined in Section 2(d) of this Service

Level Agreement).

System Availability

System Response a a ae : be Availability

“System Response Time Service Level | All transactions within t the > MetricStream Applications will

process at an average response time of 4 seconds or less

measured across the reporting period.

All batch processing will be completed within the time agreed

to by the Parties in the Business Requirements documents.

“Exclusions for Response Service Scheduled Downtime.

Levels

End User systems not meeting minimum required standards

Information Classification: Limited Access

GPS# 180319755629459 18

MetricStream Confidential

for physical memory, Processor speed, internet bandwidth or

browser version

“Subscription Services Availability “7X24 x 365

Service Level

“Exclusions for Availability Service

Levels

“99.50% to 99.0%

"99.0% to 98.5%

98.5% to 97.0%

97.0% to 90.0%

Below 90.0 %

Engagement Model:

Reporting

Quarterly Provider will provide Customer the Quarterly SLA

Performance Report for the Provider Application

covered by this SLA. It will present comparative

analysis of SLA delivery in previous consecutive

four (4) quarters, as available.

Annually — Provider will provide Customer the Annual SA

Performance Report for each Provider Application

covered by this SLA. It will present comparative

analysis of SLA delivery in last three (3) years, as

available.

Service Review Meetings

Quarterly A quarterly review meeting may be held between

Customer and Provider for the Provider

Application and Subscription Services covered

under this SLA.

Annually An annual SLA performance review meeting may

be held to review the Annual SLA Performance

Report for the Provider Application and

information Classification: Limited Access

GPS# 180319755629459 . 19

MetricStream

Confidential

of objectives for this meeting is to decide if this

SLA should be amended.

Information Classification: Limited Access

GPS# 180319755629459

20

MetricStream Confidential

EXHIBIT C

ACCEPTABLE USE POLICY

This Acceptable Use Policy (“Policy”) specifies the actions prohibited by MetricStream, Inc. to Users of

the Cloud Application. By using the Cloud Application, you acknowledge that you and users that have

gained access to the Cloud Application through your account, have read, understood, and agree to abide

by the Policies. You are responsible for violations of these Policies by any User. While it is not our intent

to control or monitor your on-line communications, we may block services that we deem to be in

violation of the Policies or that we otherwise deem harmful or offensive. MetricStream reserves the right

to modify the Policy at any time, effective upon posting of the modified Policy to the Cloud Application

URL address and/or by providing the new Policy to you.

Illegal Activities

The Cloud Application may only be used for lawful purposes. Use of the Cloud Application for

transmission, distribution, retrieval, or storage of any information, data, or other material in violation of

any applicable law or regulation (including, where applicable any tariff or treaty) is prohibited. This

includes, without limitation, the use or transmission of any data or material protected by copyright,

trademark, trade secret, patent, or other intellectual property right without proper authorization and the

transmission of any material that constitutes an illegal threat, violates export control laws, or is obscene,

defamatory, or otherwise unlawful.

Network and System Security

Violations of system or network security are prohibited and may result in criminal and civil liability.

MetricStream will investigate incidents involving such violations and may involve and will cooperate

with law enforcement if a criminal violation is suspected. Examples of system or network security

violations include, without limitation, the following:

Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test

the vulnerability of a system or network or to breach security or authentication measures without express

authorization of the owner of the system or network.

Unauthorized probing and/or scanning of any system without prior consent of the owner or system

administrator. This includes, but is not limited to, "dictionary attacks" and/or attempts to harvest or verify

email addresses.

Unauthorized monitoring of data or traffic on any network or system without express authorization of the

owner of the system or network.

Interference with service to any user, host or network including, without limitation, mail-bombing,

flooding, deliberate attempts to overload a system and broadcast attacks.

Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup

posting.

Attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal

functioning, operation, or security of any network, system, computing facility, equipment, data, or

information.

Engage in any activities that may interfere with the ability of others to access or use the Service or the

Internet.

Information Classification: Limited Access

GPS# 180319755629459 21

MetricStream Confidential

Email/Usenet

Sending unsolicited mail messages, including, without limitation, commercial advertising and

informational announcements, is explicitly prohibited. A user shall not use another site's mail server to

relay mail without the express permission of the site. All postings to Usenet must comply with that

group's usage policies. Cross-posting and/or off topic messages, including commercial messages, is

explicitly prohibited.

Nothing contained in this Policy shall be construed to limit MetricStream’s actions or remedies in any

way with respect to any of the foregoing activities, and MetricStream reserves the right to take any and all

additional actions it may deem appropriate with respect to such activities, including without limitation

taking action to recover the costs and expenses of identifying offenders and removing them from the

MetricStream service, and levying cancellation charges to cover MetricStream costs in the event of

disconnection of dedicated access for the causes outlined above.

If you become aware of any violation of these Policies by any person, including Users that have accessed

the Service through your account, please notify us at support@metricstream.com. We will notify you,

our Customer, of complaints received by us regarding each incident of alleged violation of these Policies

by your Users of the Service. You agree to promptly investigate all such complaints and take all necessary

actions to remedy any actual violations of these Policies. We may identify to the complainant that you are

investigating the complaint and may provide the complainant with the necessary information to contact

you directly to resolve the complaint. You shall identify a representative for the purposes of receiving

such communications. Additionally, any data sent to MetricStream, Inc., by either the complainant or our

client or any other party sending data to us, including but not limited to header information, log file

information, alleged abuse, and any personal subscriber or alleged subscriber information, remains the

intellectual property of the sender; however, MetricStream, Inc. may use that information to resolve the

dispute, including but not limited to, providing that information to either the complainant, our client, or

other party that MetricStream, Inc. deems as qualified in assisting in the resolution in such disputes. We

also reserve the right to install and use, or to have you install and use, any appropriate devices to prevent

violations of these Policies, including devices designed to filter or terminate access to the Cloud

Application provided by us.

Information Classification: Limited Access

GPS# 180319755629459 22

MetricStream Confidential

EXHIBIT D

SECURITY AND DATA PRIVACY SCHEDULE

This Security and Data Privacy Schedule, including all Appendices hereto {this “Schedule”), effective as

of January 31, 2020 (the “Effective Date”), is entered into by and between MetricStream, inc., a

Delaware corporation having its principal place of business at 2479 East Bayshore Road, Suite 260, Palo

Alto, California, 94303 (the “Service Provider’) and State Street Bank and Trust Company a

Massachusetts trust company having its principal place of business at One Lincoln Street, Boston

Massachusetts 02111-2900 (“State Street”) (each, a “Party” and, collectively, the “Parties”), as may be

amended upon the mutual written agreement of the Parties from time to time (the “Schedule”).

WHEREAS, State Street, and/or its affiliates, and Service Provider have entered into various agreements

and documents (each, an “Agreement”) for Service Provider to perform services as specified in the

applicable Agreement;

WHEREAS, State Street and Service Provider wish to enter into this Schedule to govern all applicable

services that require Service Provider to comply with the obligations set forth herein; and

WHEREAS, State Street and Service Provider agree that in the event that Service Provider hosts, stores,

accesses or processes State Street Data (as defined below) outside of State Street’s environment or

performs any services at State Street’s location or that require access to State Street’s network

environment or systems as provided under each applicable Agreement, Service Provider and its assigned

personnel shall comply with the terms of this Schedule.

NOW, THEREFORE, In consideration of the mutual covenants contained herein, Service Provider and

State Street hereby agree to the following provisions:

Objectives

Service Provider shall implement commercially reasonable data security measures that are

consistent with banking industry standards such that Service Provider:

a. Protects the privacy, confidentiality, integrity, and availability of all data, information, text,

visual, audio or graphic representations and other materials in any medium or format, either

electronic, or tangible which is disclosed by or on behalf of State Street to, or otherwise comes

into the possession of, the Service Provider or personnel in connection with each applicable

Agreement, including but not limited to State Street’s Confidential Information including

personal data (collectively, “State Street Data”);

b. Protects against accidental, unauthorized, unauthenticated, or unlawful access, copying, use,

processing, disclosure, alteration, transfer, loss or destruction of the State Street Data including,

but not limited to, identity theft;

c. Complies with all applicable laws, rules, regulations, directives and decisions (each, to the extent

having the force of law) that are relevant to the handling, processing and use of State Street

Data by State Street or Service Provider, on State Street’s behalf, in accordance with this

Schedule; and

Information Classification: Limited Access

GPS# 180319755629459 93

MetricStream Confidential

d. Ensures security measures and procedures Include (but shall not be limited to) appropriate

administrative, physical, technical, procedural and organizational safeguards, including, but not

limited to, the requirements listed in Appendix A and Appendix B hereto.

if there is a discrepancy between any applicable Agreement and this Schedule, this Schedule shall

control and amend that section of the applicable Agreement.

IN WITNESS WHEREOF, the Parties hereto execute this Schedule as an instrument under seal by their

duly authorized officers by affixing their signatures below.

METRICSTREAM, INC. STATE STREET BANK AND TR COMPANY

— : jf ‘p

By: cs ; By: ‘

<

Name Sess/rg Zhou name; Mi /feL— Ae WEI

rive: Crief Legal officer rite: \_LUP- Cerente (Wh

Information Classification: Limited Access

GPS# 180319755629459 24

MetricStream Confidential

Appendix A

Information Security Requirements

Security Policy Requirement

4.

As of the effective date of this Schedule or such other date as the Parties agree in writing, Service

Provider shall have implemented, and shall thereafter maintain current, a comprehensive security

policy or policies (“Security Policy”) that satisfies the requirements set forth below. Service Provider

agrees that it shall not make any change(s) to its Security Policy that effectively reduces or limits the

rights or protections offered to State Street under this Schedule generally.

Upon request by State Street on an annual basis, the Service Provider shall provide State Street's

Chief Information Security Officer or his or her designee with a copy of its then current Security

Policy and an opportunity to discuss Service Provider's security measures with a qualifi ied IT

management member of Service Provider. The Security Policy must reflect security measures added

as a result of risk assessment findings.

Service Provider shall review its Security Policy regularly, and particularly following any changes in

applicable law, advances in technology or changes to the Service Provider's information systems, in

order to verify that the Security Policy and controls set out therein remain accurate, comprehensive

and up to date.

Standards of Protection

Service Provider shall secure and protect State Street Data by using at least the same degree of care

as the Service Provider uses to secure and protect its own confidential and proprietary information

but in no event any less than reasonable care; provided, however, that with respect to those

jurisdictions which do not recognize a reasonable standard of care Service Provider shall be

obligated to use best efforts.

Data Discovery and Tracking

Service Provider and its Approved Subcontractors shall not perform data discovery, tracking, content

analysis, or other metadata or data collection on State Street Data stored in the Service Provider’s

environment without explicit written agreement.

General Training and Awareness

Service Provider, prior to making any State Street Data available, shall institute an appropriate

training and education program to ensure that its personnel are appropriately trained regarding

their responsibilities with respect to the confidentiality and non-disclosure duties including, without

limitation, any special requirements relating to State Street Data.

Risk Assessments

a. Risk Assessment — Service Provider shall perform regular, at least annually, robust,

comprehensive risk assessments which identify the State Street Data or business assets (e.g.,

facilities, equipment, devices, etc.), the threats against those assets (both internal and external),

Information Classification: Limited Access

GPS# 180319755629459 25

MetricStream \_ Confidential

the likelihood of those threats occurring and the impact upon the organization to determine an

appropriate level of Information Security safeguards.

b. Risk Mitigation — The Service Provider shall manage, control, and mitigate any risks identified in

the Risk Assessment that could result in unauthorized access, copying, use, processing,

disclosure, alteration, transfer, loss or destruction of any State Street Data, including without

limitation, explicit protection against identity theft, so as to achieve the Objectives stated in this

Schedule, commensurate with the sensitivity of the State Street Data, as well as the complexity

and scope of the activities of the Service Provider pursuant each applicable Agreement.

c. Risk Assessment Summary ~ Service Provider shall provide State Street with the written high

level summary of the Risk Assessment upon request. If State Street believes vulnerabilities or

threats have not been fully addressed in the Risk Assessment, Service Provider shall expand the

Risk Assessment to appropriately address such vulnerabilities or threats and represent and

warrant that any and all vulnerabilities and threats have been successfully remediated. Service

Provider shall promptly employ a mutually agreed, independent third party expert to perform a

follow up assessment. Service Provider agrees to at minimum remediate any risk findings, other

than those properly designated as low risk, from the follow up assessment that could potentially

affect State Street at Service Provider's expense.

d. Specific Vulnerability Risk Assessment and Remediation/Mitigation — From time to time State

Street can request from Service Provider a Risk Assessment targeted to a specific

threat/vulnerability (example: WannaCry) which can negatively impact a service provided to

State Street by the Service Provider or confidentiality, integrity, and/or availability of State

Street Data in custody of the Service Provider. Service Provider shall in reasonable time, but not

longer than 45 days, complete such Risk Assessment and provide State Street results as well as

remediation and/or mitigation plan, if applicable.

e. Security Controls Testing — Service Provider shall engage an independent external auditor to

conduct periodic, at least annually, reviews of the Service Providers security practices against

various standards, such as SSAE 16, SSAE 18, ISAE 3402, ISO 27001 Certification, Payment Card

Industry Data Security Standard (PCI DSS; acceptable only if Attestation of Compliance was

completed by a third party Qualified Security Assessor (QSA)), as applicable. Service Provider

agrees to at minimum remediate any risk findings, other than those properly designated as low

risk, resulting from this testing and provide confirmation of remediation to State Street. Upon

request, the Service Provider agrees to make such reports available for review by State Street.

5. Organizational Security

a. Responsibility - Service Provider shall assign responsibility for information security

management to appropriate skilled and senior personnel only.

b. ‘Need to Know’ Access — Service Provider shall restrict access to information systems used in

connection with the services provided under each applicable Agreement and/or to State Street

Data to only those personnel who are reliable, have sufficient technical expertise for the role

assigned and know his or her obligations and the consequences of any security breach.

c. Confidentiality - Service Provider personnel who have accessed or otherwise been made known

of State Street Data, shall maintain the confidentiality of such information. No less frequently

than annually, all Service Provider personnel that may have access to State Street Data will be

Information Classification: Limited Access

GPS# 180319755629459 26

MetricStream Confidential

required to certify that such individual has read and complied with the confidentiality and non-

disclosure duties in this Schedule. State Street reserves the right to inspect this certification.

6. Asset Management

Data Sensitivity — Service Provider acknowledges that it understands the sensitivity of the State

Street Data.

Data Control — Unless otherwise agreed to in writing by State Street, Service Provider and its

personnel shall not copy, download, transmit (to or from), or store State Street Data on any

desktop, laptop, server, portable or other device at any location, unless directly related to the

delivery of service under each applicable Agreement.

Configuration Management — Service Provider shall establish a configuration baseline for all

information systems using applicable information security standards, manufacturer

recommendations, and Industry best practices. Service Provider shall establish appropriate

monitoring to ensure that all information systems are configured according with established

configuration baseline throughout the life of the information system.

Change Management — The implementation of changes and the introduction of new systems

must be controlled, documented, and enforced by the use of formal change control procedures

including documentation, specifications, testing, quality control, and managed implementation.

External Hosting Facilities (non-cloud based) — Service Provider is solely responsible for

exercising control over the collection, use, storage, disclosure, and deletion of State Street Data

by an external hosting provider in accordance with local and international laws and based on

any additional State Street written requirements agreed upon by the Service Provider. Any and

all hardware or other infrastructure used by an external hosting provider in connection with

performing the service obligations which Service Provider has under each applicable Agreement

(“Infrastructure”) must be used solely by, and operated solely for, Service Provider in

performance of its Service obligations with State Street (i.e. not shared) and no other third

party. “Infrastructure” may be managed and maintained by third party hosting provider under a

contract with Service Provider; provided however that access to the dedicated Infrastructure is

controlled solely by Service Provider. State Street Data collected, processed, stored, disclosed,

or deleted by the external hosting provider must be identifiable by its geographic location for

compliance with local and international privacy laws.

7. Cloud Computing

Service Provider represents and warrants that it does not and shall not rely upon a SaaS, PaaS or

laaS (all variations collectively referred to as \*aaS) , in public, hybrid and/or community cloud

computing infrastructures to perform services provided to State Street, including without

limitation, the processing or storage of State Street Data including incidental processing/storage

in business support/communications systems (example: cloud-based office suite for documents

processing and email), unless specifically approved by State Street in writing. State Street shall

not unreasonably withhold such approval if the service in the \*aaS cloud infrastructure used by

Service Provider is a dedicated virtual environment in which the systems are physically or at

minimum logically separated and isolated from other tenants using strong authentication,

access controls, and encryption. Penetration testing must be conducted in accordance with

sections “11 a. Penetration Testing” and “11 b. Penetration Testing Scope” below.

Information Classification: Limited Access

GPS# 180319755629459 27

MetricStream Confidential

Service Provider leveraging cloud services must be able to specify at any time, in writing, the

physical geographic location(s) of all State Street Data while in create, store, use, share, archive,

or destroy phases when State Street Data may be handled. Service Provider must be informed in

particular as to how State Street Data may be stored, forwarded, mirrored, backed-up, and

recovered at any given time.

if Service Provider leverages externally facing cloud environments, then Service Provider will be

subject to additional cloud security controls review by State Street.

For definitions of terms used in this section refer to the section “17. Definitions and Guidance”

at the end of this Schedule.

8. Security Training — Professional

a. Privileged Access Users — In addition to its training obligations under each applicable Agreement

generally, Service Provider shall make available specific security training to all personnel granted

privileged access (e.g., root, dba, system admin, network admin, superuser level access, support,

etc.) to systems which handle or hold State Street Data and/or are used to provide services.

b. Developer — Service Provider also shall make available to development teams associated with

development efforts impacting State Street, specific training focused on well-defined and

secured coding standards.

9. Media Handling

a. Physical Security of Media — Service Provider shall prevent the unauthorized viewing, copying,

alteration or removal of any media containing State Street Data, wherever located. Removable

media on which State Street Data is stored (including, but not limited to, thumb drives, CDs,

DVDs, and tablets) by Service Provider must be encrypted using at least 256 bit AES (or

equivalent) and may not be used or re-used by Service Provider to store data of any other

customer or to deliver data to any third party unless prior to such use or re-use the State Street

Data is securely erased. [Note: excludes laptops which are referenced in separate section.]

b. Media Destruction — Service Provider shall destroy removable media and any mobile device

(such as discs, USB drives, DVDs, back-up tapes, printers, laptops and tablets) containing State

Street Data or render State Street Data on such physical media unintelligible and not capable of

reconstruction by any technical means prior to any reuse of the media, if requested by State

Street or if such media or mobile device is no longer intended to be used. All backup tapes

which for any reason are not destroyed must meet the level of protection described in this

Schedule until destroyed.

c. Paper Destruction — Service Provider shall cross shred all paper waste and dispose in a secure

and confidential manner so as to render all paper waste unreadable.

10. Communications and Operations Management

a. Penetration Testing — Service Provider shall, on at least an annual basis, contract with an

independent third party to conduct a penetration test of the Service Provider's State Street Data

Environment (SSDE). Service Provider will provide State Street with a high-level summary of the

test results including the scope and the methodology of the test and confirmation that at

Information Classification: Limited Access

GPS# 180319755629459 28

MetricStream Confidential

minimum all identified findings, other than those properly designated as low risk, have been

remediated. For definitions of terms used in this Section refer to the Section 17. Definitions and

Guidance at the end of this Schedule.

b. Penetration Testing Scope — The scope of a penetration test must include the entire SSDE

perimeter and any critical systems that may impact the security of the SSDE. This includes both

the external perimeter (public-facing attack surfaces) and the internal perimeter of the SSDE

(LAN-LAN attack surfaces). Testing must include both application-layer and network-layer

assessments. External penetration tests also include remote access vectors such as dial-up and

VPN connections. More detailed guidance provided in section 17. Definitions and Guidance at

the end of this Schedule.

c. Data Encryption — Service Provider shall encrypt or protect by other technical means State

Street Data in Service Provider's possession or control so that it cannot be read, copied, changed

or deleted by unauthorized personnel while in storage, including when saved on removable

media. FIPS 140-2 Level 3 or ISO 19790 Level 3 compliant or equivalent encryption is required

for certain data based on State Street determination. If applicable, this encryption requirement

will be communicated to Service Provider in writing before such data is transferred. The

requirement is applicable for personal data as defined in Appendix B.

d. Data Protection During Transmission or Transit — Service Provider shall encrypt using an

industry recognized encryption algorithm and protect State Street Data in Service Provider's

possession or control so that it cannot be read, copied, changed or deleted by unauthorized

personnel during transmission or transit inside or outside of Service Provider's internal network.

e. Data Loss Prevention or Equivalent Controls at least as stringent as Data Loss Prevention.

Service Provider shall implement a comprehensive data leakage solution that identifies, detects,

monitors, documents and either alerts or prevents said State Street Data from leaving the

Service Provider control without authorization in place.

f. Data Destruction — Service Provider shail agree at the request of State Street to (i) promptly

return to State Street, in the format and on the media reasonably requested by State Street, all

or any part of State Street Data; (ii) erase or destroy rendering unrecoverable all or any part of

State Street Data in Service Provider’s possession, in each case to the extent so requested by

State Street; and (iii) provide letter of attestation that State Street Data has been successfully

erased or destroyed.

g. Network Ports — Service Provider shall restrict unauthorized network traffic affecting State

Street Data.

h. Wireless Network — Service Provider shall ensure use of Wi-Fi (aka 802.11) network traffic is

encrypted using WPA2 with the AES encryption algorithm option provides for non-broadcast

SSID and mutual authentication between the server and the end devices when accessing

systems containing State Street Data.

i. Malicious Code — Service Provider shall detect the introduction or intrusion of malicious code on

information systems handling or holding State Street Data and at no additional charge to State

Street prevent the unauthorized access, disclosure or loss of integrity of any State Street Data

and remove and eliminate any effects.

Information Classification: Limited Access

GPS# 180319755629459 29

MetricStream Confidential

11. Access Control

Authorized Access — Service Provider shall maintain the logical separation such that access to all

systems hosting State Street Data and/or being used to provide services to State Street will

uniquely identify each individual requiring access, grant access only to authorized personnel

based on the principle of least privileges, and prevent unauthorized access to State Street Data.

User Access Inventory — Service Provider shall maintain an accurate and up to date list of all

personnel who have access to the State Street Data and will have a process to promptly disable

within twenty-four (24) hours of transfer or termination access by any individual personnel.

Access No Longer Required — With respect to any Service Provider personnel who no longer

requires, or is no longer authorized for whatever reason to have, access to State Street Data,

where access is managed by State Street, Service Provider shall so notify State Street in writing

at least twenty-four (24) hours prior to the date on which such access is no longer required or

authorized; unless such access is removed under exigent circumstances such that twenty-four

(24) hours prior notice is not possible in which case Service Provider shall notify State Street

immediately upon knowledge that such access shall be removed. Notwithstanding the above,

Service Provider will immediately terminate access to State Street systems and premises by any

Service Provider personnel who is either removed or is no longer actively engaged in any State

Street assignment or if such personnel ceases to be an employee or Approved Subcontractor of

Service Provider. All State Street assets including any equipment, documentation or information

will be returned upon the termination of their assignment with State Street.

Authentication Credential Management — Service Provider shall communicate authentication

credentials to users in a secure manner, with an appropriate proof of identity check of the

intended users. Passwords shall not be stored or transmitted in readable form.

Logging & Monitoring — Service Provider shall log and monitor all access to the information

systems containing State Street Data for additions, alterations, deletions, and copying of State

Street Data. The Service Provider agrees to maintain full records or system or applicable access

attempts, both successful and failed and upon request will make available to State Street, all

logs and records. Security administration logs will be retained for a minimum of sixty (60) days

and financial transactions logs will be retained for a minimum of six (6) months.

Multi-Factor Authentication for Remote Access — Service Provider shall use multi factor

authentication and a secure tunnel when accessing systems containing State Street Data

remotely.

Single Sign On access for Internet Facing Applications —Service Provider shall provide SSO

integration with State Street’s authentication systems for all users of the GRC Application.

12. Use of Laptops and Mobile Devices

b.

Encryption Requirements — Service Provider shall encrypt any laptops or mobile devices (e.g.,

Blackberries, tablets) containing State Street used by Service Provider's personnel using an

industry recognized encryption algorithm with at least 256 bit encryption AES (or equivalent).

Secure Storage — Service Provider shall require that all laptops and mobile devices be securely

stored whenever out of the personnel’s immediate possession. In the event of a lost or stolen

Information Classification: Limited Access

GPS# 180319755629459 30

MetricStream Confidential

laptop or other mobile device containing State Street Data, Service Provider shall immediately

notify State Street’s Chief Information Security Officer or his designee.

Network/ Systems Password Storage — Service Provider shall prohibit use of laptops or other

mobile devices (e.g., Blackberries, tablets) to store network or system passwords that enable

access to State Street systems or other systems that handle or hold State Street Data, unless

such passwords are encrypted.

Remote Wipe/Inactivity Timeout — Service Provider shall employ access and password controls

as well as inactivity timeouts of no longer than thirty (30) minutes on all laptops, desktops and

mobile devices used by Service Provider’s personnel and maintain the ability to immediately

upon knowledge remotely remove State Street Data from any mobile device lost, stolen or in

possession of a terminated personnel.

Laptops/Mobile Devices — Service Provider shall prohibit access to State Street Data on laptops

or mobile devices where above requirements cannot be met.

13. Information Systems Acquisition Development and Maintenance

a.

Code Analysis — Any software owned or developed by the Service Provider shall, as part of

Service Provider's development lifecycle, undergo static code analysis using a commercial off-

the-shelf (COTS) tool to identify and remediate technical security vulnerabilities. Additionally,

such code will be examined by Service Provider’s independent third party for design flaws (such

as residual debug code) that could be used to circumvent implemented security controls, and/

or for the inclusion of code that could be used with malicious intent.

State Street Data — Must be used by the Service Provider solely for the purposes specified in

each applicable Agreement. Additionally:

i. No State Street production data shall be used for any other purpose (e.g., QA testing,

development testing, User Acceptance Test areas (UAT), training, demonstration, etc.)

unless otherwise expressly agreed in writing by State Street.

ii. In instances where State Street production data is copied to other environments as

authorized by State Street in writing, such State Street Data must be copied in a secured

manner and meet the controls specified within this Schedule. State Street Data must be

protected to the same level as is applied to the State Street production data or as

otherwise authorized by State Street (e.g. masked or obfuscated data).

iii. | Production environment must be a separate environment from any other non-

production environment (e.g., development, UAT, etc.).

Software Patching — Service Provider shall regularly update and patch of all computer software

on systems that handle or hold State Street Data, with patching for vulnerabilities rated ‘critical’

or ‘high’ applied within thirty (30) days of patch availability, unless other controls have been

applied that mitigate the vulnerability.

Virus and other Malware Management — Service Provider shall provide protection from viruses

and other malware (e.g. spyware, etc.) to Service Provider's systems that handle or hold State

Street Data (includes laptops and mobile devices), using the most recently distributed version of

software including virus signatures updated at least every twenty-four (24) hours.

Information Classification: Limited Access

GPS# 180319755629459 31

MetricStream

Confidential

14. Incident Event and Communications Management

a. Incident Management/Notification of Breach - Service Provider shall develop and implement

an approved incident response plan that specifies actions to be taken when the Service

Provider, one of its Approved Subcontractors, or State Street suspects or detects that a party

has gained unauthorized access to State Street Data or systems or applications containing any

State Street Data (the “Response Plan”).

b. Response Plan shall Include:

Hi.

Escalation Procedures — An escalation procedure includes notification to senior

managers and appropriate reporting to regulatory and law enforcement agencies. The

Service Provider shall immediately report to State Street’s Chief Information Security

Officer or his or her designee via telephone (U.S. & International: State Street Global

Security +1 (617) 985 8475) or email (State Street Global Security

csecurity@statestreet.com) (and provide a confirmatory notice in writing as soon as

practicable but in any event within forty-eight (48) hours) all incidents that may in any

way affect the operation of State Street or the confidentiality, availability or integrity of

State Street Data (including backed up data), including but not limited to, any successful

or attempted unauthorized access to systems or networks which contain or provide

access to the State Street Data; provided that the foregoing notice obligation is excused

for such period of time as Service Provider is prohibited by law enforcement agencies to

notify State Street.

Incident Reporting — Service Provider will promptly furnish to State Street full details

that the Service Provider has or may obtain regarding the general circumstances and

extent of such unauthorized access, including without limitation, the categories of State

Street personal data and the number and/or identities of the data subjects affected, as

well as any steps taken to secure the State Street Data and preserve information for any

necessary investigation.

Investigation & Prevention — Service Provider shall use reasonable efforts to assist State

Street in investigating or preventing the reoccurrence of any such access and shall: (A)

cooperate with the State Street in its efforts to comply with statutory notice or other

legal obligations applicable to State Street or its clients arising out of unauthorized

access or use and to seek injunctive or other equitable relief; (B) cooperate with State

Street in any litigation and investigation against third parties deemed reasonably

necessary by State Street to protect its proprietary rights; and (C) promptly take all

reasonable actions necessary to prevent a reoccurrence of and mitigate against loss

from any such authorized access.

In addition, in the event that Service Provider reports a security incident to SSBT and the

security incident results in SSBT opening a technical support case at the “critical” level,

then Service Provider will take the following measures unless otherwise agreed between

the Parties:

(a) Service Provider will assign one or more cloud support engineers, technical account

managers or similar personnel (the “Incident Responder”) to coordinate with SSBT,

monitor details of the security incident, investigate and diagnose SSBT concerns, and

work with Service Provider’s service subject matter experts in connection with the

security incident;

information Classification: Limited Access

GPS# 180319755629459 32

MetricStream Confidential

(b) Service Provider will use commercially reasonable efforts to have the Incident

Responder respond to SSBT’s technical support case as per MetricStream Support

Service Level Agreement; and

(c) If needed and appropriate, the Incident Responder will arrange for direct interaction

between Customer and Service Provider service subject matter experts in connection

with the security incident.

iv. Personnel Training and Confidentiality — Service Provider shall ensure that all personnel

fully understand the process and conditions under which they are required to invoke the

appropriate incident response. Service Provider shall maintain absolute confidentiality

regarding actual or suspected authorized possession, use or knowledge of State Street’s

Data or any other failure of Service Provider's security measures or non-compliance with

its security policies or procedures. Service Provider agrees to immediately discontinue

use of and access to State Street’s Data, if requested, for any security reasons cited by

State Street.

15. Limited Access

From time to time, State Street grants Service Provider personnel access to State Street facilities

subject to the terms of each applicable Agreement, in order to perform the services. With respect to

those engagements where Service Provider and its personnel do not require and shall not access

State Street Data to fulfill its Service obligations to State Street except while on State Street

facilities, the terms and conditions of this Appendix apply except that the following provisions shall

replace Sections 5 through 14 above:

With respect to any Service Provider personnel who no longer requires, or is no longer

authorized for whatever reason to have, access to State Street Data, where access is managed

by State Street, Service Provider shall so notify State Street in writing at least twenty-four (24)

hours prior to the date on which such access is no longer required or authorized; unless such

access is removed under exigent circumstances such that twenty-four (24) hours prior notice is

not possible in which case Service Provider shall notify State Street immediately upon

knowledge that such access shall be removed. Notwithstanding the above, Service Provider will

immediately terminate access to State Street systems and premises by any Service Provider

personnel who is either removed or is no longer actively engaged in any State Street assignment

or if such personnel ceases to be an employee or Approved Subcontractor of Service Provider.

All State Street assets including any equipment, documentation or information will be returned

upon the termination of their assignment with State Street.

b. Service Provider shall:

i. Promptly notify State Street if Service Provider identifies a gap in the security measures

implemented by State Street;

ii. | Promptly provide State Street with information regarding any failure of State Street's

security measures or any security breach related to State Street Data that Service

Provider becomes aware of in connection with its performance of the services at State

Street's facilities; and

iii. | Maintain absolute confidentiality regarding any such failure of such security measures

or any security.

Information Classification: Limited Access

GPS# 180319755629459 33

MetricStream Confidential

c.

State Street resources, including computers, software, proprietary information, and

telecommunications equipment will not be used for any activity not related to State Street

business. All assigned mobile devices that connect to State Street are in possession of Service

Provider's Personnel at all times or kept in a secured location. State Street network will only be

accessed through an approved connection (e.g., ASG, SSL VPN etc.).

Notwithstanding anything to the contrary contained in this Schedule or each applicable

Agreement generally, if at any time Service Provider is required to copy (in print, electronic or

other form), transport, transmit, transfer or otherwise move any State Street Data to carry out

its obligations under each applicable Agreement, it shall only do so if such printed or moved

State Street Data remains on State Street’s premises, and within State Street’s network, as

applicable, at all times. In no event shall any State Street Data be removed from State Street’s

premises or its network. For purposes of each applicable Agreement, any and all information

residing with the State Street network or accessed while on State Street premises shall be

considered to be State Street Data. Further, Service Provider personnel are prohibited from the

following activities:

i. Initiating or facilitating any unauthorized attempts to access State Street information

assets,

ii. Storing or sending of State Street Data or intellectual property to personal email

accounts or any other personal account including but not limited to cloud storage

account, any public location, social media sites, help forums or blogs,

iii, | Copying, downloading or storing of State Street Data or intellectual property to

removable data devices unless authorized and the device has been encrypted and

approved by State Street,

iv. Sharing of State Street credentials (user IDs and passwords) and/or tokens with anyone

or the use of State Street credentials for accounts other than State Street.

e. Service Provider personnel will complete required State Street information security training

within the specified timeframe.

16. Definitions and Guidance

For the purpose of this Schedule, the following Cloud Computing terms are defined according to

NIST Special Publication 800-145 (Revision September 2014):

Cloud computing is a mode! for enabling ubiquitous, convenient, on-demand network access to

a shared pool of configurable computing resources (e.g., networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal

management effort or service provider interaction.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's

applications running on a cloud infrastructure. The applications are accessible from various

client devices through either a thin client interface, such as a web browser (e.g., web-based

email), or a program interface. The consumer does not manage or control the underlying cloud

infrastructure including network, servers, operating systems, storage, or even individual

application capabilities, with the possible exception of limited user-specific application

configuration settings.

Platform as a Service (PaaS}. The capability provided to the consumer is to deploy onto the

cloud infrastructure consumer-created or acquired applications created using programming

Information Classification: Limited Access

GPS# 180319755629459 34

MetricStream Confidential

languages, libraries, services, and tools supported by the provider. The consumer does not

manage or control the underlying cloud infrastructure including network, servers, operating

systems, or storage, but has control over the deployed applications and possibly configuration

settings for the application-hosting environment.

Infrastructure as a Service (laaS). The capability provided to the consumer is to provision

processing, storage, networks, and other fundamental computing resources where the

consumer is able to deploy and run arbitrary software, which can include operating systems and

applications. The consumer does not manage or control the underlying cloud infrastructure but

has control over operating systems, storage, and deployed applications; and possibly limited

control of select networking components (e.g., host firewalls).

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization

comprising multiple consumers (e.g., business units). It may be owned, managed, and operated

by the organization, a third party, or some combination of them, and it may exist on or off

premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific

community of consumers from organizations that have shared concerns (e.g., mission, security

requirements, policy, and compliance considerations). It may be owned, managed, and operated

by one or more of the organizations in the community, a third party, or some combination of

them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public, It may

be owned, managed, and operated by a business, academic, or government organization, or

some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud

infrastructures (private, community, or public) that remain unique entities, but are bound

together by standardized or proprietary technology that enables data and application portability

(e.g., cloud bursting for load balancing between clouds).

b. For the purpose of this Schedule, the Penetration Testing terms defined as:

State Street Data Environment (SSDE) is defined as the people, processes, and technology that

store, process, or transmit State Street Data or sensitive authentication data.

Critical Systems are systems involved in the processing or protection of State Street Data. For

example, security systems, public-facing devices and systems, databases, and other systems that

store, process, or transmit State Street Data. However, for the purposes of a penetration test,

there may be additional systems outside the SSDE boundaries that could affect the security of

the SSDE. Common examples of critical systems relevant to a penetration test might include:

security systems (for example, firewalls, intrusion-detection systems/intrusion-prevention

systems (IDS/IPS), authentication servers, etc.), or any assets utilized by privileged users to

support and manage the SSDE.

The following guidance applies to Penetration Testing scope:

i. The scope of an external penetration test is the exposed external perimeter of the SSDE

and critical systems connected or accessible to public network infrastructures. It should

assess any unique access to the scope from the public networks, including services that

have access restricted to individual external IP addresses. Testing must include both

application-layer and network-layer assessments. External penetration tests also include

remote access vectors such as dial-up and VPN connections.

Information Classification: Limited Access

GPS# 180319755629459 35

MetricStream Confidential

ii. | The scope of the internal penetration test is the internal perimeter of the SSDE from the

perspective of any out-of-scope LAN segment that has access to a unique type of attack

on the SSDE perimeter. Critical systems or those systems that may impact the security of

the SSDE should also be included in the scope. Testing must include both application-

layer and network-layer assessments.

iii, If segmentation controls have been implemented to separate environments,

segmentation checks should be performed from any non-SSDE environment that is

intended to be completely segmented from the SSDE perimeter. The intent of this

assessment is to validate the effectiveness of the segmentation controls separating the

non-SSDE environments from the SSDE and ensure the controls are operational.

iv. To be considered out of scope of SSDE penetration test, a system component must be

isolated (segmented) from the SSDE, such that even if the out-of-scope system

component was compromised it could not impact the security of the SSDE. Therefore,

the penetration test may include systems not directly related to the processing,

transmission or storage of State Street Data to ensure these assets, if compromised,

could not impact the security of the SSDE.

if access to the SSDE is obtained as a result of the testing, it is recommended to continue exploring

inside the network and further the attack against other systems within the CDE, and also include testing

any data-exfiltration prevention (data-loss prevention) controls that are in place.

Information Classification: Limited Access

GPS# 180319755629459 36

MetricStream Confidential

Appendix B

Vendor Management, Subcontractors, Personnel Management, Privacy, and Compliance.

1. Vendor Management Program

Service Provider agrees to participate in State Street’s vendor management program including

completing State Street’s vendor risk assessment questionnaire(s) when requested by State Street.

Requests by State Street will be no more frequent than once in any twelve (12) month period for

any services provided to State Street. Service Provider also agrees to make appropriate resources

available for follow-up phone review(s) of the questionnaire or, if requested by State Street, for an

onsite visit.

2. Subcontractors

Service Provider shall not delegate any services to be performed under each applicable Agreement

or provide any access to State Street Data or its network to a subcontractor or other third party

except to a subcontractor approved by State Street as provided herein (“Approved Subcontractor”)

who complies with the security measures at least as stringent as those described in this Schedule.

An “Approved Subcontractor” means each Service Provider's subcontractor required by the terms

herein to be approved by State Street in writing prior to performing services for State Street or

having access to State Street Data. Service Provider shall provide State Street with sufficient

information regarding each proposed subcontractor to whom Service Provider intends to either

delegate performance of all or part of the services or provide access to State Street confidential

information and/or State Street systems in order to enable State Street to determine whether State

Street can approve, in writing prior to performing services or accessing State Street confidential

information, such subcontractor-as an Approved Subcontractor. A list of Service Provider Approved

Subcontractors as of the date of this Schedule is attached hereto as Attachment 1. If Service

Provider desires to add an Approved Subcontractor to Attachment 1, Service Provider shall so notify

State Street and provide it with sufficient information to enable State Street to determine whether

or not it can consent to, in writing prior to performing services or accessing State Street confidential

information, the appointment of such subcontractor as an Approved Subcontractor. Service Provider

shall engage all subcontractors performing or supporting services hereunder pursuant to contracts

that contain or are consistent in all material respects with the provisions of applicable Agreement.

Where a subcontractor or an Approved Subcontractor processes State Street personal data, Service

Provider shall ensure that the subcontractor is bound by data processing terms at least as stringent

as those contained in the Data Processing Addendum in Attachment 2. Upon State Street's request,

Service Provider shall promptly provide State Street with a copy of the written agreement (or to the

extent permitted by law, summaries thereof) and any updates thereof, which it has with each

Approved Subcontractor having access to State Street Data. Service Provider shall remain

responsible and liable for the acts and omissions of any subcontractor to the same extent as if such

acts and omissions were performed or not performed, as the case may be, by Service Provider,

regardless of whether State Street has exercised its right to reject or approve State Street's use of

any proposed subcontractor, as applicable.

Information Classification: Limited Access

GPS# 180319755629459 37

MetricStream Confidential

Service Provider must at any given time, in writing, be able to identify any sub-contractors and sub-

processors that participate in the data processing, the chain of accountability and approach used to

ensure that data protection requirements are fulfilled.

Service Provider must at any given time, in writing, be able to identify the procedures used to inform

State Street of any intended changes concerning the addition or replacement of sub-contractors,

cloud providers or cloud sub-processors with State Street retaining at all times the possibility to

object to such changes or to terminate the applicable Agreement.

3. Background Check and Security Clearance

a.

Service Provider’s Personnel who access State Street's facilities or systems are subject to certain

credit and criminal checks conducted by State Street or its agents (“Security Clearance”)

applicable to banks pursuant to banking regulations by State Street. If any person does not pass

State Street’s Security Clearance, Service Provider shall remove such person from the

assignment. Service Provider is responsible for informing and receiving the consent of its

assigned personnel that a Security Clearance including, without limitation, fingerprinting,

identification picture for badge, and the signing of a security form and confidentiality

agreement, will be required.

Service Provider’s assigned personnel shall comply with the State Street's policies and rules,

including those relating to facilities access, systems access operating standards and procedures,

user identification and password controls, corporate information, security and data protection

and privacy, as in effect from time to time as a condition to being provided access to State

Street’s premises, systems or State Street Data. Service Provider will not, and will ensure that

Service Provider personne! do not, break, bypass, or circumvent, or attempt to break, bypass or

circumvent, any security system of State Street, or obtain, or attempt to obtain, access to any

State Street Data other than as allowed by State Street in compliance with this Schedule.

Service Provider represents and warrants that, as part of its standard hiring and vendor due

diligence practices, Service Provider personnel assigned to perform the services or otherwise

having access to State Street Data shall be subject to appropriate pre-employment background

investigations performed by or on behalf of Service Provider consistent with industry standards

taking into consideration the confidential nature of the services to be performed and the risk

and severity of damage to State Street or others that might result from its personnel’s

negligence or wrongful conduct. Service Provider shall make available, upon request from State

Street, evidence (such as invoices for services) that will not pose a privacy issue that the

background investigations have been performed on such personnel.

4. Physical Security

a.

Securing Physical Facilities - Service Provider shall maintain all systems hosting State Street

Data and/or providing services on behalf of State Street in a physically secure environment that

restricts access to only authorized individuals, detects any unauthorized access or access

attempts, and reports incidents and non-conformance of security policy to management. A

secure environment includes 24x7 security personnel governance or equivalent means of

monitoring of controls for all relevant locations (including, without limitation, buildings,

computer facilities, and records storage facilities).

Information Classification: Limited Access

GPS# 180319755629459 38

MetricStream

Confidential

b. Secure Physical Processing Locations — Service Provider shall keep an up-to-date record of the

location of each data center used in connection with the provisions of services and the owner of

such data center and shall provide such record to State Street upon request. Further Service

Provider shall promptly notify State Street of any transfer or relocation of material portions of

State Street Data.

5. Personal Data

a. Compliance — To the extent applicable, Service Provider will retain, handle, process, host, have

access to and/or otherwise use any personal data contained within the State Street Data

perform its obligations hereunder in a manner that complies with all applicable laws, rules,

regulations, ordinances, directives, decisions and codes, including, without limitation, relevant

data protection and privacy laws.

b. Global Data Protection and Privacy

When processing State Street personal data, Service Provider shall comply with the

terms of and complete and execute a Data Processing Addendum substantially in the

form of Attachment 2 (“Data Processing Addendum”), which agreement, together with

the terms of this Agreement, will govern the processing of any and all State Street

personal data in connection with the Services. Where the Service Provider processes or

transfers any State Street personal data outside of the European Economic Area (“EEA”),

Service Provider agrees to execute the European Commission Contractual Clauses with

the relevant State Street entity as set out in the Data Processing Addendum.

For avoidance of doubt, this Schedule shall apply to the processing of any State Street

personal data, irrespective of which jurisdiction the data subject resides and

notwithstanding the fact that the Service Provider has executed the Data Processing

Addendum.

To the extent that it is determined by any data protection authority that this Agreement

or the Data Processing Addendum is insufficient to comply with the applicable data

protection and privacy laws of to the extent required otherwise by any changes in the

applicable data protection and privacy laws or the enactment of new data protection

and privacy laws during the Term, the Parties agree to work cooperatively and in good

faith to amend this Agreement or execute Data Processing Addenda, if any, in a

mutually agreeable and timely manner or to enter into further mutually agreeable data

processing addenda in an effort to comply with any data protection and privacy laws

applicable to the Parties.

Service Provider shall take such actions, without further consideration and at Service

Provider's expense, necessary to protect State Street personal data against

unauthorized or unlawful processing and accidental or intentional loss, destruction or

damage as are appropriate to State Street as data controller or owner of the State

Street personal data and/or satisfy within a timely manner requests or requirements of

relevant governmental or data protection regulatory authorities, provided that Service

Provider shall not be obliged to take any measures higher than that required by law,

without additional charge to State Street.

State Street shall have the responsibility to notify all its employees, contingent workers

or participants as may be required by applicable data protection and privacy laws of the

collection and intended usage of their personal data. Service Provider shall provide State

Street with any and all information, including applicable State Street personal data,

Information Classification: Limited Access

GPS# 180319755629459 39

MetricStream Confidential

which State Street requires to respond, in a timely manner and in compliance with

applicable data protection and privacy laws, to any inquiries, notices, claims or demands

brought by a data subject in connection with the usage of their personal data.

vi. | Upon the request of State Street or one of its Related Companies, Service Provider shall

(i) enter into additional Data Processing Addenda as State Street may require, and (ii)

use reasonable efforts to cooperate in connection with the preparation of the additional

Data Processing Addenda and any required annexes to such additional Data Processing

Addenda, including providing any additional information requested by the relevant data

protection authorities within the period of time specified by such authorities, or, if no

time period is specified by the applicable data protection authorities, within a

reasonable time.

vil. Service Provider acknowledges that to the extent that it maintains or has access to

certain State Street personal data of Massachusetts residents, Service Provider is

obligated to comply with the Massachusetts Office of Consumer Affairs and Business

Regulation standards for the protection of personal information of Massachusetts

residents, 201 CMR 17.00 (“Standards”). Service Provider certifies that for so long as it

has State Street personal data of Massachusetts residents thereafter and to the extent

that the Standards are applicable to the Services that Service Provider provides

hereunder, Service Provider shall maintain information security safeguards and protect

such State Street personal data in compliance with the Standards and that it shall notify

State Street in writing immediately if it is no longer in compliance with the Standards.

Service Provider further certifies to State Street that it has a written information

security program in compliance with the Standards.

c. “Special” Personal Data Processing. Service Provider shall provide enhanced controls for

“special” categories of State Street personal data when requested by State Street, including but

not limited to encryption at rest and during transmission.

6. Preparation of Examination Reports

In accordance with Appendix A Section 5(e) above, Service Provider shall, upon State Street’s

request and at its sole expense, engage its independent outside accounting firm to prepare certain

periodic Service Organization Control! Reports (“Examination Reports”) in accordance with the

standards of the American Institute of Certified Public Accountants (“AICPA”), or any successor U.S.

standards or guidelines to the same or analogous standards or guidelines in non-US. jurisdictions

(collectively, “Auditing Standards”), evaluating the Services performed by Service Provider (to the

extent that the Auditing Standards contemplates the evaluation of such Services). Service Provider

represents and warrants that it shall promptly provide State Street with true and correct copies of

any Examination Reports prepared pursuant to this Section and agrees that it will promptly remedy

any shortcomings disclosed in any Examination Reports and implement any reasonable

recommendations contained therein as to such shortcomings. To the extent compliance with the

Auditing Standards requires, or the Parties reasonably mutually agree on, the joint preparation of

the Examination Reports evaluating the Services performed by Service Provider, State Street shall,

and shall cause its independent outside accounting firm to, cooperate in good faith with Service

Provider and its independent outside accounting firm to jointly prepare such Examination Reports

and the Parties shall each pay their respective costs of such preparation.

Information Classification: Limited Access

GPS# 180319755629459 40

MetricStream Confidential

7. Audit Rights

Service Provider shall permit one or more State Street personnel or agents (including State Street's

internal or external auditors and such governmental and data protection authorities governing State

Street), at such times as shall be requested, at least 60 days in advance and once annually, to inspect

and take extracts from any records (redacted to remove references to matters unrelated to the

materials or services under each applicable Agreement) maintained by Service Provider or its

subcontractors in connection with each applicable Agreement and to visit and inspect any premises

where services are being performed (including, as applicable, walk-through of primary and backup

data centers, subject to generally-applicable restrictions imposed by any third party operators of

such data centers) to verify that Service Provider is employing reasonable procedures in compliance

with the terms of this Schedule including without limitation as to confidentiality and data security

obligations hereunder. At State Street’s request, Service Provider shall provide State Street or its

personnel or agents with any reports of Service Provider's internal and external auditors in

connection with Service Provider’s system of internal accounting controls as they relate to Service

Provider’s controls and security requirements and the services provided under each applicable

Agreement (redacted to remove references to matters unrelated to such services) and remedial plan

to address any deficiencies set out in the report.

Information Classification: Limited Access

GPS# 180319755629459 4

MetricStream Confidential

Exhibit E

Data Privacy Addendum

DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM (“Addendum”) supplements, amends and forms part of the Cloud

Services Agreement (“Principal Agreement(s)”) previously entered into between STATE STREET BANK

AND TRUST COMPANY (“State Street”) acting on its own behalf and as agent for each State Street

Affiliate and METRICSTREAM, INC. (“Service Provider’) acting on its own behalf and as agent for each

Service Provider Affiliate.

Except as modified below, the terms of the Principal Agreement(s) shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and

conditions set out below shall be added as an Addendum to the Principal Agreement(s) with effect from

25 May 2018 (“Addendum Effective Date”). Except where the context requires otherwise, references in

this Addendum to the Principal Agreement(s) are to the Principal Agreement(s) as amended by, and

including, this Addendum.

1. DEFINITIONS AND INTERPRETATION

1.1. For purposes of this Addendum only, the following terms shall have the meanings set out below

and any other capitalised terms not defined herein shall retain the meaning ascribed to them in

the Principal Agreement(s):

(a) “Affiliate” means, in relation to either State Street or Service Provider, an entity that

owns or controls, is owned or controlled by or is under common control or ownership

with State Street or Service Provider (as applicable), where control is defined as the

possession, directly or indirectly, of the power to direct or cause the direction of the

management and policies of an entity, whether through ownership of voting securities,

by contract or otherwise;

(b) “Applicable Laws” means:

{i) European Union or Member State laws with respect to any State Street Personal

Data in respect of which any State Street Group Member is subject to Data

Protection Laws; and

(i) any other applicable law with respect to any State Street Personal Data in

respect of which any State Street Group Member is subject to any other Data

Protection Laws;

(c) “Contracted Processor” means Service Provider or a Sub-processor;

(d) “Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic

legislation of each Member State and as amended, replaced or superseded from time to

time, including by the EU General Data Protection Regulation 2016/679 (“GDPR”) and

laws implementing or supplementing the GDPR and any data protection laws

Information Classification: Limited Access

GPS# 180319755629459 42

MetricStream Confidential

1.2.

1.3.

1.4.

substantially amending, replacing or superseding the GDPR following any exit by the

United Kingdom from the European Union, and to the extent applicable, the data

protection or privacy laws of any other country;

(e) “Restricted Transfer” means:

(i) a transfer of State Street Personal Data from any State Street Group Member to

a Contracted Processor; or

(ii) an onward transfer of State Street Personal Data from a Contracted Processor to

a Contracted Processor, or between two establishments of a Contracted

Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by

the terms of data transfer agreements put in place to address the data transfer

restrictions of Data Protection Laws) in the absence of the appropriate safeguards as set

forth in article 46 of the GDPR;

(f) “Services” means the services and other activities to be supplied to or carried out by or

on behalf of Service Provider for State Street Group Members pursuant to the Principal

Agreement(s);

(g) “Standard Contractual Clauses” means the contractual clauses set out in Decision of the

Commission of the European Union 2010/87/EU between Data Controller and Data

Processor (or any replacement European Commission standard contractual clauses from

time to time);

(h) “State Street Group Member” means State Street or any State Street Affiliate;

(i) “State Street Personal Data” means any Personal Data processed by a Contracted

Processor on behalf of a State Street Group Member pursuant to or in connection with

the Principal Agreement(s); and

{j) “Sub-processor” means any person (including any third party and any Service Provider

Affiliate, but excluding an employee of Service Provider or any of its sub-contractors)

appointed by or on behalf of Service Provider or any Service Provider Affiliate to process

Personal Data on behalf of any State Street Group Member in connection with the

Principal Agreement(s).

The terms “Controller”, “Data Subject’, “Personal Data’, “Personal Data Breach”,

“process/processing”, “Processor” and “Supervisory Authority” shall have the same meaning as

in article 4 of the GDPR. The words “include/including” shall be construed to mean include

without limitation.

In this Addendum a reference to a section is to a section to this Addendum unless otherwise

stated.

For the purposes of the Principal Agreement(s) and this Addendum, State Street shall act as a

Controller and Service Provider shall act as a Processor,

Information Classification: Limited Access

GPS# 180319755629459 43

MetricStream Confidential

3.1,

3.2.

3.3.

4.1.

AUTHORISATION

Service Provider warrants and represents that Service Provider is duly authorised (or

subsequently ratified) to enter into this Addendum for and on behalf of any Service Provider

Affiliate who processes any State Street Personal Data before any such Service Provider Affiliate

commences with the processing of the State Street Personal Data on behalf of any State Street

Group Member.

DATA PROCESSING

Service Provider and each Service Provider Affiliate shall and shall procure that each Sub-

processor shall:

{a) comply with all applicable Data Protection Laws when processing State Street Personal

Data; and

(b) only process State Street Personal Data in accordance with the relevant State Street

Group Member's documented instructions unless processing is required by Applicable

Laws to which the relevant Service Provider (or Service Provider Affiliate) is subject, in

which case Service Provider or the relevant Service Provider Affiliate shall inform the

relevant State Street Group Member of that legal requirement before the relevant

processing of that Personal Data.

State Street shall instruct Service Provider and each Service Provider Affiliate (and authorise

Service Provider and each Service Provider Affiliate to instruct each Sub-processor) to:

(a) process State Street Personal Data; and

(b) transfer State Street Personal Data to any country or territory in accordance with

section 4,

as reasonably necessary for the provision of the Services and consistent with the Principal

Agreement(s).

State Street is duly and effectively authorised to give the instruction set out in section 3.2 on

behalf of itself and each relevant State Street Affiliate.

Appendix 1 to this Addendum details certain information regarding the Contracted Processors’

Processing of the State Street Personal Data as required by article 28(3) of the GDPR. State

Street may make reasonable amendments to Appendix 1 by written notice to Service Provider

from time to time as State Street reasonably considers necessary to ensure its compliance with

its obligations under the GDPR. Nothing in Appendix 1 (including as amended in accordance with

this section 3.4) shall confer any right or impose any obligation on any party to this Addendum.

INTERNATIONAL TRANSFERS

Subject to section 4.3, each State Street Group Member (as “data exporter’) and Service

Provider and each Service Provider Affiliate, as appropriate, (as “data importer’) hereby enter

into the Standard Contractual Clauses set out in Appendix 4 to this Addendum in respect to any

Information Classification: Limited Access

GPS# 180319755629459 44

MetricStream Confidential

4.2.

4.3.

4.4,

4.5.

5.1.

5.2.

Restricted Transfer from that State Street Group Member to that Service Provider or Service

Provider Affiliate.

The Standard Contractual Clauses shall come into effect under section 4.1 on the later of:

{a) the data exporter becoming a party to them;

(b) the data importer becoming a party to ‘them; and

(c) commencement of a Restricted Transfer.

Section 4.1 shall not apply to a Restricted Transfer unless its effect, together with other

reasonably practicable compliance steps (which, for the avoidance of doubt, do not include

obtaining consents from Data Subjects), is to allow the Restricted Transfer to take place without

breach of applicable Data Protection Laws.

Additional terms for Standard Contractual Clauses in effect under section 4,1:

{a) for the purposes of Section 5(a) of the Standard Contractual Clauses, the processing

described in section 3 is deemed an instruction by State Street to process State Street

Personal Data, subject to Service Provider and each Service Provider Affiliate’s

compliance with applicable Data Protection Laws; and

(b) pursuant to Section 5(h) of the Standard Contractual Clauses, State Street agrees that

Service Provider and each Service Provider Affiliate may engage new Sub-processors as

detailed in section 7.

State Street agrees that the copies of the Sub-processor agreements that Service Provider and

each Service Provider Affiliate must send to State Street pursuant to Section 5(j) of the Standard

Contractual Clauses may be redacted to remove confidential commercial information not

relevant to the requirements of this Addendum, and Service Provider and each Service Provider

Affiliate will provide such copies to State Street only upon State Street’s written request.

TECHNICAL AND ORGANISATIONAL MEASURES AND SECURITY

Taking into account the state of the art, the costs of implementation and the nature, scope,

context and purposes of processing as well as the risk of varying likelihood and severity for the

rights and freedoms of natural persons, Service Provider shall and shall procure that each

Contracted Processor shall implement and maintain, appropriate technical and organisational

measures in relation to the processing of Personal Data by Service Provider or Contracted

Processor to ensure a level of security appropriate to that risk including, as appropriate, the

measures referred to in article 32 of the GDPR and Appendix 2 to this Addendum.

In assessing the appropriate level of security, Service Provider shall take into account all risks

that are presented by processing the relevant Personal Data, in particular from a Personal Data

Breach.

Information Classification: Limited Access

GPS# 180319755629459 45

MetricStream Confidential

7.1,

7.2,

7.3,

74.

SERVICE PROVIDER PERSONNEL

Without limitation of any obligation under the Principal Agreement(s), Service Provider

undertakes that it and each Service Provider Affiliate shall take all reasonable steps to ensure

the reliability of any employee, agent or contractor of any Contracted Processor who may have

access to the State Street Personal Data, ensuring that all such individuals are subject to

confidentiality undertakings or professional or statutory obligations of confidentiality, and

ensuring in each case that access is strictly limited to those individuals who need to know/access

the relevant State Street Personal Data, as strictly necessary for the purposes of the Principal

Agreement(s), and to comply with Applicable Laws in the context of that individual's duties to

the Contracted Processor.

SUB-PROCESSING

To the extent strictly necessary, State Street authorises Service Provider and each Service

Provider Affiliate to appoint further Sub-processors in accordance with this section 7 and any

other restrictions in the Principal Agreement(s).

Service Provider and each Service Provider Affiliate may continue to use those Sub-processors

already engaged by Service Provider or any Service Provider Affiliate as at the Addendum

Effective Date as listed in Appendix 3 to this Addendum, subject to Service Provider and each

Service Provider Affiliate in each case as soon as practicable meeting the obligations set out in

section 7.4.

Service Provider shall give State Street prior written notice of the intended appointment of any

new Sub-processor, including full details of the processing to be undertaken by the Sub-

processor. If, within one month of receipt of that notice, State Street or a State Street Affiliate

notifies Service Provider in writing of any reasonable objections to the intended appointment

neither Service Provider nor any Service Provider Affiliate shall appoint (or disclose any State

Street Personal Data to) that proposed Sub-processor until State Street or a State Street Affiliate

and the Service Provider have agreed on reasonable steps to address the objections raised by

State Street or a State Street Affiliate and State Street has been provided with a reasonable

written explanation of the steps to be taken. In the event that no such reasonable steps can be

agreed between State Street or a State Street Affiliate and the Service Provider and where such

a change cannot be made within one month from Service Provider's receipt of State Street or

the State Street Affiliate’s notice, notwithstanding anything in the Principal Agreement(s), State

Street may by written notice to Service Provider with immediate effect terminate the Principal

Agreement(s) to the extent that it relates to the Services which require the use of the proposed

Sub-processor.

With respect to each Sub-processor, Service Provider or the relevant Service Provider Affiliate

shall:

{a) before the Sub-processor first processes State Street Personal Data (or, where relevant,

in accordance with section 7.2), carry out adequate due diligence to ensure that the

Sub-processor is capable of providing the level of protection for State Street Personal

Data required by the Principal Agreement(s);

Information Classification: Limited Access

GPS# 180319755629459 46

MetricStream Confidential

75,

8.1.

8.2.

(b) ensure that the arrangement between the (i) Service Provider, or (ii) the relevant

Service Provider Affiliate, or (iii) the relevant intermediate Sub-processor; and the Sub-

processor, is governed by a written contract including terms which offer at least the

same level of protection for State Street Personal Data as those set out in this

Addendum and meet the requirements of article 28(3) of the GDPR;

(c) if that arrangement involves a Restricted Transfer, ensure that appropriate safeguards

are in place under article 46(2) of the GDPR. If the appropriate safeguard is adoption of

the Standard Contractual Clauses, ensure that the Standard Contractual Clauses are at

all relevant times incorporated into the agreement between (i) Service Provider, or (ii)

the relevant Service Provider Affiliate, or (iii) the relevant intermediate Sub-processor,;

and the Sub-processor, or before the Sub-processor first processes State Street Personal

Data procure that it enters into an agreement incorporating the Standard Contractual

Clauses with the relevant State Street Group Member(s) (and State Street shall procure

that each State Street Group Member party to any such Standard Contractual Clauses

co-operates with their population and execution); and

{d) provide to State Street for review such copies of the Contracted Processors’ agreements

with Sub-processors (which may be redacted to remove confidential commercial

information not relevant to the requirements of this Addendum) as State Street may

request from time to time.

Service Provider and each Service Provider Affiliate shall ensure that each Sub-processor

performs the obligations under sections 3.1, 5, 6, 8.1, 9.3, 10 and 12.2, as they apply to

Processing of State Street Personal Data carried out by that Sub-processor, as if it were party to

this Addendum in place of Service Provider.

DATA SUBJECT RIGHTS

Service Provider and each Service Provider Affiliate shall assist each State Street Group Member

by implementing appropriate technical and organisational measures, insofar as this is possible,

for the fulfilment of the State Street Group Members’ obligations, as reasonably understood by

State Street, to respond to requests to exercise Data Subject rights under the Data Protection

Laws.

Service Provider shall:

(a) promptly notify State Street if any Contracted Processor receives a request from a Data

Subject under any Data Protection Law in respect of State Street Personal Data; and

(b) ensure that the Contracted Processor does not respond to that request except on the

documented instructions of State Street or the relevant State Street Affiliate or as

required by Applicable Laws to which the Contracted Processor is subject, in which case

Service Provider shall to the extent permitted by Applicable Laws inform State Street of

that legal requirement before the Contracted Processor responds to the request.

Information Classification: Limited Access

GPS# 180319755629459 47

MetricStream Confidential

9.1.

9.2.

9.3.

10.

PERSONAL DATA BREACH

in respect of any Personal Data Breach, the Service Provider shall:

(a) notify State Street of the Personal Data Breach without undue delay upon becoming

aware of the Personal Data Breach; and

(b) provide State Street without undue delay (wherever possible, no later than twenty four

(24) hours after becoming aware of the Personal Data Breach) with such details as State

Street reasonably requires regarding:

(i) the nature of the Personal Data Breach, including the categories and

approximate numbers of Data Subjects and Personal Data records concerned;

(ii) any investigations into such Personal Data Breach;

(iii) the likely consequences of the Personal Data Breach; and

(iv) any measures taken, or that the Service Provider recommends, to address such

Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if Service Provider cannot

provide all these details within such timeframes, it shall (before the end of this

timeframe) provide State Street with reasons for the delay and when it expects to be

able to provide the relevant details (which may be phased), and give State Street regular

updates on these matters.

Service Provider shall promptly (and in any event within two (2) business days) inform State

Street if it receives a complaint or request relating to either party’s obligations under Data

Protection Laws relevant to this Addendum, including any compensation claim from a Data

Subject or any notice, investigation or other action from a Supervisory Authority and provide

State Street with full details of such complaint.

Service Provider shall co-operate with State Street and each State Street Group Member and

take such reasonable commercial steps as are directed by State Street to assist in the

investigation, mitigation and remediation of each such Personal Data Breach.

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

VAAL FA ee NN cv aE a ee SS ee eee awe’

Service Provider and each Service Provider Affiliate shall provide reasonable assistance to each

State Street Group Member with any data protection impact assessments, and prior

consultations with Supervising Authorities or other competent data privacy authorities, which

State Street reasonably considers to be required of any State Street Group Member by article 35

or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely

in relation to processing of State Street Personal Data by, and taking into account the nature of

the processing and information available to, the Contracted Processors.

Information Classification: Limited Access

GPS# 180319755629459 48

MetricStream Confidential

11.

11.1,

11.2.

11.3.

12.

12.1.

12.2.

DELETION OR RETURN OF STATE STREET PERSONAL DATA

Lb Le ee Ee OOOO

Service Provider shall without delay, at State Street’s written request, either securely delete or

securely return all the Personal Data to State Street in such form as State Street reasonably

requests after the earlier of:

(a) the end of the provision of the relevant Services related to processing; or

(b) once processing by Service Provider of any Personal Data is no longer required for the

purpose of the Service Provider's performance of its relevant obligations under this

Addendum,

and securely delete existing copies (unless storage of any data is required by Applicable Law

and, if so, Service Provider shall inform State Street of any such requirement).

Each Contracted Processor may retain State Street Personal Data to the extent required by

Applicable Laws and only to the extent and for such period as required by Applicable Laws and

always provided that Service Provider and each Service Provider Affiliate shall ensure the

confidentiality of all such State Street Personal Data and shall ensure that such State Street

Personal Data is only processed as necessary for the purpose(s) specified in the Applicable Laws

requiring its storage and for no other purpose.

Service Provider shall provide written certification to State Street that it and each Service

Provider Affiliate has fully complied with this section 11.

AUDIT RIGHTS

Without limiting any other right of State Street under the Principal Agreement(s), Service

Provider shall maintain complete, accurate and up to date written records of all categories of

processing activities carried out on behalf of State Street, containing such information as State

Street may reasonably require, including:

(a) the name and contact details of Service Provider’s representative and data protection

officer (if any);

(b) the categories of processing carried out on behalf of State Street and each State Street

Group Member;

{c) where applicable, details of transfers of Personal Data to a third country or an

international organisation; and

(d) a general description of the technical and organisational security measures referred to

in section 5.1.

Service Provider shall make available to State Street on request in a timely manner (and in any

event within three (3) business days):

(a) copies of the records under section 12.1; and

information Classification: Limited Access

GPS# 180319755629459 49

MetricStream Confidential

12.3.

12.4.

12.5.

13.

13.1.

13.2.

(b) such other information as State Street reasonably requires to demonstrate Service

Provider's compliance with its obligations under Data Protection Laws and this

Addendum.

Service Provider shall at no cost to State Street:

(a) allow for and contribute to audits, including inspections, conducted by State Street or

another auditor mandated by State Street for the purpose of demonstrating compliance

by Service Provider with its obligations under Data Protection Laws and this Addendum;

and

(b) provide (and procure) reasonable access for State Street or such other auditor (where

practicable, during normal business hours) to:

(i) the facilities, equipment, premises and sites on which Personal Data and/or the

records referred to in section 12.1 are held, and to any other equipment or

facilities used in the provision of the Services (in each case whether or not

owned or controlled by Service Provider); and

(ii) to Service Provider Personnel,

provided that State Street gives Service Provider reasonable prior notice of such audit

and/or inspection.

Service Provider shall promptly resolve, at its own cost and expense, all data protection and

security issues discovered by State Street and reported to Service Provider that reveal a breach

or potential breach by Service Provider of its obligations under this Addendum.

State Street shall be entitled to share any notification, details, records or information provided

by or on behalf of Service Provider under this Addendum with any State Street Group Member,

its professional advisors and/or any Supervisory Authority.

GENERAL TERMS

Governing law and jurisdiction.

(a) The Parties to this Addendum hereby submit to the choice of jurisdiction stipulated in

the Principal Agreement(s) with respect to any disputes or claims howsoever arising

under this Addendum, including disputes regarding its existence, validity or termination

or the consequences of its nullity.

(b) This Addendum and all non-contractual or other obligations arising out of or in

connection with it are governed by the saws of the country or territory stipulated for this

purpose in the Principal Agreement(s).

Order of precedence.

(a) Nothing in this Addendum shall reduce Service Provider's or any Service Provider

Affiliate’s obligations under the Principal Agreement(s) in relation to the protection of

Information Classification: Limited Access

GPS# 180319755629459 . 50

MetricStream

13.3.

13.4.

{b)

Confidential

Personal Data or permits Service Provider or any Service Provider Affiliate to process (or

permit the processing of) Personal Data in a manner which is prohibited by the Principal

Agreement(s). In the event of any conflict or inconsistency between this Addendum and

the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

Subject to section 13.2(a), with regard to the subject matter of this Addendum, in the

event of inconsistencies between the provisions of this Addendum and any other

agreements between the Parties, including the Principal Agreement(s) and including

(except where explicitly agreed otherwise in writing, signed on behalf of the Parties)

agreements entered into or purported to be entered into after the Addendum Effective

Date, the provisions of this Addendum shail prevail.

Changes in Data Protection Laws, etc.

(a)

(b)

(c)

(d)

State Street may:

(i) by at least sixty (60) calendar days’ written notice to Service Provider from time

to time make any variations to the Standard Contractual Clauses, as they apply

to Restricted Transfers which are subject to a particular Data Protection Law,

which are required, as a result of any change in, or decision of a competent

authority under, that Data Protection Law, to allow those Restricted Transfers to

be made (or continue to be made) without breach of that Data Protection Law;

and

(ii) propose any other variations to this Addendum which State Street reasonably

considers to be necessary to address the requirements of any Data Protection

Law.

lf State Street gives notice under section 13.3{a)(i) State Street shall not unreasonably

withhold or delay agreement to any consequential variations to this Addendum

proposed by Service Provider to protect the Contracted Processors against additional

risks associated with the variations made under section 13.3(a)(i).

if State Street gives notice under section 13.3(a)(ii), the Parties shall promptly discuss

the proposed variations and negotiate in good faith with a view to agreeing and

implementing those or alternative variations designed to address the requirements

identified in State Street's notice as soon as is reasonably practicable.

Neither State Street nor Service Provider shall require the consent or approval of any

State Street Affiliate or Service Provider Affiliate to amend this Addendum pursuant to

this section 13 or otherwise.

Severance. Should any provision of this Addendum be invalid or unenforceable, then the

remainder of this Addendum shall remain valid and in force. The invalid or unenforceable

provision shall be either (i) amended as necessary to ensure its validity and enforceability, while

preserving the Parties’ intentions as closely as possible or, if this is not possible, (ii) construed in

a manner as if the invalid or unenforceable part had never been contained therein.

Information Classification: Limited Access

GPS# 180319755629459 54

MetricStream Confidential

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal

Agreement(s) with effect from the Addendum Effective Date.

METRICSTREAM, INC, STATE STREET BANK AND TRUST COMPANY

iy ~ ae - Y. \_f fp .

By: —————— By, “271 ¢¢ <4 4.

name: Michec.. Meh

Title: AV Oe Crh. ff Nl for

Information Classification: Limited Access

GPS# 180319755629459 §2

MetricStream Confidential

APPENDIX 1

DATA PROCESSING DETAILS

This Appendix includes certain details of the processing of Personal Data as required by article 28(3) of

the GDPR.

Information Classification: Limited Access

GPS# 180319755629459 53

MetricStream Confidential

Subject Matter of | The performance of the services documented in the Principal Agreement(s).

processing

Duration of | The processing shall continue until the later of:

processing

- the relevant Principal Agreement(s) being terminated or expiring in

accordance with its terms and any notice period or transition period

prescribed by that Principal Agreement(s) having expired; and

- the Service Provider no longer being subject to an applicable legal or

regulatory requirement to continue to store the Personal Data

a

Nature and purpose | The processing is being conducted in order to facilitate the performance of the

of processing services documented in the relevant Principal Agreement(s).

Types of personal | No personal data is entered into the system by the user. The system receives a

data feed from My WorkDay with the fields listed below. Name, employee id, job

desc, job code, bank title, employee class and descry, fte, band, hr status, start

date, last start date, term date, etc.

Attachments are added to the audit workpapers to evidence the work

performed. These attachment s may contain Personal information or

confidential information. This information should be redacted prior to adding

the documents if possible. |

Categories of Data | Employees, contractors , vendors from My Workday , no client data

Subject Last Name

First Name

Middle Name

Employee ID

Job Code

Description

Bank Title

HR Status

Start Date

Term Date

City

Information Classification: Limited Access

GPS# 180319755629459 54

MetricStream Confidential

Location Code

Contact End Date

DeptID

DeptID Description

Level 1 Name

Level 2 Name

Level 3 Name

Level 4 Name

Supervisor ID

Supervisor Name

Lvl 1 Mgr Bank Title

Contact End Date |

State Street’s | As set out in this Addendum and the relevant Principal Agreement(s).

obligations and

rights (as data

controller)

information Classification: Limited Access

GPS# 180319755629459 55

MetricStream

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES

As set out in the Security Schedule (as defined and appended to the Principal Agreemeni(s)).

Information Classification: Limited Access

GPS# 180319755629459

Confidential

56

MetricStream Confidential

APPENDIX 3

LIST OF THIRD PARTIES PROCESSING PERSONAL DATA ON BEHALF OF SERVICE PROVIDER

NOT APPLICABLE

Information Classification: Limited Access

GPS# 180319755629459 57

MetricSteam Confidential

APPENDIX 4

STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors

established in third countries which do not ensure an adequate level of data protection

1. MetricStream, Inc., having its principal place of business at 2479 East Bayshore Road, Suite 260,

Palo Alto, California 94303 (the data importer); and State Street Bank and Trust Company,

having its principal place of business at One Lincoln Street, Boston, Massachusetts (the data

exporter),

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate

safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals

for the transfer by the data exporter to the data importer of the personal data specified in Exhibit 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data

subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the

European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data (°);

(b

—

‘the data exporter’ means the controller who transfers the personal data;

(c

—

‘the data importer’ means the processor who agrees to receive from the data exporter personal

data intended for processing on his behalf after the transfer in accordance with his instructions and

the terms of the Clauses and who is not subject to a third country’s system ensuring adequate

protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d

—

‘the sub-processor’ means any processor engaged by the data importer or by any other sub-

processor of the data importer who agrees to receive from the data importer or from any other sub-

processor of the data importer personal data exclusively intended for processing activities to be

carried out on behalf of the data exporter after the transfer in accordance with his instructions, the

terms of the Clauses and the terms of the written subcontract;

(e

—

‘the applicable data protection law’ means the legislation protecting the fundamental rights and

freedoms of individuals and, in particular, their right to privacy with respect to the processing of

personal data applicable to a data controller in the Member State in which the data exporter is

established;

Information Classification: Limited Access

GPS# 180319755629459 58

MetricStream Confidential

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal

data against accidental or unlawful destruction or accidental loss, alteration, unauthorised

disclosure or access, in particular where the processing involves the transmission of data over a

network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are

specified in Exhibit 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5{a) to

(e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party

beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause

6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared

or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the

data exporter by contract or by operation of law, as a result of which it takes on the rights and

obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause

6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data

importer have factually disappeared or ceased to exist in law or have become insolvent, unless any

successor entity has assumed the entire legal obligations of the data exporter by contract or by

operation of law as a result of which it takes on the rights and obligations of the data exporter, in which

case the data subject can enforce them against such entity. Such third-party liability of the sub-

processor shall be limited to its own processing operations under the Clauses.

4, The parties do not object to a data subject being represented by an association or other body if the

data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to

be carried out in accordance with the relevant provisions of the applicable data protection law (and,

Information Classification: Limited Access

GPS# 180319755629459 59

MetricStream Confidential

(b)

(c)

(d

—

(e)

(f)

(g)

(h)

(i)

(i)

where applicable, has been notified to the relevant authorities of the Member State where the data

exporter is established) and does not violate the relevant provisions of that State;

that it has instructed and throughout the duration of the personal data-processing services will

instruct the data importer to process the personal data transferred only on the data exporter’s

behalf and in accordance with the applicable data protection law and the Clauses;

that the data importer will provide sufficient guarantees in respect of the technical and

organisational security measures specified in Exhibit 2 to this contract;

that after assessment of the requirements of the applicable data protection law, the security

measures are appropriate to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorised disclosure or access, in particular where the processing

involves the transmission of data over a network, and against all other unlawful forms of processing,

and that these measures ensure a level of security appropriate to the risks presented by the

processing and the nature of the data to be protected having regard to the state of the art and the

cost of their implementation;

that it will ensure compliance with the security measures;

that, if the transfer involves special categories of data, the data subject has been informed or will be

informed before, or as soon as possible after, the transfer that its data could be transmitted to a

third country not providing adequate protection within the meaning of Directive 95/46/EC;

to forward any notification received from the data importer or any sub-processor pursuant to Clause

5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to

continue the transfer or to lift the suspension;

to make available to the data subjects upon request a copy of the Clauses, with the exception of

Exhibit 2, and a summary description of the security measures, as well as a copy of any contract for

sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or

the contract contain commercial information, in which case it may remove such commercial

information;

that, in the event of sub-processing, the processing activity is carried out in accordance with Clause

11 by a sub-processor providing at least the same level of protection for the personal data and the

rights of data subject as the data importer under the Clauses; and

that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

information Classification: Limited Access

GPS# 180319755629459 60

MeitricStream Confidential

(a)

(b

—

(c

—

(d

et

{e

—

(f)

(g)

i)

(i)

to process the personal data only on behalf of the data exporter and in compliance with its

instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to

inform promptly the data exporter of its inability to comply, in which case the data exporter is

entitled to suspend the transfer of data and/or terminate the contract;

that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the

instructions received from the data exporter and its obligations under the contract and that in the

event of a change in this legislation which is likely to have a substantial adverse effect on the

warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of

data and/or terminate the contract;

that it has implemented the technical and organisational security measures specified in Exhibit 2

before processing the personal data transferred;

that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority

unless otherwise prohibited, such as a prohibition under criminal law to preserve the

confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless

it has been otherwise authorised to do so;

to deal promptly and properly with all inquiries from the data exporter relating to its processing of

the personal data subject to the transfer and to abide by the advice of the supervisory authority

with regard to the processing of the data transferred;

at the request of the data exporter to submit its data-processing facilities for audit of the processing

activities covered by the Clauses which shall be carried out by the data exporter or an inspection

body composed of independent members and in possession of the required professional

qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in

agreement with the supervisory authority;

to make available to the data subject upon request a copy of the Clauses, or any existing contract for

sub-processing, unless the Clauses or contract contain commercial information, in which case it may

remove such commercial information, with the exception of Exhibit 2 which shall be replaced by a

summary description of the security measures in those cases where the data subject is unable to

obtain a copy from the data exporter;

that, in the event of sub-processing, it has previously informed the data exporter and obtained its

prior written consent;

that the processing services by the sub-processor will be carried out in accordance with Clause 11;

Information Classification: Limited Access

GPS# 180319755629459 61

MetricStream Confidential

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data

exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the

obligations, referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive

compensation from the data exporter for the damage suffered.

2. Ifa data subject is not able to bring a claim for compensation in accordance with paragraph 1

against the data exporter, arising out of a breach by the data importer or his sub-processor of any of

their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually

disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data

subject may issue a claim against the data importer as if it were the data exporter, unless any successor

entity has assumed the entire legal obligations of the data exporter by contract of by operation of law,

in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its

own liabilities.

3. Ifa data subject is not able to bring a claim against the data exporter or the data importer referred

to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred

to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually

disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data

subject may issue a claim against the data sub-processor with regard to its own processing operations

under the Clauses as if it were the data exporter or the data importer, unless any successor entity has

assumed the entire legal obligations of the data exporter or data importer by contract or by operation of

law, in which case the data subject can enforce its rights against such entity. The liability of the sub-

processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights

and/or claims compensation for damages under the Clauses, the data importer will accept the decision

of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the

supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

Information Classification: Limited Access

GPS# 180319755629459 62

MetricStream Confidential

2. The parties agree that the choice made by the data subject will not prejudice its substantive or

procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so

requests or if such deposit is required under the applicable data protection law.

2, The parties agree that the supervisory authority has the right to conduct an audit of the data

importer, and of any sub-processor, which has the same scope and is subject to the same conditions as

would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation

applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any

sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the

measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding

clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the

data exporter under the Clauses without the prior written consent of the data exporter. Where the data

importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall

do so only by way of a written agreement with the sub-processor which imposes the same obligations

on the sub-processor as are imposed on the data importer under the Clauses ( 1}. Where the sub-

processor fails to fulfil its data protection obligations under such written agreement the data importer

shall remain fully liable to the data exporter for the performance of the sub-processor’s obligations

under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a

third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to

Information Classification: Limited Access

GPS# 180319755629459 63

MetricStream Confidential

bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the

data importer because they have factually disappeared or have ceased to exist in law or have become

insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data

importer by contract or by operation of law. Such third-party liability of the sub-processor shall be

limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in

paragraph 1 shall be governed by the law of the Member State in which the data exporter is established,

namely, the United Kingdom.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and

notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The

list shall be available to the data exporter’s data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data

importer and the sub-processor shall, at the choice of the data exporter, return all the personal data

transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify

to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it

from returning or destroying all or part of the personal data transferred. In that case, the data importer

warrants that it will guarantee the confidentiality of the personal data transferred and will not actively

process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of

the supervisory authority, it will submit its data-processing facilities for an audit of the measures

referred to in paragraph 1.

Information Classification: Limited Access

GPS# 180319755629459 64

MetricStream

On behalf of the data exporter:

Name (written out in

full):

Position:

Address:

Other information

necessary in order for the

contract to be binding (if

any):

On behalf of the data importer:

Name (written out

in full):

METRICSTREAM,

INC,

Position:

Address: 2479 East Bayshore Rd. Suite. 260, Palo Alto, CA 94303

Other information

necessary in order for the

contract to be binding (if

any):

Information Classification: Limited Access

GPS# 180319755629459

Confidential

65

MetricStream Confidential

Exhibit 1

to the Standard Contractual Clauses

This Exhibit forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional

necessary information to be contained in this Exhibit

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

[A trust company specialising in services to mutual funds and their advisers, collective

investment funds, corporate and public pension furids, insurance companies, operating

companies and non-profit organisations.]

Data Importer

The data importer is (please specify briefly activities relevant to the transfer):

A provider of GRC products and services |

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employee and Contractor information . |

Categories of data

The personal data transferred concern the following categories of data (please specify):

The system receives a feed from My WorkDay with the fields listed below. Name, employee id

, job desc, job code, bank title , employee class and descry, fte, band, hr status, start date, last

start date, term date. Etc.

Special categories of data (if appropriate)

Information Classification: Limited Access

GPS# 180319755629459 66

MetricStream

Confidential

The personal data transferred concern the following special categories of data {please specify}:

eo

Information Classification: Limited Access

GPS# 180319755629459 67

MetricStream Confidential

Exhibit 2

to the Standard Contractual Clauses

This Exhibit forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer

in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures set out in the Security Schedule contained in the

Principal Agreement(s).

Information Classification: Limited Access

GPS# 180319755629459 68

MetricStream

Information Classification: Limited Access

GPS# 180319755629459

Exhibit F

List of Subcontractors

NONE

Confidential

69

MetricStream Confidential

Exhibit “G”

Open Source Components/Third Party Software

Metric Stream represents and warrants that Customer's use of the open source components, if any,

included as part of the Cloud Application will be in compliance with the terms of the applicable open

source license subject to Customer’s compliance with the terms and conditions of this Agreement. A list

of the Open Source Software and the applicable licenses is listed below

Publisher Name of Open Source Component

Apache 2.2.21

Tomcat 6.0.29

FOP 0.20.5

Jakarta Log Kit

Apache Batik 1.5

Avalon Framework 4.0

MySQL Connector J 3.0

LDAP SDK 4.17

Java Mail AP! 1.3

Apache Ant

JAXP

Xerces

Tiny Java Web Server 1.95

a

|

Apache Velocity template engine 1.5

json library 2.2.1 for JDK 1.3

| | opencsv-1.8.jar

Ext Js 3.2.0

tinyMCE 3.5.0.1

| gson 14

BouncyCastle 1.42.0

OIOSAML 5922

Apache Commons libraries in ECP

| BeanUtils 1.8.0

Codec 1.2

Collections 3.2

Digester 1.8.1

Discovery 0.2

| Http Client 3.1 HTTP/1.1 compliant HTTP

lO

Lang 2.3

Logging 1.1.1

——e |

Information Classification: Limited Access

GPS# 180319755629459 70

MetricStream

Confidential

| | Jasper 4.7

| OpenOffice 3.3

R215

Information Classification: Limited Access

GPS# 180319755629459

71

MetricStream Confidential

Exhibit “H”

Prohibition on Human Trafficking and Modern Slavery

To the extent applicable, Metric Stream represents, warrants and undertakes that:

(i) neither Metric Stream nor any of its officers, employees, agents or subcontractors has: (A)

committed an offence under the Modern Slavery Act 2015 and/or any other laws, rules or regulations

prohibiting human trafficking and/or slavery (a “Offence”); or (B) been notified that it is subject to an

investigation relating to an alleged Offence or prosecution under the Modern Slavery Act 2015 and/or

any other laws, rules or regulations prohibiting human trafficking and/or slavery; or (C) is aware if any

circumstances within its supply chain that could give rise to an investigation relating to an alleged

Offence or prosecution under the Modern Slavery Act 2015 and/or any other laws, rules or regulations

prohibiting human trafficking and/or slavery,

{ii) it shall comply with the Modern Slavery Act 2015 and any other laws, rules or regulations

prohibiting human trafficking and/or slavery;

(iii) its responses to Customer's modern slavery and human trafficking due diligence questionnaire

are complete and accurate and not misleading; and

(iv) it shall notify Customer immediately in writing if it becomes aware or has reason to believe that

it, or any of its officers, employees, agents or subcontractors have, breached or potentially breached any

of Metric Stream’s obligations under this Section. Such notice to set out full details of the circumstances

concerning the breach or potential breach of Metric Stream’s obligations.

During each twelve-month period of the Term, upon request by Customer, Metric Stream shall prepare

and deliver to Customer an annual slavery and human trafficking report setting out the steps it has

taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any

part of its business.

Information Classification: Limited Access

GPS# 180319755629459 72

MetricStream

EXHIBIT |

LIST OF THIRD-PARTY PRODUCTS

None

Information Classification: Limited Access

GPS# 180319755629459

Confidential

73

MetricStream Confidential

EXHIBIT J

Order Form No. 1

This Order Form (“Order Form”) is issued under the Master Subscription Agreement entered into by and

between MetricStream, Inc., and State Street Bank and Trust Company, a Massachusetts trust company

(“Customer”) and dated January 31, 2020. (“Agreement”). MetricStream and Customer may be referred

to individually as a “Party” and collectively as the “Parties.”

For good and valuable consideration, the receipt and sufficiency of which is acknowledged, the

MetricStream will provide Customer with the following:

Cloud Hosting: MetricStream will provide the Customer with Premium Cloud

Application Services including Encryption of the Database at Rest (TDE)

Type of License: Annual Subscription License

Subscription Begin Date: The Subscription Begin Date shall be the date upon which this

Agreement becomes fully executed.

Subscription Term: The Initial Subscription Term shall begin on the Subscription Begin Date

and shall continue for a period of one (1) year unless terminated

pursuant to Section 3.2 of the Agreement (“Initial Term”).

Fees: The Fees for the Initial Term shall be as follows:

Fee | Yr.1

Cloud Services - Premium | $180,000

Encryption of the Database at Rest (TDE) Service Fee: $90,000

Enhanced Security Fee: 560,000

Total Annual Fees $330,000 |

Cloud Services Fees [incorporated in table above]

Encryption of the Database at Rest

({TDE) Service Fee [incorporated in table above]

Enhanced Security Fee: [incorporated in table above]

Invoice Schedule: As used herein, “Fees” are defined as, collectively or individually, the

License Fee, Cloud Services Fee and Platform Fee. MetricStream may

invoice upon State Street’s Acceptance of the Cloud Hosting services.

For each year thereafter, the Fees will be invoiced 30 days prior to the

anniversary signature date of this Order Form.

Information Classification: Limited Access

GPS# 180319755629459 74

MetricStream Confidential

Fee for renewal Terms The Fees for each subsequent Term (post expiry of Initial Term) shall be

increased by an amount equai to two and one-half percent (2.5%).

Payment Terms: Net 45 days from the date of receipt of Invoice.

Invoice Address: As provided on State Street’s purchase order.

Purchase Order Information: 0 If no Purchase Order is required.

\*% If Purchase Order required, Purchase Order No.:

"

Purchase Orders must be issued within two (2) weeks of the

Subscription Start Date. Failure to issue a Purchase Order shall not

relieve Customer of its obligations to pay all invoices pursuant to

the Payments Terms above. To the extent any terms in the PO

conflicts with this Order Form, the terms of this Order Form shall

govern.

Documentation List: User’s Manual, System Administrator Manual and Training Documents

Premium OnDemand Cloud Services Description

The Premium Cloud Application Services includes:

e © @

Unlimited number of MetricStream Applications

Supports unlimited named users

Supports up to 2000 active/concurrent users

Production Environment - Dedicated Instance

Pre —Production Environment - Dedicated Instance

Disaster Recovery Environment - Dedicated Instance in a separate Data center

© In the event of a Disaster, the disaster recovery instance will be brought online. The

Recovery Time Objective (RTO) is less than six (6) hours and the Recovery Point

Objective (RPO) is less than 1 hour. Backup application servers are not used, nor are

redundant locations.

System administration and support services as set forth in the Service Level Agreement in

Exhibit B

e Application and database performance tuning services

e Backup and Recovery Services

o Perform daily backups of data off the server and backups of data off site. All

Licensee data will be encrypted for these backups. In the event of system failure,

data could potentially be lost for up to a 1-hour period.

o Encrypted Backup retention (off-site) is 15 days

o If data from the system is accidentally deleted by Licensee, restoration of this data

may be charged at MetricStream’s then current hourly rates.

© Network Connectivity

o A 100GB/month bandwidth will be provided to Licensee. This is normally

sufficient for access.

o Access to the Internet from the Licensee’s site and/or computers will be the

responsibility of the Licensee.

Information Classification: Limited Access

GPS# 180319755629459 . 75

MetricStream Confidential

Encryption of data-in-transit and data-at-rest

24/7 Network Operations Center (NOC) and Service Operations Control (SOC)

Host Intrusion Prevention System (HIPS)

Third party Identity Access Management (IAM) integration (LDAP/AD/SSO)

IP Filtering

Compliance - SOC2, and HIPAA

IN WITNESS WHEREOF, the Parties, have executed this Order Form through their authorized

representatives,

METRICSTREAM, INC. - STATE STREET a AND TRUST COMPANY

By: 7

Name: TESS! (q Zhe Ud

bi t/ Title: VW (Gz ie it Avy AK, -

Diet kéga

Title:

Information Classification: Limited Access

GPS# 180319755629459 76

MetricStream Confidential

Exhibit K

Audit Methodology — Information Classification — Use of Personal Data

Handling of Pll in Internal Audit Workpapers

e Audit workpapers are restricted to Corporate Audit staff for viewing except when requested

by regulators or other external parties approved in line with the Corporation’s Supplemental

Requirements for NIST 800 53R4 Standards. Audit workpapers are not provided to

customers of State Street.

e Though workpapers are classified as limited access and upon discussion with the Privacy

Office, personal data is allowed to be within the audit workpapers and attachments without

further access restriction or redaction on the condition that only data necessary to conduct

testing is retained. In most cases, a single, unique “identifier” (e.g., legal entity ID, account

#, employee #) is used and other Pll is redacted.

e Per discussion with the audit owners, “higher risk” personal data that may be

included in audits of Global Human Resources (e.g., incentive compensation,

payroll), Global Security (e.g., background checks, investigations) and Corporate

Compliance (e.g., know your customer requirements and files. IN these cases the

audit owners either (a) did not include the high risk Pll at all and only described the

data so that another individual could run the same report or (b) redacted the data to

only include a single unique identifier .Further, audit owners confirmed that where

possible, documentation is reviewed on-site or live rather than obtaining electronic

support

e The main scenario where we are aware of two identifiers being used is user access testing,

which may include employee name and employment ID.

Controls in Place

e There are two key controls in every audit to prevent the inclusion of personal data:

o All workpapers undergo at least one level of review, typically by an AVP or above, to

approve content and a final review, typically by a VP or above, to close the audit and

confirm compliance with information classification requirements

e In addition to these controls, Audit’s Quality Assurance team reviews a sample of audits

each year for compliance with our methodologies, including information classification

standards

Information Classification: Limited Access

GPS# 180319755629459 77

MetricStream

EXHIBIT L

Master Services Agreement dated December 30, 2011

Information Classification: Limited Access

GPS# 180319755629459

Confidential

78

MASTER SERVICE AGREEMENT

METRICSTREAM, INC.

and

STATE STREET BANK AND TRUST COMPANY

Effective December 30, 2011

06/11

MASTER SERVICE AGREEMENT

MASTER SERVICE AGREEMENT together with its Schedules (“Agreement”) made this 30th day

of December, 2011, by and between MetricStream, Inc., a Delaware corporation with a principal place

of business located at 2600 East Bayshore Road, Palo Alto, CA 94303 (“Service Provider") and State

Street Bank and Trust Company (“SSBT”), a Massachusetts trust company with a principal place of

business located at One Lincoln Street, Boston, Massachusetts 02111-2900 (cach, a “Party” and,

collectively, the “Parties”),

WHEREAS, SSBT desires to engage Service Provider to implement its Internal Audit Solution;

WHEREAS, the Service Provider offers such Services;

WHEREAS, Service Provider has represented to SSBT that it has the requisite expertise to provide

the Services and Deliverables; and

WHEREAS, SSBT desires to retain Service Provider, and Service Provider has agreed, to pravide the

Services and the Dellverables on the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the mutual agreements herein contained Service Provider

and SSBT hereby agreeas follows:

1. — Definitions

11. “Approved Subcontractor” means each Service Provider subcontractor required by the

terms of Section 2.8 to be approved by SSBT in writing prior to performing Services or

having access to SSBT Confidential Information under this Agreement.

"1.2, “Confidential Inforination” means all information which relates to research, development,

and business activities of Discléser and Discloser’s parent, subsidiary, affiliated companies,

customers. and third party vendors, if any, whether in documentary, database, electronic, oral

or any other form, and any and all. trade secrets, trade knowledge, know-how, formulae,

processes, systems, software, algorithms, data, programs, training aids, printed materials,

methods, books, records, client files, employee or other Personnel names, identity and

information, policies and procedures and other information relating to the operation of

Discloser, and shall be deomed to include all notes, analyses, compilations, studies,

interpretations or other documents prepared by Reoipient based on the Confidential

Information made available to it by Discloser. “Confidential Information” as to SSBT shall

include, without limitation, SSBT.Personal Data, SSBT Content and Third Patty Content.

The terms of this Agreement are. “Confidential Information” as to both Parties.

1.3, “Data Protection and Privacy Laws” means all federal, state and foreign laws, rules,

yegulations, directives and governmental or data protection authority decisions, in each case,

having the force of law applicable to the- collection, use, storage and/or disclosure of

personally identifiable data and sensitive personal information including, without limitation,

Title V of Gramm-Leach-Bliley Act of 1999, Japan’s Personal Information Protection Law,

The Massachusetts Standards: for the Protection of Personal Information of Residents of the

Commonwealth (201 C.M.R. 17.00, ‘et seq.), and the UK Markets in Financlal Instruments

Directive and the European Union Directive 95-46.

1,4. “Deliverables” means all data, information, materials, inventions, compyter programs and

computer software (including, without limitation, all source code), designs, samples,

specifications, schematics, processes and formulae, development tools, inventions, ideas,

145;

1.6,

17.

1.8.

1.9,

1,10,

1,11,

112,

1.13.

1.14,

concepts, know-how, ‘techniques, materials, flow charts, outlines, lists, compilations,

manuscripts, whitings and pictorial materials, and all documentation and media constituting,

deseribing ox relating to the foregoing including, without limitation, manuals, memoranda and

" records and deliverables, conceived, created, developed and/or reduced to practice in

connection with a Statement of Work by: Service Provider, or jointly by SSBT and Service

Provider, or otherwise. by Service Provider pursuant to specifications or materials provided by

SSBT. .

Piscloser” means the Party providing the Confidential Information.

“Force Majeure Event” means any clroumstance or cause beyond a Patty’s reasonable

control and not caused by such Party, its agents or Personnel, including, without limitation,

acts of God; strikes, lockouts, riots, insurrections, civil disturbances, sabotage, embargoes,

blockades, acts of war, acts or failures to act of any governmental or regulatory body (whether

civil or military, domestic or foreign), governmental regulations superimposed after the fact,

communication line failures, power failures, fires, explosions, floods, accidents, epidemics,

earthquakes or other natural or man-made disasters, and all occurrences similar to the

foregoing. .

“Flour Worked” means the lesser of 8 hours or actual hours spent engaged In providing the

Services at SSBT’s offices or elsewhere, as contemplated by a Statement of Work, or actual

hours spent engaged in providing support services necessary for the successfil performance

of the Services contemplated under a Statement of Work.

‘$ntellectual Property Rights” means copyrights (including rights in software), patents,

trademarks, trade names, service marks, business names (including intemet domain names),

design rights, database rights, semi-conductor topography rights, rights in undisclosed or

confidential information (such as know-how, ttade secrets and inventions (whether patentable

or-nof)). and all other intellectual property or similar proprietary sights of whatever nature ~

(whether registered or not and including applications to register or rights to apply for

registration) which may now or in the future subsist anywhere in the universe,

“Personnel” means any and all full or part-time employees, temporary employees,

consultants, contractors or subcontractors, :

“Recipient” means the Party receiving the Corifidential Information.

‘Related Company (collectively, “Companies’)” means in relation to elther Service

Provider or SSBT, a subsidiary or affiliate of such Party.

“Services” ineans the services and Deliverables provided by Service Provider to SSBT

pursuant to this: Agreement, as further described in each Statement of Work.

“SSBT Content” means the specifications and/or materials, proprietary tools .and

methodologies including, but not limited to software and hardware, provided by SSBT to

Service Provider or of which Service Provider otherwise becomes aware.

“SSBT Personal Data” means data, information, text, visual or graphic representations and

other materials in'any medium or format, electronic, tangible or otherwise of a personal,

sensitive or confidential nature conceming or relating to.a living individual who is or can be

identified either from the data or from the data in conjunction with other Information that is

in, or is likely to come into, the possession of the Service Provider including, but not limited

to, any customer, contractor, Personnel or agent of SSBT, its Related Companies or any of

1.15,

1.16.

1 17,

2.

2.1,

their customers, contractors, Personnel, or agents which would be subject to application of

Data Protection and Privacy Laws and which:

(a) is provided or made available to the Service Provider ot any of its Related Companies by

or at the direction of SSBT or any of its Related Companies in connection with the

provision of the Services, so

(b) the Service Provider and any of its Related Companles create, collect, procéss, store,

generzite or transmit in connection with the provision of the Services, or

(©) the Service Provider becomes aware of as a result of or in connection with the

\_\_ performance this Agreement.

SSBT Persorial Data shall not include business contact information.

“Standard Tools” means Service Provider's proprietary tools, methodologles and materials

developed pricr to the performance of Services and used by Service Provider in the

performance of its business and specifically set forth in a Statement of Work and which do

not contain, and are not derived from, SSBT’s Confidential Information.

“Statement of Work’ means the document in the form attached as Schedule A that

establishes the scope of the Services to be performed, defines the context, describes specific

tasks, activities ‘and Deliverables, and identifies the responsibilities of the Parties.

“Third Party Content” means the. third party specifications and/or materials, tools and

methodologies, Including, but not limited to software and hardware, and other third party deta

and information provided by SSBT to Service Provider or of which Service Provider becomes

aware,

Services

Scope of Services.

(a) Service Provider shall provide SSBT with the Services, as desctibed in one or more

Statements of Work in accordance with the terms and timeftames set forth therein. No

Services shall be. provided by virtue of this Agreement alone but shall be provided in

accordance with the applicable Statement of Work. :

(b) If there is a discrepancy between the Statement of Work and this Agreement,. this

Agreement shall control-unless the Statement of Work specifically references and amends

a Section of this Agreement. . , ‘

(c) If a proposal submitted by Service Provider contains multiple phases, each shall be

addressed by a separate mutually agreed upon Statement of Work, unless otherwise

agreed by the Parties, provided that the option to go forward with each phase shall be at

the sole option of SSBT,

(d) Each Statement of Work will provide the project objectives and scope of Services, the

roles and responsibilities of Service Provider and SSBT, the operating model,

Deliverables, acceptance criteria, project management and quality approach as well as

costs and other details, Unless otherwise set forth in the applicable Statement of Work,

all written Deliverables delivered to SSBT shall be written in the English language.

Service Provider shall be responsible for preparation of each Statement of Work with

cooperation by SSBT.

2.26

2.3,

dt,

2.5.

Acquisition of. Services by SSBT Related Companies. SSBT Related Companies may

receive Services from the Service Provider under this Agreement, In such event, each SSBT

Related Company that signs a Statement of Work shall be considered “SSBT” as such term 1s

used herein and shall be subject to the terms and conditions of thls Agreement and beneficiary

of all rights hereunder.” Each SSBT Related Company shall be solely responsible for its

obligations under this Agreement and under the Statement of Work signed by such SSBT

Related Company.

\_ Scheduling, Service Provider shall provide all Services and Deliverables in accordance with

the timeframes: establistied in the applicable Statement of Work and/or project. plan as

developed-by Service Provider and SSBT pursuant to such Statement of Work, Service

Provider shall provide SSBT with advance written notice in the event Service Provider

foresees any difficulties in meeting the timeftames or costs established in the applicable

Statement of Work and shall be liable for all costs and expenses Incurred by SSBT as a result

of Service Provider's delay, For the avoidance of doubt, any modified timeframes and

additional costs shall be subject to SSBT’s prior written consent. Service Provider will not

exceed any estimate of time, feds or costs without the prior written consent of SSBT. All -

changes to any engagement desired in any Statement of Work, including fess or timeframe for: —

delivery of Deliverables, shall be effective and binding on SSBT only if contained in a

Change Order signed by oach Service Provider and SSBT.

Enrollment in SSBT Vendor Management System. Within thirty (30) days of, the date

hereof, unless SSBT has otherwise directed Service Provider, Service Provider will be -

required to enroll in the SSBT Vendor Management System and to pay all fees assoclated

with such enrollment, if any, as disclosed by SSBT from time to time. If Service Provider

fails to enroll in the SSBT Vendor Management System within thirty ($0) days of receipt of

notice from SSBT, SSBT shall be entitled to terminate this Agreement without further

lability in accordance with the terms hereunder unless the Parties can mutually agree to an

alternative vendor management and payment arrangement.

Praject Team.

(a) Service Provider shall provide and/or perform the Services and its other obligations

hereunder using suitable Personnel with appropriate skills and expertise in accordance

with the terms of this Agreement, including the Statement of Work.

(b) Service Provider shall develop a team of its Personnel to provide Services under this

Agreement including, as necessary, but not limited to, its Project Manager as herelnafter

defined in Section 12.1 (“Project Team”) and agrees not to rotate or otherwise transfer

members of the Project Team more frequently then every twelve (12) months without the

prior written authorization of SSBT. In addition, any member of the Project Team whom

SSBT identifies as “Key Personnel” in the applicable Statement of Work shall remain

\_ engaged in the project described on such Statement of Work on a full time basis unless

otherwise agreed to in writing by SSBT-or unless no longer employed by Service

Provider. The initial members of the Project Team shal! be set forth In the Statement.of”

Work, if requested by SSBT.

(c) If any members of the Project Team cease to provide the Services in accordance with the

terms of this Agreement for any reason, Service Provider shall promptly teplace such

member(s) with Personnel as reasonably determined by SSBT or Service Provider having

similar qualifications and experlence and ensure that any such replacements are

jnnmediately trained and brought up to date on Services being provided’ at no chargé to

SSBET. ‘

2.7,

(d) Service Provider represents and warrants that it complies and will continue to comply

with all applicable laws, regulations, and other legal obligations to Service Provider's

Personnel, specifically including, but not limited to, employment laws, and prohibitions

against insider trading and accepting bribes.

(e) Service Provider acknowledges and agrees that, in the course of providing the Services,

Service Provider Personne! may have access to, or acquire, knowledge of confidential,

proprietary or sensitive information regarding SSBT, its Related Companies or ‘their

clients, Personnel or other parties with whom SSBT or its Related Companies have 4

\_ relationship, Service Provider will advise such Service Provider Personnel of the

standards imposed upon them with respect to the Services they render pursuant to the -

terttis of this Agreement and shall remain responsible for any breach of confidentiality, ’

security or privacy by any Service Provider Personnel, including without limltation any

subcontractors. Service Provider Personnel shall execute SSBT’s Standard of Conduct

upon request by SSBT and provision of such Standard of Conduct for review. —

(f) Service Provider shall be responsible to ensure that its Project Team is fully adequately

trained so that the Project Team (i) performs the Services in accordance with the terms of

the Statement of Work and (i!) complies with all of the terms of this Agreement.

Service Management, Service Provider will designate an authorized representative to

manage the relationship for Service Provider who will:

(a) be acceptable to SSBT;

(b) be the primary contact for SSBT in dealing with operational issues arising under this

Agreement;

(c) have overall responsibility for managing and coordinating the delivery of the Services;

(a) meet regularly with the SSBT’s authorized representatives; and

(e) have thé power and authority to make decisions with respect to actions to be teken in the

ordinary course of day-to-day performance of the Services In accordance with this

Agreement.

Service Provider Relationship.and Benefits. Service Provider will be responsible for;

(a) all compensation, including but not limited to, base, incentive,‘ and overtime

compensation, As applicable;

(b) all retirement (as required to exempt SSBT under Section 414(n) of the Internal Revenue

Code and its implementing regulations) and.medical coverage (as tay be required under

a similar law), payroll taxes, and required payments/deductions when and where

. applicable; and . ‘

(c) any einployee benefits that Service Provider provides or is legislatively required to be

provided to the Project Team, as Service Provider's employees. OO

Service Provider, inciuding its Personnel, will furnish Services as an Independent contractor

and not as an employee or agent of SSBT, any SSBT Company or any company. affiliated

with or serviced by SSBT and Service Provider Personnel have no power or authority to act

for, represent, ot bind SSBT or any SSBT Related Company, in any manner. Service

Provider shall be solely responsible for resolving aty afd all persorinel issues and wages or

2.8.

2.9,

salary matters pertaining to the Project Team performing Services under this Agreement,

including without limitation any issues of bonus or incentive compensation, the withholding

of all appropriate income and other payroll taxes, payment of overtime compensation, and

additional legal requirements of a like nature, Service Provider's Personnel are not entitled to

any compsnsation or benefits from the SSBT, Inoluding but not limited to retirement, medical

coverage, life insurance,-or other benefits, which may be afforded to SSBT"s regulat

employees,

Subcontractors,

(a) Service Provider shall provide SSBT with sufficient information regarding each proposed

subcontractor to whom Service Provider intends to either delegate performance of all or

part of fhe’Services or provide access to SSBT Confidential. Information.and/or SSBT

systems in order to etable SSBT to determine whether SSBT can approve, in writing

prior to performing Services or accessing SSBT Confidential Information, such

subcontractor as an Approved Subcontractor. A list of Service Provider Approved

Subcontractors as of the date of this Agreement is attached-hereto as Schedule B.

(b) If, at any time during the terni of this Agreement, Service Provider desires to add an

Approved Subcontractor to Schedule B, Service Provider shall so notify SSBT and

provide it with sufflofent information to enable SSBT to determine whether or not it can

consent to, in writing prlor to performing Services or accessing SSBT Confidential

Information; the appointment of such subcontractor as an Approved Subcontractor.

(c) Upon SSBT’s request, in order for SSBT to comply with applicable Data Protection and

Privacy Laws, Service Provider shall promptly provide SSBT with a copy of the written

agreement (or to the extent permitted by faw, summaries thereof) and any updates thereof,

wiitch it has with each Approved Subcontractor having access to SSBT Personal Data.

(d) Service Provider shall remain responsible and liable for the acts and omissions of any

subcontractor to the same extent as if such acts and omissions wee performed or not

performed, as the case may be, by Service Provider, regardless of whether SSBT has -

exercised its right to reject or approve SSBT’s use of any proposed subcontractor, as

‘applicable, Service, Provider shall be responsible for paying the subcontractor and, as

applicable, filing appropriate information returns as required by state and federal laws and

regulations.

Corrective Actions. If the Services are not provided with the skill and expertise requited by

this Agreement, Service Provider shall undertake the following corrective actions for any

problem or issue reported by SSBT:

(a) SSBT will notify Service Provider's Project Manager when there is a problem or issue

with the delivery of Services (including any breach of law, or inappropriate conduct of

any Service Provider or Approved Subcontractor employee or other Personnel), :

(b) Service Provider's Project Manager will meet with SSBT within one (1) business day (or

such other time as mutually agreed upon by the Parties) to assess the delivery problems or

issues and develop a corrective action plan at no cost to SSBT.

(c) Unless mutually agreed upon by the Parties, the corrective action plan shall provide 4

remedy:

(i) for-ctitical. business matters within one (1) business day including removal of the

subject employee or other Personnel, if requested by SSBT; and

2.10.

2.11,

2.12,

2.13.

(ii) for normal business matters within five (5) business days including removal of

the subject employee or other Personnel, if requested by SSBT.

(d) Notwithstanding anything to the contrary contained herein, SSBT may immediately

remove any employee or other Personnel of Service Provider or Approved Subcontractor

for breach of privacy or confidentiality or for any security reasons.

Communications.

(a) Uniess otherwise set forth in the applicable Statement of Work, Service Provider shall

establish and maintain a system to ensure continued communications between Service

Provider and SSBT,

(b) If Service Provider Is located outside of the United States, Service Provider shall assign

one (1) US-based employee who is fluent In the English language to be responsible for

serving as liaison between SSBT and Service Provider (the “SSBT Liaison”). Such BSBT

. Liaison shall be available to SSBT during SSBT’s standard business hours to address

Service Provider’s- questions and facilitate problem resolution. Such SSBT Liaison shall

also serve as Service Provider's designated agent for service of process in the United

States. ‘

(c) Service Provider shall ensure that all other Service Provider employees-or other Personnel

who have authority to communicate with SSBT shall be fluent in English and the

language of the applicable local jurisdiction where the Services are being performed

and/or have a cettified translator and/or interpreter at such|Personnel’s disposition in

order to ensure continued effective communications between SSBT and Service Provider,

at Service Provider's expense. :

Working Arrangement. Except as otherwise provided n a Statement of Work, Personnel of

Service Provider assigned to SSBT and/or SSBT projects shall have sufficient access to the

following SSBT resources to enable the performance of the Services: physical resources such

as desks, local telephones, storage space, office supplies and food facilities, subject to

compliance with SSBT’s policies and procedures including those relating to corporate

information security,

Third Party Consents, Before commencing any Services, Service Provider shall provide

SSBT with a written list of all SSBT software, hardware and other resources to which Service

Provider will require access in order to perform the Services, including any SSBT Content or

Third Party Content and such list shall be included in the applicable Statement of Work. ‘To

the extent that SSBT requires any thitd party consents in order for Service Provider to access

and use such resources ih connection with the provision of the Services, SSBT shall obtain

such consents. Service Provider shall, and shall ensure that its Personnel and Approved

Subcontractors shall, abide by all restrictions imposed by third partles regarding such

resources including compliance with any licensing or other terms governing socess to any

hardware or software.

Final Acceptance Procedure,

(a) Except as‘ otherwise provided in a Statement of Work, upon completion of each

Deliverable identified under a Statement of Work and delivery of such Deliverable to

SSBT, Service Provider shall advise SSBT in writing that SSBT must provide Service

Provider with written notice of its acceptance or rejection of the Deliverable,

(b) SSBT shall respond within ninety (90) days of its receipt of the request either:

3

3.1.

(i) \_\_ finally accepting the Deliverable, or

(i) notifying Service Provider of Its rejection of the Deliverable and detailing and

documenting what it considers to be incomplete or not performing in accordance

with the material specifications with a description of such deficiency which is the

basis for rejection of such Deliverable, .

(c) Ifa deficiency is claimed, Service Provider shall respond to SSBT within fourteen (14)

days of recelpt of SSBT’s response with a plan to cure the deficlency. The plan shall

include the period required to cure the deficiency, provided, however, that the cure period

tay not exceed ninety (90) days. After completing its efforts to cure the Deliverable,

Service Provider shall provide SSBT with the revised Deliverable and the acceptance

procedure described herein will be followed again. If SSBT, at any time In its sole

discretion, determines that the deficiency has not been cuted to SSBT’s satisfaction

and/or that the revised Deliverable does not otherwise conform to its specifications or

applicable documentation, SSBT shall have the option to extend the cure period or

terminate the applicable Statement of Work. If SSBT chooses to terminate the Statement

of Work, SSBT, in its sole discretion shall either:

(i) retain all other Deliverables and recelve a full refund of all fees paid for the

unaccepted Deliverable, or

(ii) ‘if SSBT reasonably believes that the conforming Deliverables have insufficient

value without successful delivery by Service Provider of all Deliverables

contemplated in the applicable Statement of Work, return all Deliverables and

receive a full refund of all fees pald under the Statement of Work.

SSBT shall not be charged for Service Provider's cure of any doficiency in any

Deliverable provided to SSBT for testing pursuant to this Section 2.13 whether the

applicable engagement is 4 time and materials or fixed rate engagement.

(d) To the extent that Deliverables that have been returned to Service Provider contain any

Confidential Information of SSBT or any SSBT Related Company, or of any third party,

Service Provider shall destroy all notes, memoranda, programs or other materials,

wherever located so as to become permanently unintelligible, which Service Provider

made or possesses relating in any way to any of the foregoing and confirm such

destruction with SSBT in writing,

Service Changes

Definition of Changes, The Parties shall use the procedures set forth in this Section‘3 to:

(a) add new or additional services;

(b) modify, upgrade or otherwise change the Services (including the elements and/or

“frequency of any task performed as part of the Services); or

(c) change the means or manner in which the Services are provided (collectively,

“Changes”); ,

Any chariges to Services or timing or method of delivery of the Services or to fees relating to

the Services must be made in accordance with the terms of this Sectlon, SSBT will not be

responsible for payment of fees associated with any Change unless such Change is processed

in accordance with the terms hereof.

32,

3d)

3.4.

4,

4.1.

Change Request Procedure, The Party that wishes to make a Change shall deliver to the

other Party a written request that contains as much detail as is teasonably practicable

regarding the nature and scope of the Change, including the proposed implementation date,

the priority of the Change in relation to other pending Changes, and the fees associated with

any proposed Change (each such request, a “Change Request”), The Parties shall develop a

process, subject to the direction of the Steering Committee, to ensure that any Change

Requests that entail development of Deliverables are managed and prioritized appropriately.

Acceptance of a Change Request, The Parties shall work together to agree on the terns that

will govern any Change, provided, however, that no Change shall be implemented until such

time as SSBT agtées to the applicable Change Request In-wrlting (“Change Order”). In the

event that the Parties are unable to agtee upon the terms of a Change Request, the matter may

be referred to the Escalation Procedure desoribed in Section 13, -

Fees for Changes. The Partics acknowledge and agree that not all Changes will involve the

imposition of additional chatges. The Parties will negotiate in good faith to reach agreement

on applicable development costs and/or operational fees, if any, that will apply to such

Change. In connection with each assessment, the Parties shall, among other things, consider:

(a) the materiality of the Change;

(b) the degree to which the Change Request involves substantially simflar functlons, duties

and/or workloads as then performed by Service Provider as part of the Services;

(c) the cost of developing and implementing the Change;

(d) projected third party charges;

(e) the timing of the Change in relation to then-current resource levels and other pending

projects arid initiatives;

(f) the resource allocation and cost profile of providing the Services after implementation of

the Change; ; . .

(2) whether upfront costs can be recouped within a commercially reasonable time frame;

(lh) whether the Change involves the cteation of assets or competencies that Service Provider

can employ to service.other customers;

(i) whether the requested Change addresses matters which should reasonably have been

known to Service Provider prior to commencement of the Services or results from

miscalculation or érror on the part of Service Provider; and ,

(J) such other considerations as the Parties deem relevant under the circumstances.

For the avoidance of doubt, no changes In fees will be final until agreed in writing by both

Parties. The cost of any Change due to Service Provider’s error or otherwise attributable to

Service Provider or an Approved Subcontractor shell be borne solely by Service Provider.

Fees and Expenses

Service Fee. SSBT shall pay Service Provider for Services provided under a Statement of

Work.in accordance with any one or all of the following, as speclfled In the applicable

Statement of Wotk:

10

, 4.2.

4.3.

4, 4.

4.5,

(a) time and materials at an individual flat rate per Hour Worked per individual furnished by

Service Provider;

(b) a fixed rate for completion of all Services and delivery of all conforming Deliverables; or

(c). at-any other rate agreed to by SSBT and Service Provider, set forth in such Statement of

Work, ~ ,

‘Travel and Other Expenses, Subject to the terms of this Section 4.2, SSBT shall reimburse

Service Provider for all reasonable travel and other expenses (over and above normal daily

expenses of working and commuting) in connection with Services as furttier provided under a

Statement of Work, All such travel and other expenses must be authorized by SSBT prior to

being incurred unless otherwise provided in the applicable Statement of Work.

Additional Charges, SSBT shall also pay as additional charges under this Agreement

-amounts, equal to any taxes, however designated, levied, or based on this Agreement, or on

Services provided hereunder, including state or local sales taxes, value added taxes, and use

or service taxes, if applicable, or amounts in liew thereof paid or payable by Service Provider

in respect of the foregoing exclyding any taxes based upon Service Provider’s net or gross

income, -In the event that any tax levied hereunder is later held to be invalid, Service Provider

shall refund to SSBT any amount, paid by SSBT of the tax held to be invalid. Upon request

by SSBT, Service Provider will make available to SSBT local resources in order for SSBT to

determine the impact of any applicable taxes on the provision of Services by Service Provider

under this Agreement. ; .

Pricing and Performance Meetings. Service Provider shall attend quarterly meetings and

such additional meetings as SSBT may reasonably request, in, order to discuss pricing and

etformance issues with SSBT. At the request of either Party, the other Party will-include its.

genlor management in any such meeting. If at any time during the term of this Agreement,

Service Provider offers a customer that is similarly situated to SSBT services that are similar

to the Services at a lower price ot oh more favorable terms than that in effect at the time the

Services are provided to SSBT hereunder, Service Provider shall notify SSBT of the terms

thereof, and SSBT shall receive the benefit of such lower price or more favorable terms for

the Services while such lower price ot more favorable terms are in effect, Ifat any time there

is a deficiency in the performance of the Services, the Parties shall establish and invoke a

remedial plan,

Invoices. Service Provider shall provide SSBT with monthly invoices in accordance with the

milestone: payment schedules set forth in the Statement of Work for the Services and

Deliverables accepted by SSBT and for travel and other expenses incurred under a Statement

of Work during the preceding monthly period or if no such schedule is in offect such invoices

shall be permitted within fifteen (15) days of the end of each month, The invoices will

indicate distribution of charges by name of employee or other Petsonnel, assigned

identification umber, project name, SSBT project manager, rate, hours worked, fee for the

period and applicable expenses, if any and any additlonal information requested by SSBT.

Invoices must be substantlated by receipts for expenses amounting to more than twenty-five -

dollars ($25.00) to the extent that receipts for such expenses are normally Issued. SSBT shall

pay Service Provider all undisputed amounts of the Service Pravider’s correct invoice within

forty-five (45) days of SSBT’s receipt of the applicable invoice, Service Provider shall offer

a discount for payment by SSBT of an invoice prior to such forty-five (45) day period.

Unless otherwise set forth in the Statement of Work, all invoices shall be converted into U.S.

dollars using the conversion rate used by SSBT on the date of payment. All invoices and any

judgments, taxes and other payments due under this Agreement shall be paid in U.S. dollars

unless otherwise designated by SSBT. SSBT is not responsible or obligated for the payment

11

4,6,

5.

5.1.

of any ‘fees, chaiges or expenses desoribed in any invoice which is not received by SSBT

within ninety. (90)-days of the date such invoice was to have been provided by Service

Provider in accordance with this Agreement or applicable Statement of Work. In addition,

any payment made by SSBT in the amount of any invoice received from Service Provider

shall be declaréd to be full and final payment of such amount and for all Services which are

the subject of such invoice.

U.S, Tax Documentation and Withholding:-Tax, In the event that Service Provider is not a

United Stafes person, as' defined by, the Internal Revenue Code of 1986, as antended or its

implementing-regulations, and receives U.S. source income, Service Provider shall provide to

SSBT, if requested by SSBT, a) a certificate of foreign status of beneficial owner for United

States tax withholding (in general, IRS Form W-8) or other certificate-necessary to document

Service Provider under U.S. tax laws, rules and regulations, including any appropriate cfaim

of tax treaty benefits and b) for any payments characterized as services, a statement of the

tocation (inside the U.S, or outside the U.S.) where such services are furnished, U.S. source

income includes, but Is not limited to, payments for services furnished by Service Provider

inside the U.S, and leases and licenses of property used by SSBT inside the U.S. If, instead,

Service Provider is a United States person for U.S. tax purposes, and [f requested by SSBT,

Service Provider will provide to SSBT a certificate of U.S, status (i.e, IRS Form W-9).

SSBT is authorized to withhold taxes from any payments made to Service Provider at a rate

required by United States tax.Jaw and to report such. payments and taxes as required by

United States bax law.

Confiden: if an, Protection

Use Restrictions,

(a) Without piior written approval from Discloser, Recipient shall not use the Confidential

Information ‘of the Discloser other than as necessary to carry out its obligations hereunder

and such use shall comply with the terms of this Agreement, including, withont

limitation, documents required in order to comply with Data Protection and Privacy

Laws.

(b) The Recipient shall secure and protect the Discloser’s Confidential Information from

unauthorized use or disclosure and shall:

(i) not disclose, sell, assign, publish, lease, release, transfer or otherwise make

available the Discloser’s Confidential Information in any form to or for the use or

benefit of, any person or entity without the Discloser’s consent;

(ii) not possess or assert Hens or other rights in of to the Discloser’s Confidential

Information;

(iii) not duplicate any material containing the Disoloser’s Confidential Informatlon

except in the direct performance of its obligations under the Agreement;

(iv) not disclose any of Discloser’s Confidential Information to any of its Personnet

except on a “need to know basis” as required to provide the Services described in

this Agreement and subject to Section 5,5 below; and

(v) ot disclose any of Discloser’s Confidential Information to any third party,

Including without limitation, its Approved Subcontractors, without the prior written

‘consent of Discloser, and, with respect to Service Provider as Recipient, an

agreement in writing from such third party to use or disclose SSBT Confidential

12

5. 2.

5.3,

Information only’ to the ‘extent necessary to carry out the obligations under this

Agreement and for no other purposes and to maintain and process the Confidential

Information in compliance with applicable Data Protection and Privacy Laws.

(c) Confidéntial Information may not be disclosed. or used by the Recipient or any of its

Related Companies, officers, directors, agents, professional advisors, Approved

Subcontractors, or Personnel, except to the extent necessary to carry out its obligations

under this Agreement and for no other purpose. '

(d) Notwithstanding any other provision in this Agreement, nothing contained in this Section

5 will be construed as obligating either Patty to disclose its own Confidential Information

\_ to the other Party, or as granting to or conferring on a Party, expressly or by implication,

"any rights or license to the Confidential Information of the other Party.

Service Provider Additional Use Restrictions, Without limiting the generality of the

foregoing, Service Provider shall: ©

(a) not permit any Confidential Information of SSBT to be disclosed to any entity that

competes with SSBT, or its Related Companies, or any products thereof, -

(b) not provide such access to any Personnel who directly services a business that competes

now ox in the future with SSBT or its Related Companies;

(c) train all Service Provider Personnel on the special restrictions set forth herein applicable

to SSBT Confidential Information;

(d) provide meaningful compensation incentives to senior Service Provider employees ~

relating to compliance with Service Provider confidentiality obligations hereunder with

tespect to SSBT;

(e) segregate and protect SSBT Confidential Information by configuration of its information

and processing systems or by adopting other appropriate measures; and

(f) use determined, prudent and reasonable efforts to strengthen the provisions in its

agreements with each of its Approved Subcontractors, including, without limitation,

where possible making such provisions comparable to the confidentlality obligations of

Service Provider hereunder,

Security,

(a) The Service Provider shall have implemented as of the date of this Agreement, and shall

thereafter continue to maintain current, a comprehensive security policy or policles

(‘Security Policy”) that satisfies the requirements set out in Schedule D {the “Security

Schedule”). In addition to the requirements of the Security Schedule, Recipient shall

have established prior to receipt of-any of Discloser’s Confidential Inforination, and shall

continue to maintain for so Jong as Disoloser’s Confidential Information is in Recipient's

possession or control, generally accepted industry “best practices” systems security

measures :designed to guard against the destruction, loss, or alteration, of Discloser's

Confidential Information that are no less rigorous than those maintained by Recipient for

its own information of a similar nature, and that aré consistent with a reasonable care

standard except In those Jurisdictions which do not recognize such reasonable standard of

cate in which case Recipient shall be obligated to use best efforts.

\

13

(b) Service Provider’s Personnel who access SSBT’s facilities or systems are subject to

certain credit and criminal checks conducted by SSBT or’ its agents (‘Security

Cleatance”) applicable to banks pursuant to banking regulations by SSBY. If any person

does not pass SSBT’s Security Clearance, Service Provider.shall remove such person

from the assignment, Service Provider is responsible for informing and recelving the

consent of its assigned Personnel that a Security Clearance including, without Imitation,

fingerprinting, id picture for badge, and the signing of a security form and confidentiality

agreement, will be required, Service Provider's execution of this Agreement indicates

that these requirements have been met.

(c) Service Provider's assigned.Personnel shall comply with the SSBT’s policies and rules,

including those relating to facilities access, systems access operating standards and

procedures, user identification and password controls, corporate information, security and

data protection and privacy, as in effect from.time to time as a condition to being

provided access to SSBT’s premises, systems or SSBT Confidential Information. Service

Provider will not, and will ensure that Service Provider Personnel do not, break, bypass,

or circumvent, or attempt to break, bypass or circumvent, any security system of SSBT or

its Related Companles, or obtain, or attempt to obtain, access to any SSBT Confidential

Information other than as allowed by SSBT in compliance with this Agreement. Service

Provider will immediately terminate access to SSBT systems and premises by any Service

Provider Personnel who is either removed or is no longer actively engaged in any SSBT

assignment or if such Personnel ceases to be an employee of Service Prov! der,

(d) Service Provider acknowledges that to the extent that it maintains or has access to certain

SSBT Personal Data of Massachusetts residents, Service Provider is obligated to comply

with the Massachusetts Office of Consumer Affairs and Business Regulation standards

for the protection of persorial information of Massachusetts residents, 201 CMR 17.00:

(“Standards”), Service Provider certifies that for so long as it has SSBT Personal Data of

Massachusetts residents thereafter and to the extent that the Standards are applicable to

the Services that Service Provider provides hereunder, Service Provider shall maintain

information security safeguards and protect such SSBT Personal Data in compliance with

the Standards and that it shall notify SSBT in writing immediately if it is no longer in

‘compliance with the Standards. Service Provider further certifies to SSBT that it has a

written information security program in. compliance with the Standards.

5.4, Employee Non-Disclosure Agreements. \_

(a) Service Provider represents and warrants that any Service Provider Persormel (elther

directly or indirectly through theii respective employers) having access to any SSBT

Confidential Information will have signed a confidentiallty agreement with Service

Provider requiring that such Personnel maintain confidentiality of information such as

SSBT Confidential Information and assign all other Intellectual Property Rights in: all

" materials and products created by such Personnel to Service Provider and disclaiming any

ownership interest therein,

(b) In addition Service Provider will Issue a nondisclosure and confidentiality agreement

between SSBT and each Service Provider Personnel that may have access to SSBT

Confidential Information that minimally requires such Service Provider Personnel to

comply with Service Provider's confidentiality and non-disclosure duties hereunder.

Within thirty (30) days thereafter, Service Provider will use diligent efforts to collect such

agreements in fully exeouted and binding form, provided that within ninety (90) days

following the effective date of the Agreement, Service Provider will have collected all

such agreements in fully executed and binding form. During such ninety (90) day period,

14

5 5,

5.6.

V

Service Provider will provide SSBT wlth monthly updates indicating the status of all such

agreements, ;

Return or Destruction of Confidential Information.

(a) Upon Service Provider's completion of its obligations associated with such SSBT

Confidential Information under the Services or termination of the Agreement for any

reason. whatsoever, Service Provider shall give SSBT no less than sixty (60) days’ prior

written notice of Service Provider's intent to destroy, or otherwise dispose of, any SSBT

Confidential information other than SSBT Personal Dafa, including but not limited to

destroy all notes, memoranda, compilations, derivative works, data files or other matetials

prepared by or on behalf of Service Provider that contain or otherwise reflect or refer to

“SSBT Confidential Information (“Other Relevant Records”) and which are not required

by applicable law to be kept by it, Service Provider shall not destroy any such Other

Relevant Records so as to render any and all SSBT Confidential Information permanently

unintelligible unless and until SSBT has been provided by the Service Provider with such

SSBT Relevant Records or has confirmed in writing that SSBT approves thet the same to

be destroyed. At SSBT’s request, Service Provider will certify in writing that it has

returned or destroyed all copies of SSBT Confidential Information and Other Relevant

Records in the possession or control of Service Provider or any of its affiliates, officers,

directors, agents, professional advisors, Approved Subcontractors and employees or other

Personnel, .

(b) If, at any time during the term of the Agreement any part of the SSBT Personal Data

ceases to be required by the Service Provider for the performance of Its ob] igations under

this Agreement, Service Provider shall promptly notify SSBT and retum to SSBT or‘at

‘SSBT's written request (but not otherwise) destroy, all coples of such SSBT Personal

Data in the Service Provider's possession or control no longer required, in a useable

machine-ready and industry standard format and on the media as agreed by the Partles

with prior notice to SSBT of such return and certify to SSBT that the same has been

completed, At any time during the Agreement, SSBT may request, in writing, that

Service Provider return, destroy or erase all coples of the SSBT Personal Data under

Service Piovider’s contro! or in its possession in which case Service Provider shall

promptly comply with all such requests in accordance with the foregoing obligations set

forth in this Section, as applicable, Under no circumstances shall Service Provider

withhold any SSBT Personal Data requested by SSBT.

(c) Notwithstanding anything herein to the contrary, Service Provider may retain copies of

SSBT Personal Data as requited by any record retention requirements applicable to

Service Provider under applicable law or as required to pursue or défend claims or other

actions under or relating to this Agreement and as otherwise consistent with its regulatory

and\_ audit ‘obligations, which ‘data shall remain subject to the confidentiality rights and

obligations hereunder notwithstanding termination of the Agreement.

Data Remediation, Service Provider shall implement and maintain procedures for

reconstructing SSBT Personal Data that is deleted, lost, destroyed or altered, Service

Provider shall remedy and correct, at SSBT’s request and at no charge te SSBT, any

destruction, loss, or alteration of any SSBT Personal Data caused by the Service Provider, its

Personnel, subcositractors or other agents or agents. Service Provider shall correct any errors

or inaccuracies In SSBT’s Confidential Information caused by Service Provider’s failure to

comply. with the provistons of this Agreement and promptly notify SSBT of any errors,

inaceutacies, material destruction, loss or alteration of SSBT’s Confidential Information

provided to Service Provider of which Seryice Provider becomes aware.

15

5.7.

5.8.

6.

6.1.

6.2,

6.3,

Survival, Service Provider’s confidentiality and non-disclosure obligations hereunder with

respect to SSBT Confidential Information and obligations of privacy will continue during the

term of this Agreement and survive expiration or termination. of the Agreement as follows: (i)

as to.any-portion of the SSBT Confidential Information that constitutes a trade seoret under

applicable law, the obligations will continue for as long as SSBT continues to treat such

information asa trade secret; and (Ii) as to all other SSBT Confidential Information, the.

obligations will survive for three (3) years after Service Provider’s fulfillment of Its

obligations under the Immediately preceding paragraph (Return or Destruction of”

Confidential information). .

Exclusions. The term Confidential Information shall exclude such information which is:

(a) alteady available to the public other than by breach of this Agreement;

(b) rightfully recelved from a third party not in breach of any obligation of confidentiality;

(ce) independently developed by either Party without access to the Confidential Information

‘of the other; or

(d) proven to be already known to the recipient at the time of disclosure,

Confidential Information may be produced in compliance with applicable law or a court

order, provided the Recipient first gives the Discloser reasonable notice of such law or order,

gives the Disctoser an opportunity to object to and/or limit such production and discloses only

that portion of Confidential Information which legal counsel to Recipient advises is required

by such law or court order.

Intellectual Property Ri

Deliverables. All Deliverables shall belong exclusively to SSBT. Service Provider

- acknowledges that al! Deliverables are being created for SSBT as “works made for hire” and

shall be the exclusive property of SSBT. To the extent the Deliverables are not deemed a

“work for hire” under applicable law, Service Provider hereby irrevocably assigns. and

transfers to SSBT all right, title and interest in the Deliverables, including but not limited to

patent and copyright interests and rights to create derivative works, and shall execute all

documents reasonably and provide all assistance necessary for SSBT to perfects in rights in

such Deliverables. All tangible written Deliverables shall contain a copyright notice as

follows: “[Description of code or deliverable as appropriate] is the copyxighted, proprietary

property of State Street Bank and Trust Company and its subsidieries and afflllates which -

retain all right,title and interest therein.” ”

Service Provider Tools, All of Service Provider's Standard Tools shall remain the property

of Service Provider. If any Standard Tools are used or incorporated. into Deliverables by

Service Provider in its performance of the Services hereunder, Service Provider hereby grants

to SSBT a petpetual, irrevocable, nonexclusive, worldwide, royalty-free, paid-up license to

use, display, copy and modify such Standard Tools. In addition, Service Provider grants to

SSBT a perpetual right to modify or eliminate any Standard Tool, or part thereof, that is

incorporated in a Deliverable solely for use with such Deliverable.

SSBT Personal Data, As between Service Provider and SSBT, the Parties acknowledge that

all SSBT ‘Confidential Information, Including but not limited to SSBT Persona! Data, is and

shall remain the exclusive property of SSBT and/or its Related Companies. SSBT reserves all.

Intellectual Property Rights which may subsist in SSBT Personal Data or SSBT Confidential

Information generally.

16

6. 4,

6,5.

6.6,

6.7.

6.8,

6.9.

6.19,

Assignment of Intellectual Property Rights. In the event that, at any time and from time to

time, through the provision of the Services the Service Provider is deemed by law to be the

first owner of any database right ot other Intellectual Property Rights in any SSBT

Confidential Information, the Service Provider will immediately- assign all Intellectual

Property Rights in that SSBT Confidential Information to SSBT, and will do such things, at

SSBT’s cost, as SSBT may reasonably consider necessary to give effect to this clause,

SSBT Content. All SSBT Content is owned ‘solely by SSBT and is the Confidential

Information of SSBT. Subject to the terms and conditions of this Agreement SSBT grants to

Service Provider a worldwide, royalty-free, non-exclusive and non-transferable license to

store, manage and use any SSBT Content providéd to Service Provider by SSBT, all solely in

connection with and for the purposes of providing the Services to SSBT hereunder. Such

license shali terminate immediately upon the termination of this Agreement or earlier, upon

completion of the Statement of Work.

.Third Party Content, All Third Party Content is owned solely by SSBT or the applicable

third party and shall-be considered the Confidential Information of SSBT and such third party.

Subject to the terms and conditions of this Agreement, SSBT grants to Service Provider a

limited, non-exclusive, non-transferable and revocable right to use, the Third Party Coritent

solely in connéction with and for the purposes of providing the Services to SSBT hereunder

subject to any restrictions Imposed by such third party. Such right of use shall terminate

immediately upon the misuse of such Third Party Content by Service Provider, the~

termination of this Agreement or upon completion of the Statement of Work, whichever

occurs first.

Limitations on Use of Intelleetual Property. Service Provider agrees that [t will not: ,

(a) permit any, third party to use SSBT Content or the Third Party Content;

(b) sell, rent, license or otherwise use SSBT Content or the Third Party Content in the

operation of a service bureau, or for any purpose other than as expressly authorized under

this Agreement; or

(c) allow or cause any information accessed or made avatlable through use of the SSBT

Content or Third Party Content to be published, redistributed or retransmitted or used for

any purpose other than as expressly authorized under this Agreement,

No Modifications; Reverse Engineering, Service Provider agrees not to, modify the SSBT

Content or the Third Party Content in any way, enhance or otherwise create derivative works

based upon the SSBT Content or the Third Party Content or reverse engineer, decompile or

otherwise attempt to secure the source code for all or any part of the SSBT Content or the

Third Party Content, without SSBT’s express prior consent.

Modifications. SSBT reserves the right to modify or eliminate any portion of the SSBT

Content, SSBT Personal Data or Third Party Content in any way at any time.

No Warranties, Because of the nature of computer information technology, including but

not {Imited to the use of the internet, and the necessity of relying upon thitd party technology

vendors, the SSBT Content, SSBT Personal Data or Third Party Content is provided “AS TS”

and SSBT FOR ITSELF, ITS SSBT RELATED COMPANIES AND ANY RELEVANT

LICENSORS EXPRESSLY DISCLAIMS ANY AND ALL REPRESENTATIONS AND

WARRANTIES CONCERNING THE SSBT CONTENT, SSBT PERSONAL DATA OR

THIRD PARTY CONTENT TO BE PROVIDED HEREUNDER, WHETHER EXPRESS,

IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION ANY. IMPLIED

17

6.11,

6.12.

7,1.

7.2.

WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A

PARTICULAR PURPOSE OR QUALITY OF SERVICES.

Export. Setvice Provider acknowledges that certain software, technical data and other

information to be provided heteunder and certain transactions hereunder may be subject to

export controls under the laws.and regulations of one or more jurisdictions. Service Provider

will not export or ré-export-any such items or any direct product thereof or undertake any

transaction in violation of any such laws or regulations. Service Provider will be responsible

for, and will co-ordinate and oversee compliance with such export Jaws in respect of such

items exported or imported hereunder. '

Termination. SSBT may terminate use of the SSBT Content, SSBT Personal Data or the

Third Patty Content by Service Provider Immediately and without prior notice in the event of

the failure of such person to comply with the provisions of Sections 6.7 or 6.8.

Compliance with Law; Change in Law

Compliance. Hach Party will perform its obligations hereunder in a manner that complies

with all applicable U.S. federal and state laws, rules, regulations, and applicable non-U.S.

laws, regulations, ordinances, directives, decisions and codes (including identifying and

procuring required permits, certificates, approvals and inspections and any relevant Data

Protection and Privacy Laws). If a charge of non-compliance by. either Party with any such

laws, regulations, ordinances, directives, decisions, policles or codes is made, the Party

charged with such non-compliatice will promptly notify the other Party of such charges in

writing and any remediation plan,

Notice of Material Adverse Effects, Service Provider will promptly notify SSBT of:

(a) any notice of violation of any applicable statutes, ordinances, orders, directives, decisions,

judgments; decrees, rules or regulations promulgated by any regulatory, administrative or

judicial authority that relates to the performance of the Services or which mey have a

material adverse effect on its ability to fulfill its duties and obligations under this

Agreement; :

(b) the commencement of any litigation or any regulatory, administrative or judicial

proceeding or investigation adverse to Service Provider that relates to the performance of

the Services or which may have a material adverse effect on its ability to fulfill its duties

and obligations under this Agreement or relating to any breach of privacy or security;

(c) any material adverse change in the financial condition of Service Provider including in

any event of a downgrade by a nationally recognized ratings agency or removal of

Service Provider from any nationally recognized securities trading exchange by any.

regulatory and exchange authority or loss of a client from which Service Provider

recelves a material portion of its aggregate revenues;

(d) any other event relating to Service Provider which may have a material adverse effect on

its ability to perform the Services or fulfill its duties and obligations under this

Agreement, as the case may be, including, but not limited to, any applicable statutes,

ordinances, orders, judgments, directives, decisions, decrees, rules or regulations that

: would have a substantial adverse effect on the confidentiality, privacy or security-related

obligations provided for under this Agreement; /

18

7.3.

8

8.1,

8 edie

8.3.

8.4.

8.5.

(e) any breach or suspected. breach by Service Provider or its Personnel, Approved

Subcontractors, agents ot others of any security, confidentiality or privacy provision

hereunder; ‘ ‘

(f) any misuse of, or‘improper access to any proprietary intellectual property of SSBT or

SSBT Confidential Information; and

(g) any breach or suspected breach of Service Provider's Security Policy which results in, or

which may result in, Improper access to the information or data of any client of Service

Provider together with details as to such event.

Financials, Setvice Provider will furnish to SSBT such financial data, information and

statements as SSBT may reasonably request in order for SSBT to verify the financial

condition of Service Provider and its ability to perform the terms of this Agreement,

including, without limitation and if so requested, audited balance sheet, statement of income,

changes in stockholders’ equity and changes in financial position for any period reasonably

requested by SSBT,

Global Data Protection and Privacy

Service Provider certifies and continues to certify during the terms of this Agreement ‘that

Service Provider and each of its Related Companies adhere to the Safe Harbor Agreement

between the U.S. Department of Commerce and the European Commission with respect to

personally identifiable Information that {s transferred from the European Econotnic Area to

the United States (the “Safe Harbor Certification”) in accordance with the terms set forth in

Schedule:C-2. In lieu of executing the Data Processing Agreement, Service Provider shall

comply with the terms of Schedule C-2 which, together wiih the terms of this. Agreement,

shall govern the processing of any and all SSBT Personal Data terms under this Agreement

(the “Safe Harbor Certification”). .

If, at any time during the term of this Agreement the Service Provider or any of its Related

Companies fail to comply with Section 8.1 above, Service Provider shall comply with the

terms of Schedule C and complete and execute the Data Processing Agreement substantially

in the form of Schedule C-] attached to this Agreement (“Data Processing Agreement”),

which agreement, together:with the terms of this Agreement, will govern the processing of

any and all SSBT Personal Data in connection with the Services,

For avoidance of doubt, the Security Schedule shall apply to the processing of any SSBT

Personal Data, itrespectlve of which jurisdiction the data subject resides and notwithstanding

the fact that the Service Provider has executed the Data Processing Agreement or,

alternatively; complies with the terms of the Safe Harbor Certification.

To the extent that it is determined by any data protection authority that this Agreement, the

Data Processing Agreement or the Safe Harbor Certification is insufficlent to comply with the

applicable Data Protection and Privacy Laws or to the extent required otherwise by any

changes in the applicable Data Protection and Privacy Laws’ or the enactment of new Data

Protection and Privacy. Laws during the Term, the Parties agres to work cooperatively and in

good falth to amend this Agreement or execute Data Processing Agreements, if any, in a

mutually agreeable and timely manner or to enter into futher miutually agreeable data

processing agreements in an effort to comply with any Data Protection and Privacy Laws

applicable to the Parties.

Service Provider shall take such actions, ‘without further consideration and at Service

Provider's expense, necessary to protect SSBT Personal Data against unauthorized, or

19

8, 6.

8.7,

9,

9.1,

9,2.

unlawful processing and accidental or intentional loss, destruction or damage as are

appropriate to SSBT as data controller or owner of the SSBT Personal Data and/or satisfy

within a timely manner requests or requirements of relevant governmental or data protection

regulatory authorities, provided that Service Provider shall not be obliged to take any

measures higher than that required by law, without additional charge to SSBT,

SSBT shall have the responsibility to notify all its employees, contingent workers ot

particlpants as may be required by applicable Data Protection and Privacy Laws of the

“collection and Intended usage of their personal data. Service Provider shall provide SSBT

with any and all. informatlon, including applicable SSBT Personal Data, which SSBT requires

to respond, in atimely manner and in compliance with applicable Data Protection and Privacy

Laws, to any inquiries, notices, claims or demands brought by a data subject in connection

with the usage of their personal data,

Upon the request of SSBT or one ofits Related Companies, Service Provider shall;

(a) enter into additional Data Processing Agreements as SSBT may require, and

(b) use reasonable efforts to cooperate In connection with the preparation of the additional

Data Processing Agreements and any required annexes to such additional Data Processing

Agreements, including providing any additional information cequested by the relevant

data protection authorities within the period of time specified by such authorities, or, if no

time period is specified by the applicable data protection authorities, within a reasonable

time.

Warranties

Performance, Service Provider represents and warrants and undertakes that:

(a) the Services provided hereunder will be performed by qualified Personnel in a good and

workmanlike manner in the estimated and projected time specified in the applicable

Statement of Work or project plan;

(b) the Deliverables and Services will conform to the specifications stated in the applicable

Statement of Work;

(c) if applicable, the Deliverables will process information with respect fo securities

designated in multiple currencies;

(d) if applicable, the Deliverables will process information with respect to securities

designated in decimals;

(e) neither the Deliverables nor any update or revision thereof will include any virus or

mechanism that is designed to delete, disable, Interfere with or otherwise harm the

Deliverables (or SSBT's hardware, data or other programs), make It inaccessible to SST

once the Deliverable has been installed, or that is intended to provide access to or produce

modifications not authorized by SSBT; and

(f) no Deliverable will contain open source software or freeware unless SSBT has

specifically authorlzed such use in writing,

Execution, Delivery, Ete, Service Provider represents, warrants and undertakes that the

execution, delivery and performance by Service Provider of this Agreement including, but hot

limited to, any Data Processing Agreements executed by the Parties:

20

9,3.

9.4,

9.5,

(a) are within Service Provider’s corporate powers,

(b) have been duly authorized by all necessary corporate action under its organizational

documents,

(c) require no action by or in respect of, or filing with, any governmental body, agency or

official other than those which have already been duly taken or made or will be duly

taken or made as arid when required, ,

(a) require no consents or approvals with respect to any data subject to Data Protection and

Privacy Laws which Is provided by Service Provider to SSBT, including any Personnel

placed at SSBT as part of the Services provided by Service Provider other than those

which have alréady been received,

(e) do not contravene or constitute a default under any provision of appileable law, regulation

or decision or of the organizational documents of Service Provider or any agreement,

judgment, order, decree or other instrument binding upon Service Provider, and

(f) this Agreement constitutes a legal, valid and binding obligation.

Service Provider agrees to Inform SSBT immediately if any statement set forth in this Section

9.2 ceases to be true and correct as of any date after the date hereof, . ©

Litigation, Service Provider represents and warrants that it is not the defendant in any

litigation anywhere in the world:

(a) which if determined adversely would have a material and adverse effect on Service

Provider's ability to perform the Services or comply with the terms of the Agreement; or

(b) concerning the infringement and/or misappropriation of any Intellectual Property Rights

" and nto claims are pending relating to any intellectual property services performed or

products developed by Service Provider.

“In addition, Service Provider represents and warrants that it is not the subject of any

investigation or proceeding initlated by any governmental or regulatory authority and will

notify SSBT upon the commencement or any such Investigation or proceeding,

Records Retention, Service Provider yepresents and wacrants that it shall keep proper and

sufficlent books of account and records atid supporting documentation sufficient to document

the performance of its obligations heveunder and the related fees charged to SSBT with

respect to Services provided hereunder and shal! make such books of account and records and

supporting documentation available to SSBT for audit and In connection with a response to a

regulatory authority. Sorvice Provider representsafd warrants that it shall retain such books

-of account, records and supporting documentation until not earlier than seven (7) years

following the completion of the Services to which such performance and fees relate,

Employees. Service Provider -represenits and warrants that it has entered into agreements

with:

(a) each of its employees, wherein Service Providers’ employees acknowledge that they are

employees of Service Provider and not employees of SSBT, and waive any and all

employment related claims they may have at any time against SSBT, even If subsequently

deemed to be an employee of SSBT; and

21

9.6,

57,

9.8.

(b) each of its subcontractors requiring the subcontractor to enter into agreements with each

of its employees containing the provisions set forth above in {a). \_

Preparation of Examination Reports. To the extent the Services provided by Service

Provider involve hosting services for SSBT or the processing of data belonging to SSBT or its

clients in the capacity as an outsourcer of SSBT, Service Provider represents and warrants

that {t shall, at its sole expense, engage its‘ independent outside accounting firm to prepare

petlodic reports (“Examination Reports”) in compliance with the ptovistons of the American

Institute of Certified Public Accountants’ (“AICPA”) Statement on Auditing Standards No,

70, Reports on the Processing of Transactions by Service Organizations (“SAS 70”), the

AICPA’s Statement on Standards for Attestations Engagerhents No. 16, Reporting on

Controls at a Service Organization (“SSAB 16"), any successor U.S, standards or guidellnes

to the same or analogous standards or guidelines in non-U.S, jurlsdictions (collectively,

“Auditing Standards”), evaluating the Services performed by Service Provider (to the extent

that the Auditing Standards contemplates the evaluation of such Services). Service Provider

represents and warrants that it shall promptly provide SSBT with true and correct copies of

any Examination Reports prepared pursuant to this Section 9.6 and agrees that it will

promptly remedy atty shortcomings disclosed in any Examination Reports and implement any.

reasonable recommendations contained therein as to such shortcomings. To the extent

compliance with the Auditing Standards requires, or the Parties reasonably mutually agree on,

the joint prepatation of the Examination Reports evaluating the Services performed by

Service Provider, SSBT shall, and shall cause Its independent outside accounting firm to,

cooperate in good faith with Service Provider and Its independent outside accounting firm to

jointly prepare such Examination Reports and the Parties shall each pay their respective costs

of sich preparation.

Disaster Recovery/Business Continuity. Service Provider represents and warrants that it

shall develop and implement, at its sole expense, an adequate disaster recovery plan to ensure

disaster recovery/business continuity and back-up capabilities for the Services, Service

Provider shall provide SSBT with a written copy of its disaster recovery/business continuity

plan and any material modification promptly upon SSBT’s request. Additional information

regarding Service Provider’s disaster tecovery/business continuity procedures, including

business recovery timeframes, will be included, as needed, in the applicable Statement of

Work. Inthe event of

(a) a Force Majeure Event that has had or may have a catastrophic effect on the ability of

Service Provider to provide Services to SSBT or SSBT to receive the Services or receive

and use any Deliverable, or

(b) a security breach of SSBT or Service Provider's facilities or SSBT’s Confidential

Information,

Service Provider shall notify SSBT of the same in writing (a “Disaster Notice”) within 24

hours and shall develop any work-around that is necessary to ensure that SSBT continues to

recéive the Services.

Background Investigations. Service Provider represents and warrants that, as patt of its

standard hiring and vendor due diligence practices, Service Provider Personnel assigned to

perform the Services or otherwise having access to SST Confidential Information shall be

subject to appropriate pre-employment background investigations performed by or on behalf

of Service Provider consistent with industry standards taking into consideration the

confidential nature of the Services to be performed and the risk and severity of damage to

SSBT or others that might result from Personnel’s negligence or wrongful conduct. Service

Provider shall. make available, upon request from SSBT, evidence (such as invoices for

services) that will not pose a privacy issue that the background investigations have been

22.

9.9.

910,

9,11,

9.12,

performed on such Personnel. In addition, Service Provider shali ensure that any Service

Provider Personnel assigned to work an any SSBT engagement remains compliant with all

applicable laws, roles and regulations, including without limitation, those telating to

immigration, — . ;

Green, Policy. Service’ Provider represents and warrants that it has and will maintain a

responsible environmental “green” policy whereby Service Provider makes responsible use of

environmental resources and exercises conservation of natural resources. ‘

Gift Policy. Service Provider represents and warrants that it has and will maintain a gift -

policy prohibiting any employee of Service Provider from providing gifts or entertainment of

a matertal value to employees of clients or parties receiving Services from Service Provider in

return for favorable treatment of any kind,

Deemed Export, Service Provider represents and warrants that it will not provide access,

yelease or transfer any Client technology or Information to any third party or employee of

Service Provider which could be considered as a “deemed export” of such Client technology

or information under applicable U.S. Export Administration Regulations, International Traffic

or Atms Regulations, or regulations of the U.S. Department of Commerce or U.S. Department

of State,

Corrupt Practices, Service Provider represents and warrants that it shalt not engage in

- corrupt, unfair of fraudulent practices in connection with the provision of the Services

9.13.

10.

10.1.

hereunder, including, but not limited to, the Service Provider or its Pers onnel accepting bribes

or making offers, payments, or promise to pay to any person, including, but not limited to, an

executive, official, employee or agent of (Gj) a governmental department, agency of

instramentality, (ii) a wholly or partially government-owned of controlled company or

business, or (Iii) a political party (collectively, “Government Official”), for the purpose of

influencing aty act, decision or failure to. act by such persons or Government Officials or

securing an improper advantage In order to obtain, retain ot direct business.

DISCLAIMERS. THE SERVICE PROVIDER WARRANTIES STATED HEREIN SHALL

BE IN LIEU OF ANY AND ALL OTHER WARRANTIES EXPRESS OR IMPLIED,

INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Indemnification

Intellectual Property Indemnification,

(a) By Service Provider, Service Provider shall defend at its sale cost and expense or, at its

option, settle, any claim or proceeding brought against SSBT or SSBT Related Company

to the extent that itis based on an assertion that the Deliverables or the Services constitute

infringement of any Intellectual Property Rights, and shali indemnify and hold SSBT

harmless from and agalnst all costs, damages and expenses, including reasonable

attomey’s fees, asserted against SSBT or SSBT Related Company which result from any

such claim, Without limiting the generality of the foregoing, should the Deliverables or

Services or any part thereof become, or in Service Provider's opinion be likely to become,

- the subject of a clalm of infringement or the like under applicable patent or copysight or

trade secret laws, Service.Provider shall either procure for SSBT the right to continue

using the Deliverables or Services, or to replace or modify the Deliverables or Services,

without changing thelr functional capabilities, so that the Deliverables or Services

becomes non-infringing, If Service Provider is unable to do either of the foregoing within

thirty (30) days, upon request, Service Provider shall refund the entire fees paid to Service

23

10.2.

10.3.

10.4.

10.5,

10.6,

“Provider by SSBT prorated to reflect use of the Deliverable or Services by SSBT or any

SSBT Related Company prior to commencement of the Claim or proceeding described

-herein,

(b) By SSBT, SSBT shall defend at its sole cost and expense or, at its option, settle, any

claim or proceeding brought against Service Provider to the extent that it is based on an

assertion that the SSBT Content constitutes infringement of any Intellectual Property

Rights, and shall indemnify and hold Service Provider harmless from and against all

costs, damages and expenses, including reasonable attornéy’s fess, asserted against

‘Service Provider which result from any such claim, provided that Service Provider

notifies SSBT promptly in writing of any such claim or proceeding. This subsection shall

constitute Service Provider's sole remedy as to matters covered in this subsection.

Personal Injury and Property Damage, Each Party shall indemnify, defend, and hold

harmless the other Party from and against all claims and actions and all damages, costs and

expenses incidental to such claims or actions (including reasonable attorney’s fees), based

upon or arising out of damage to property or injuries to persons or other tortuous acts caused

or contributed to by the indemmifying Party or anyone acting under its direction or coritrol or

on its behalf in the course of its performance under this Agreement, provided that each

Party’s aforesaid indeinity and hold harmless agreement shall not be applicable to any .

Tability based upon the negligence of the other Party,

Employment Claims. Service Provider shall indemnify, defend and hold harmless SSBT

from and.against all claims and actions and all damages, costs and expenses incidental to

claims or actions (including reasonable attorneys’ fees) based upon or arising out of any

employment related claims by Service Provider's Personnel or subcontractors, or Personnel of

Service Provider's subcontractors, including without Limitation, for any médical coverage, life

insurance, or other benefits from SSBT which may be afforded to SSBT’s Personnel and

other matters for which Service Provider is responsible pursuant to this Agreement, including

Section 2.8 and any immigration and employment related issues and requirements which may

atise in connection with such Personnel,

Confidentiality/Data Protection Claims. In the event of a breach of any provisions of

Section 5 or 8 of this Agreement by Service Provider, any of Its Related Companies, or any of

their current or former Personnel, directors or officers, or failure to perform any of Service

Provider's obligations and responsibllities hereunder and more specifically, with réspect to

the breaches of the Data Protection and Privacy Laws, the Service Provider shall be liable to

~ SSBT, SSBT’s Related Companies, as well as their Personnel, clients, parents, subsidiaries or

affiliated companies, as applicable, for any damages caused thereby, Ifa data subject is not

able to bring an action against SSBT. arising out of a breach by the Service Provider as the

data importer of any of the Service Provider’s obligations under this Agreement arising under

the transmission of SSBT Personal Data to the Service Provider becayse SSBT has

disappeared factually or has ceased to exist in law or became insolvent, the Service Provider

agrees that the data subject may issue a claim against the Service Provider as data importer as

if Service Provider were the data exporter.

‘Content Indemnification, Service Provider shaJl indemnify, defend and hold harmless

SSBT from and sgainst all claims and actions and all damages, costs and expenses incidental

to claims or actions (including reasonable attorneys’ fees) based upon or arising out of

Service Provider's of its current or former Personnel use of any SSBT Content or Third Party

Content in violation of this Agreement (excluding claims under Section 10,1(b)).

Indemnification Procedures, Promptly after the receipt by a Party (the “Indemnified Party”)

of notice of any claim, determination, suit or cause of action with respect to which the other

Party is obligated to provide indemnification (the “Indemnifying Party”) pursuant to this

24.

IL

11.1,

11,2,

\* 12,

12.1.

12.2.

Agreement, the Indemnified Party shall give the Indemnifying Party written notice thereof,

provided, however, that any delay by the Indemnified Party to so notify the Indemnifying

Party shall relieve the Indemnifying Party of its indemnification obligations only to the extent

that such delay materially prejudices the Indemnifying Party's defense, The. Indemnifying

Party shall be entitled to assume control of the defense and the negotiations, if any, regarding

settlement of this matter, If the Indemnifying Party assumes such control, the Indemnified

Party shall be entitled to participate in the defense and negotiations of such matter at its own

expenses if thé Indemnifying Party does not assume control of the defense and negotiations,

the Indemtiified Party may conduct such defense and negotlations and its reasonable costs and

expenses shall be subject to indemnification. The Patties agree, at the Indemnifying Party’s

expense, to reasonably cooperate in'such negotiations, defense or settlement and to give each

other full access to any information relevant thereto. The Indemnified Party shall not enter

into any settlement of such matter without the written consent of the Indemnifying Party, and

the Indemnifying Party shall not be obligated to indemnify the Indemnified Party for any

settlement entered into without the written consent of the Indemnifylng Party, Ifthe consent

of the Indemnified Party is required to effectuate any settlement negotiated by the

" Indemnifying Party, then such consent shall not be unteasonably withheld.

” Limitation of Ciabili

Cap on Liability. Except for claims under Sections 5, 6, 8, and 10 and except for gross

negligence, willful misconduct and fraud the Parties agree that the total liabillty ofeach of the

Parttes for any breach of its obligations under this Agreement shall not exceed the total of

fees recelved by Service Provider under any Statement of Work out of which such liabliity

arises,

EXCLUSION OF DAMAGES. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO

THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY INDIRECT, PUNITIVE,

INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT

LIMITED TO SUCH DAMAGES ARISING FROM BREACH OF. CONTRACT OR

WARRANTY OR FROM NEGLIGENCE OR STRICT LIABILITY), IN CONNECTION

WITH THIS AGREEMENT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE

POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE LEGAL OR

BQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH THE

CLAIM IS BASED. .

Project Management

Project Managers. Service Provider and SSBT each shall appoint a project manager (each a

“Project Manager”), Each Project Manager will meet regularly and will work together toward

a timely implementation in accordance with the Statement of Work. The Project Managers

will plan the project, select and agree on resources, quality check the activities and progress

of the project, and resolve any disputes that may arise. Service Provider's Project Manager

will be acceptable to SSBT and be the primary contact for SSBT in dealing with operational,

performance or other issues atising under the Agreement. Service Provider's Project

Manager will have overall responsibility for directing all of the Service Provider's activities

including, but not limited to, the overall managing and coordinating of the delivery of

Services, and will be vested with all necessary power and authority to fulfill that

responsibility and make decisions on behalf of Service Provider with respect to actions to be

taken in the ordinary course of day to day performance of Services under this Agreement.

Steering Committee,

(a) If requested by either Party, Service Provider and SSBT each shall appoint an executive

sponsor and establish a steering cominitiee, which shall include the executive sponsors

25

12.3.

13.

13, 1,

13.2.

\_and the Project Managers (“Steering Committes”) for the purpose of facilitating

communications and’ establishing a formal escalation procedure to resolve any disputes

between the Parties. ‘

(b) The Steering Committes will review: perlodic progress reports prescribed by the’ project

management team of SSBT and Service Provider, meeting perlodically to discuss the

statug, scope, and budget of the project, as well as the roles and responsibilities of project

management. The Steering Committee will also aid in resolution of disputes that cannot

be resolved by the prospect mandgement. Each executive sponsor will serve as a liaison

between the project management team and executive management, In addition to serving

on the Steering Committee, executive sponsors will assist in resolving open issues

remaining within the Steering Committee.

Project Management Procedure. In order to maintain communications between the Parties,

Service Provider and SSBT shall ensure that the following procedures are in place:

(a) Regularly scheduled Project Managers meetings to present and discuss issues, to ensure

project Deliverables and milestones are met within the established timeline;

(b) Biweekly Steering Committee meetings to review project status and provide status

updates; and

(c} Progress reports, summarlzing accomplishments, difficulties, potential or actual slippage

in meeting deadiInes, hours worked in excess of estimates, Deliverables completed, and

tasks in progress.

Escalation Procedure

Scope. Any dispute, controversies or claims arising under this Agreement (each, a “Dispute”)

shall be subject to the escalation process set forth in this Section 13; provided, however, that,

notwithstanding anything to the contrary in such Agreement, a Party may - institute

proceedings for appropriate equitable relief if it makes a determination that a breach (or

potential breach) of the terms of this Agreement by the other Party may result in damages or

consequences that shall be immediate, severe and incapable of adequate redress after the fact,

so that 4 temporary restraining order or other immediate injunctive relief is the only adequate

remedy. Any provisional relief obtained pursuant to this Section 13.1 shall be limited as

appropriate to preserve the exclusive jurisdiction of the courts of the Commonwealth of

Massachusetts courts to resolve the dispute between the Parties.

Escalation Procedures,

(a) If either Party identifies a Dispute that requires resolution, it will give the other Party’s

Project Manager prompt written notice thereof, The Parties’ Project Managers will then

fegotiate in good faith on a regular and frequent basis to resolve the Dispute as

expeditiously as feasible, If the Project Managers are unable to resolve the Dispute

within a reasonable period of time not to exceed ten (10) days after notice of the Dispute

is given unless extended by agreement of the Partles, either Project Manager may refer

the Dispute to the Steering Committee,

(b) Promptly after referral as provided iri subparagraph (a) above, the members of the

Steering Committee will negotiate in good faith on a regular basis to resolve the Dispute

as expeditiously as feasible, bit no later than thirty (30) days after referral. If the

members of the Steering Committee are unable ‘to resolve the Dispute within such time

frame, the Steering Committee may sefer the Dispute to the senior executive of SSBT

26

14.

14.1 a

14,2,

14.3.

having management responsibility for the Service Provider relationship and the seniot

executive or other manager of Service Provider with management responsibility for the

SSBT relationship (collectively, the “Senlor Executives”).

(c) Promptly after referral as provided in subparagraph (a) above, the Senior Executives will

negotiate in good faith on a regular basis to resolve the Dispute as expeditiously as

feasible, but no later than thirty (30) days after referral. Thereafter, the Senior Executives

will submit a joint written recommendation for any issue(s) of the Dispyte upon which

they agreed and separate written recommendations for any issue(s) of the Dispute upon

which they disagreed upon or which remain unresolved. SSBT and Service Provider

agree to bé bound by such joint written. recommendation and to deem the issue(s) the

Senior Executives agreed upon to be no longer included in the Dispute. Either Party may

seek to resolve arty issues that remain unresolved through Litigation,

(d) The purpose of preparing and submitting the written recommendation desoribed above (or

any other report or statement on the matter) (collectively, “Dispute Statements”) is to

facilitate the resolution process, However, the Dispute Statements will not limit either

Party froin identifying any additional relevant jssues during the resolution process, nor

will the Dispute Statements constitute a waiver of, or prejudice or limit either Party’s

rights or remedies with respect to, the issue(s) addressed therein. Moreover, the Dispute

Statements shall not constitute an admission by cither Party and shall not be used by

either Party for any purpose other than to demonstrate the Issues that had been agreed

upon by the Parties,

(©) Service Provider shall not be permitted to terminate any Services because of a Dispute

provided that the Parties are working in good faith towards the resolution of the Dispute

in accordance with the terms of these escalation procedures.

Term and Termination

Term, This Agreement shall be effective when signed by both Parties-and thereafter shal!

remain In effect until terminated in accordance with the terms hereof (‘‘Term”), Each

Statement of Work shall be effective when signed by both Parties, and thereafter shall remain

in effect until terminated: ,

(a) as provided in the applicable Statement of Work, or

(b) in accordance with the terms of this Agreement.

Termination for Convenience. SSBT may terminate this Agreement and/or.any Statement

of Work at any time for SSBT’s convenience upon the provision of thirty (30) days prior

written notice to Service Provider. During such thirty (30) day period, Service Provider shall

only perform Services necessary to wind down and exit the engagement described in the

Statement of Work during such thirty (30) day perlod and tasks associated with knowledge

transfer, Unless otherwise specifically stated in the applicable notice of termination, SSBT's

termination of any Statement of Work for convenience shall not result in the automatic

termination of this Agreement. For any engagement which is on a time and materials basis,

SSBT may limit or suspend any further Services at any time upon five (5) days prior notice

without termination of any Statement of Work and without liability hereunder.

Termination for Cause, Either Party may term{nate this Agreement or a Statement of Work

upon written notice (“Termination for Cause”) if the other Party:

27

14,4,

15.

16. —

(a) ceases doing business and its business is not continued by another corporation or entity

which has agreed to assume such Party’s obligations to which SSBT consents In writing;

(b) files for or becomes a Party to any involuntary bankruptcy, receivership or similar

\* proceeding, and such proceeding is not dismissed within forty-five (45) calendar days

after filing:

(©) takes an assignment for the benefit of creditors; of

(d) fails to perform any term or provision of this Agreement in accordance with the Statement

of Work and such failure to perform continues for a period of thirty (30) days after receipt

of such written notice,

In addition to the foregoing, SSBT may terminate this Agreement for cause in the event that

Service Provider becomes thé subject of a criminal and/or regulatory proceeding and/or

investigation and such proceeding and/or investigation may impact SSBT’s receipt of the

Services on the terms provided in the applicable Statement of Work.

Transition Cooperation, Service Provider agrees that upon termination of this Agreement or

Statement of Work for any reason it shall provide sufficient efforts and cooperation to ensure

an oyderly and efficient transition of the Services to SSBT or another vendor. Service

Provider shall provide full disclosure to SSBT of the product and Services and any third party

suppliers required in the performance of this Agreement, Except as provided herein with

respect to transition cooperation, upon the termination of this Agreement, Service Provider

shall immedlately discontinue the provislon of all Services to SSBT,

Major Competitors

Service Provider shall not offer services to SSBT’s clients in competition with SSBT. If so

provided in a Statement of Work, no Service Provider Personnel identified in the Statement of

Work shall during the period of their. assignment under the Statement of Work and for a

period of one hundted eighty (180) days from the last day of their assignment shall be

assigned to a similar project under which they participate for SSBT’s major competltors, as

’ defined in the Statement of Work, The list of Service Provider Personnel subject to these

"restrictions, as set forth in the Statement of Work, and the list of major competitors, as set

forth In the Statement of Work, may be reviewed and updated from time to time as may be

appropriate. —

Audit Rights

Service Provider shall permit one or more SSBT Personnel or agents (including SSBT’s

internal or external auditors and such governmental and data protection authorities governing

SSBT and SSBT Related Companies), at such times as shall be reasonably’ requested, to

inspect and take extracts fiom any records (redacted to remove references to matters unrelated

to the materials or Services under this Agreement) maintained by Service Provider or its

subcontractors in connection with this Agreement and any Statement of Work and to visit and

inspect any premises where services are being performed (including, as applicable, walk- -

through of primary and backup data centers, subject to. generally-applicable restrictions

imposed by any third party operators of such data centers) to verify that Service Provider is

employing reasonable procedures in compliance with the terfns of this Agreement including

without limitation as to confidentiality and data security obligations hereunder. At SSBT’s

request, Service Provider shall provide SSBT or its Personnel or agents with any reports of

Service Provider’s internal and externa! auditors in connection with Service Provider's system

of intemal accounting controls as they relate to Service Provider's controls and security

requirements atd the Services under this Agreement (redacted to remove references to

28

17.

17.1.

17.2.

17.3.

1 7.4.

matters unrelated to such services) and remedial plan to address any deficiencies set out in the

report.

General

Force Majeure: Neither Party shall be liable for any acts or omissions resulting from a Force

Majeure Event. The Party affected by an Force Majeure Event, upon giving prompt notice to

the other Party, shall be excused ftom performance hereunder on a day-to-day basis to the

extent of such prevention, restriction or interference (and the other Party shall likewise be

excused’ from performance of its obligations on a day-to-day basis to the extent that such

obligations relate to the performance so prevented, restricted, or interfered with); provided

that the Party so affected shall use all commercially reasonable efforts to avoid or remove

such cause-of non-performance and to minimize the consequences thereof and both Parties

shall resume performance hereunder forthwith upon removal of such cause, In the event-that

any Force Majeure Event continues for longer than ten (10) days, SSBT may terminate this

Agreement immediately upon the provision of written notice to Service Provider.

Assignment, Neither this Agreement nor any rights and duties hereunder may be assigned or

transferred, by. operation of law or otherwise, or delegated by SSBT or-Service Provider

without the prior written consent of the other Party. SSBT may assign this Agreement to a

subsidiary or affiliate or a successor in interest in case of a merger or acquisition of SSBT or

in case of a transfer of all or substantially all of its assets, or the assets of a major division, to

another Patty. This Agreement shall be binding and shall inure to the benefit of any such ©

successors and’ assigns of the respectlve Parties,

Notices, Any notice or other communication given or permitted hereunder shall be in writing

and mailed by registered or certified mail or overnight courler as follows:

Ifto Service Provider, to:

MetricStream, Inc, =

2600 E, Bayshore Road

Palo Alto, CA 94303

Attention: Controller

If to SSBT, to:

State Street Bank and Trust Company

One Lincoln Street

Boston, Massactiusetts 02111

Attention: ITAM

State Street Bank and Trust Company

One Lincoln Street

Boston, Massachusetts 02111

Attention: Chief Procurement Officer

of to such other address as either Party shall have theretofore designated by notice in writing.

Such notice shall be deemed to have been given on the date such notice is deposited in the

matl, duly addressed, and with postage prepared by the other Party.

Insurance, Service Provider represents that it now carries, and agrees that it will continue to

carry, with insurers having a Best Rating of A, at a minimum, insurance In the following

amounts:

Auto Liabili $ 1,000,000

29

17.5,

17.6.

17.7,

17.8.

Employers Liabilit

Statuto

Workers Compensation

In addition, SSBT may require additional insurance coverage depending upon Service

Provider's business or the work to be performed by Service Provider on behalf of SSBT. .

If requested by SSBT, certificates of all such insurance indicating that SSBT, its parent,

subsidiaries, affiliates and their respective officers, agents and employees, have been named

as additional insured’s where applicable, shall be provided to SSBT and sfiall contain a

provision that SSBT shall receive thirty (30) days’ written notice of cancellation or

modification of all such insurance coverage. To the extent that Service Provider is based

outside of the United States and/or will be providing any Services from outside of the United

States, Service Provider shall ensure that its insurance coverage applies to losses occurring

outside of the United States. Service Provider’s policy will be considered primary coverage

for claims arlsing out of the contractual relationship.

No Waiver. Any failute by either Party hereto to enforce at any time any term or condition

under this Agreement shall not be considered a waiver of that Party's right thereafter to

enforce each and every ferm and condition of this Agreement.

Titles, The titles to the paragraphs of this Agreement are solely for the convenience of the

Parties and are not an aid in the interpretation of this Agreement.

Affirmative Action, SSBT is afi equal employment opportunity employer and is a federal

contractor. Consequently, the Parties to this contract agree that, to the extent applicable, they

will comply with Executive Order 11246, the Vietnam Era Veterans Readjustment Assistance

Act of 1974 ard the Rehabilitation Act of 1973. The Parties to this contract further agree that

these laws and their implementing regulations, as applicable, are incorporated herein by this

reference. ,

Governing Law and Jurlsdiction; Arbitration, This Agreement is deemed to be made

under and shall be construed according to the laws of the Commonwealth of Massachusetts

without giving effect to principles of conflicts of laws. Except for actions for injunctive relief

initlated by SSBT to protect SSBT Confidential Information, which may be brought In any

court of competent jurisdiction, all action relating to thls Agreement shal! be brought in thie

appropriate state or federal court located In Boston, Massachusetts. Bach of the Parties

irrevocably consents to the jurisdiction and venue of the fedetal and state courts. of the

Commonwealth of Massachusetts. To the extent SSET reasonably believes that any non-

United States jurisdiction in which any Services are performed or which may apply to the

Services may: not recognize or enforce any Massachusetts or other United States law

provision or judgment rendered by a United States judicial or administrative entity, SSBT

inay submit any dispute to any applicable international arbitration tribunal for arbitration in

accordance with the arbitration rules at the thne applicable in the applicable jurisdiction. The

arbitration. tribunal will consist of three arblirators, The language to be uséd will be both

Bnglish and the language of the local non-United States jurisdiction. An arbitration award

rendered by such a tribunal will be enforceable under the Convention on the Recognition and

Enforcement of Foreign Arbitral Awards (1958). The arbitration fee will be borne by the

30

losing Party unless otherwise determined by the arbitration award. During the course of

arbitration this Agreement will continue to be performed.

17.9, Reference and Publicity, Service Provider shal! not use, and shall cause Its employees and

-other Personnel, and any Approved Subcontractors and agents to yefrain from using,

(a) SSBT's name or the name of any SSBT Related Company;

(b) the name of any employee or other Personnel of SSBT or any SSBT Related’ Company;

and ;

(c) a logo, irademak or any other {intellectual property of SSBT or any SSBT Related

Company in any marketing or advertising materials, customer Jists of any website of

Service Provider without SSBT’s prior wtilten approval, which may be withheld for any

yeagon, . .

17.10. Tnjunctive Roltef, Tie Parties agrees that money damages may not be a sufficlent semedy

for any breach of this Agrecment Involving the disclosures’ of the Parties’ Confidential

Information. Ag such, each Party shall be entitled to seek specific performance and injunctive

or other equitable rellaf'as a yemedy for any such breach without Hiaving to post a bond.

17,11, Survival. Ternlnation of this Agreement or a Statement of Work shalt In no way relleve

efiher Paty of lis duties or obligations inowrred pursuant to this Agreement or Statement of

Work prlor to termination thereof. The provisions of Paragraphs 5, 6, 8, 9, £0, H1, 14.4, and

16 shall survive any termination of this Agreement or the Statement of Work,

17,12. Entive Agreement, This Agreement and the Statements of: Work constitute the entire

Agreement between Service Provides and SSBT; it shall not be amended, altered, or changed

except by a written agreement signed by tho Parties hereto,

IN WITNESS WHEREOF, the nndersigued, by their Authorized Representatives, have executed this

Agreement as of the day and year firs! set forth above, ,

METRICSTREAM, INC,

af

Schedule A

Statement of Work

STATEMENT OF WORK

Confidentiality — This document is being submitted by FUISSeRICe Provider Named to |

State Street Bank and Trust Company, with the explicit understanding that the contents would

not be divulged to any third party without prior written consent ftom State Street Bank and

Trust Company,

This Statement of Work (the "SOW”) dated as of KMonth=iXX, 20 defines a business transaction

between State Street Bank and Trust Company, on behalf of itself and its affillates and subsidiaries

(‘Client’), and <Full#SeiviceiProviderName> (‘Service Provider’) In which Service Provider will

provide - services ("Work"). It establishes the scope of the Work

to be performed, sets forlh the objectives to be achlaved, describés the start and delivery dates,

specific tasks, activities and deliverables, the criteria for successful completion of the Work and

Identifies the responsibillties of the parties,

This SOW is issued pursuant to the \_\_\_\_\_\_\_] Master Services Agreement

("Agreement") between Client and Service Provider dated SMorith> XX, 200X. This SOW Is subject to

the terms and conditions contalned In the Agreement, as may be amended from tlma to time, by and

between the partles and Is made a part thereof. Any term not otherwise defined herein, shall have the

meaning specified in the Agreement

PROJECT MANAGERS: For the purposes of this SOW, the following individuals are considered to be

the project managers:

State Street Project Manager: - Phone:,

Service Provider Project Manager: Phone:\_\_\_\_

OBJECTIVES AND SCOPE OF PROJECT:

Service Provider will perform the following scope of Work under this SOW:

The following services are out of scope under this SOW:

APPROACH AND METHODOLOGY:

Service Provider will adhere to the following approach arid methodelogy when performing the Work

defined In thts SOW:

32

PROJECT DELIVERABLES AND PROJECT PROGRESS:

The following Information identifies the dellverables and thelr corresponding progress percentage of

completion te the total engagement.

Deliverable(s) ery Date Progress Payment %

1.

2.

3.

4.

CLIENT RESPONSIBILITIES:

The following are responsibilities, deliverables, and other obligations of Client

SERVICE PROVIDER RESPONSIBILITIES:

The following are responsibiities, dellverables, and other obligations of Service Provider:

MUTUAL RESPONSIBILITIES:

The following are responsibilities, deliverable and other obligations of both Client and Service

Provider: (l.e. participate In meetings):

ASSUMPTIONS:

The following are assumptions made by both Client and Service Provider and: involved in the

performance of services under thls SOW:

LOCATION:

The services shall be performed .., (at State Street location or Service Provide location, combination

or remotely) ,

SCHEDULE AND TERM:

The parties: currently anticipate the Work will begin on RiMonth> “XX, 20\_\_ and will conclude on

SMionti>ikz, 20\_, Any changes to the scope and objectives of the Work that Impact the project

timing, profect cost, or the project deliverables, will be made solely by written agreement of the

patties, Service Provider will not exceed any estimate of time, fees or expenses set forth herein

without the prior written consent of Client. Client shall not be responsible for payment for any work

33

perfarmed or fees of expenses Incurred In excess of the estimates set forth herein unless agreed to in

writing In advance by Client. .

COMPENSATION / PAYMENT MILESTONES:

Service Provider represents that the total project fees for performance of all Work in accordance with

the terms hereof shall not exceed: §, :

Service Provider will involce Client according to the following payment schedule for Work performed

during this engagement:

ENGAGED CONSULTANTS AND RATES:

HOURLY ecu ane ESTIMATED

NENW HOURS pieteks)

Partner / Senior Principal $0.00 $0.00

Director $0.00 $0.00

Sr. Manager $0.00 $0.00

Sr. Consultant { Manager $0.00 $0,060

Consultant $0.00 $0.00

Jr, Consultant / Analyst $0.00 $0.00

Support $0.00 \_ $0.00

TOTALS: 0 $0.00

Blended Rate:

Total Experises Not To Exceed: §

Client will relmbursa Sérvice Provider for all actual, reasonable out of pocket expenses Incurred

{without markup) directly related to this Work up to a maximum of fifteen (15%) percent of the total

fees payable under this SOW. Service Provider will be responsible for promptly providing upon

Client's request copies of ail receipts In excess of seventy five ($75.00) dollars. :

BILLING AND PAYMENT:

Upon completion of each deliverable as outlined above, Service Provider shall submit such

deliverable for Client's testing and acceptance as provided In the Agreement. Upon notice by Client

to Service Provider that such deliverable has been successfully tested and accepted by Client,

Service Provider will submit an invoice for payment of the related progress payment based on the

percentage completion such deliverable represents to the total project fees payable which will be pald

In accordance with the terms of the Agreement. Each Invoice shail identify the completed and

accepted deliverable(s), the progress percentage being billed, and If applicable, the time spent on

each deliverable by Service Provider's.

MANAGEMENT PROCEDURES (if different from the terms of the Agreement):

Change Control Process -

34

01/18/2012 06:81 FAX : a, ~-\* fj0027008

Diapute Resolution Process ;

Status MeetingelReports. ,

COMPLETION OF ENGAGEMENT: ra

This SOW shall be deemed to be eovnpleted when all Work and deliverables have been

completed ahd delivered by ‘Service Provider arid have been tested and socepted by Client or:

sither party terminates a sow In aocordanea with the terms of the Agreement, ”

STATEMENT OF AGREEMENT:

IN WITNESS WHEREOF, Service. Provider and ‘Client have causad this sow to be signed. and

delivered by thelr daly authorized represontalive, all 88 of the date first hereln above written. “re

STATE STREET BANK AND serail Y METRCSTREAM, ING

35

Schedule B

Approved Subcontractors

36

Schedule C

Data Privacy

Any Service Provider that accesses, views, uses, copies, modifies, creates, stores, discloses,

transmits, or otherwise processes Non U.S, Personal Data, shall éxecute with SSBT the Data

Processing Agreement substantially in the form of Schedule C-1 attached to this Agreement (“Data-

Processing Agreement”), which agreement together with the texms of this Agreement shall govern the

processing of all SSBT Personal Data transferred to the Service Provider from the Economic

European Area or any other jurisdiction in connection under the Agreement.

Service ‘Provider shall comply with the terms and conditions of the Data Processing

Agreement in all material respects.

In the event of any conflict or inconsistency between this Agreement and the Data Processing

Agreement concerning the treatment or processing of Non U.S. Personal Data, the Data Processing

Agreement shall control. :

Upon the request of SSBT or one of its Related Companies, Service Provider shall:

(a) enter into additional Data Processing Agreements as SSBT may require, and

(b) use reasonable efforts to cooperate in connection with the preparation of the

additional Data Processing Agreements and any requited annexes to such additional Data

Processing Agteements, including providing any additional information requested by the

relevant data protection authorities within the period of time specified by such authorities, or,

ifno time period is specified by the applicable data protection authorities, within a reasonable

time.

37

Schedule C-1

!

For the purposes of Article 26(2) of Directive 95/46/RC for the transfer of personal data to processors

established in third countries which do not ensure an adequate level of data protection

Name of the data exporting

organization: ,

Address:

Tel: fax: e-mail:

Other information needed to identify the organization

(the data exporter)

And

Name of the data importing

organization: ,

Addiess;

Tel: fax: e-mail:

Other information needed to identify the organization

(the data importer)

each a ‘party’; together ‘the partles’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate

safeguards with respect to the protection of privacy and fundamental rights and freedoms of

individuals for the transfer by the data exporter to the data importer of the personal data specified in

Appendix 1. : ,

‘

Clause ]

\* Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categorles of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data

subject’ and ‘supervisory authority’ shall have the same meaning as in Direotive 95/46/RC of the

European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data ( ";

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal

data intended for processing on his behalf after the transfer in accordance with his instructions

38

(d)

(f)

and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate

protection within the meaning of Article 25(1) of Directive 95/46/EC;

‘the sub-processor’ means any processor engaged by the data importer or by any other sub-

processor of the data Importer who agrees to receive from the data importer or from any other

sub-processor of the data importer personal data exclusively intended for processing activities to

be cartled out on behalf of the data exporter after the transfer in accordance with his instructions,

the terms of the Clauses and the terms of the written subcontract; ,

‘the applicable data protection law’ means the legislation protecting the fundamental rights and

freedoms of individuals and, in particular, their right to privacy with respect to the processing of

personal data applicable to a data controller in the Member State in which the data exporter is

established;

‘technical and organizational security measures’ means those measures aimed. at protecting

personal data against accidental or unlawful destruction or accidental loss, alteration,

unauthorized disclosure or access, in patticular where the processing involves the transmission of

data over a network, and against all other unlawful forms of processing,

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where

applicable dre specified in Appendix 1 which forms an integral part of the Clauses,

Clause 3 ,

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause

5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-

parly beneficiary.

2, The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g),

Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has

factually disappeared or has ceased to exist in faw unless any successor entity has assumed the

entire legal. obligations of the data exporter by contract or by operation of law, as a result of which

it takes on the rights and obligations of the data exporter, In which case the data subject can

enforce them against suoh entity, .

3, The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g),

Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and

the data importer have factually disappeared or ceased to exist in law or have become insolvent,

unless any successor entity has assumed the entire legal obligations of the data exporter by

contract or by operation of law as a result of which It takes on the rights and obligations of the

data exporter, in which case the data subject can enforce them against such entity. Such third-

Party liability of the sub-processor shall be limited to its own ptocessing operations under the

Clauses, ,

4, The partles do not object to a data subject being represented by an association or other body if

the data subject 80 expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will

-continue to be carried out in accordance with the relevant provisions of the applicable data

protection law (and, where applicable, has been notified to the relevant authorities of the

39

Data Transfer Agreement, for the transfer of personal data to Data Processors in third

countries

( Standard contractual clauses ftom C(2010) 593 )

Member State whete the data exporter is established) and does not violate the relevant \*

provisions of that State;

(b) ‘that it has instructed and throughout the duration of the personal data-processing services will

instruct the data importer to process the personal data tratisferred only on the data ‘exporter’s

behalf‘and in accordance with the applicable data protection law and the Clauses:

(c) that the data Importer will provide sufficient guarantees in respect of the technical and

organizational security measures specified in Appendix 2 to this contract; ,

(d) that after assessment of the requirements of the’ applicable data protection law, the security

measuees ate appropriate to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorized disclosure or access, in particular where the

processing involves the transmission of data over a network, and against all other untawfut.

forms of processing, and that these measures ensure a level of seourity approptiate to the risks

presented by the processing and the nature of the data to be protected having regard to the

state of the art'and the cost of theif implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves spectal categories of data, the data subject has been informed or

will be infoemed befare, or as soon as possible after, the transfer that its data could be

transmitied to a third country not providing adequate protection within the meaning of

Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to

Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter

decides to continue the transfer of to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception

of Appendix 2, and a summary description of the security measures, as well as a copy of any

contract for sub-processing setvices which has to be made in accordance with the Clauses,

unless the Clauses or the contract contain commercial information, in. which case it may

remove such commercial information;

(i) that, In the event of sub-processing, the processing aotivity is carried out in accordance with

Clause 11 by a sub-processor providing at feast the same level of protection for the personal

data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligattons of the data importer (\*)

“The data importer agrees and watratts:

(a) to process the personal data only on behalf of the data exporter and in compliance with its

instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it

agrees to inform promptly the data exporter of Its inability to comply, In which case the data |

exporter Is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling

the instructions received from the data exporter and its obligations under the contract and that

40

C) Mandatory requitemonts of the nations legistaiion applicable Lo the data importer which do not go bayond what is necossary ina

democratle society on Ihe basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that Is, if they constitute a

necessary measure to safeguard nalonal security, defenco, public secutity, the prevention, investigation, detection and prosecution of

criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the

protection of the data snoject or the rights and frecdoms of others, aro not in contradiction with the standard contractual clauses. Some

exantples of'such mandatory requirements whieh do not go beyond what Js necessary dn a democmtic aoclety are, inter alfa,

Internationally recognised sanctions, tax-reporting requirements-or antl-money-laundering reporting requirements.

Data Transfer Agreement, for the transfer of personal data to Data Processors in third

countries —

( Standard contractual clauses from C(2010) 593 )

in the event of a change in this legislation which is likely to have a substantial adverse. effect. -

on the warranties and obligations provided by the Clauses, it will promptly notlfy the change

to the data exporter as soon as it is aware, In which case the data exporter is entitled to

suspend the transfer of data and/or terminate the contract;

(ec) that it has implemented the technical and organizational security measures specified in

Appendix 2 beforé processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement

authority unless otherwise prohibited, such as a prohibition under criminal law to

preserve the confidentiality of a law enforcement investigation;

(i) any accidental or unauthorized access; and

(iii)any request received ditectly from the data subjects without responding to that request,

untess it has been otherwise authorized to do so;

(8) to deal promptly and properly with all inquiries ftom the data exporter relating to its

processing of the personal data subject to the transfer and to abide by. the advice of the

supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the

processing activities covered by the Clauses which shall be carried out by’ the data exporter or

an inspection body composed of independent members and in possession of the required

professional qualifications bound by a duty of confidentiality, selected by the data exporter,

where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing

contract for sub-processing, unless the Clauses or contract contain commercial information, in

which case it may remove such commercial information, with the exception of Appendix 2

which shall be replaced by a summary description of the seotrity measurés in those cases

where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained

its priot written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with

Clause 11;

(1) to send promptly a copy of any sub-processor agreement it concludes undes the Clauses to the

data exporter,

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of

the obligations, referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to

receive compensation from the data exporter for the damage suffered.

2. Ifa data subject is not able to bring a claim for compensation in accordance with paragraph 1

against the data exporter, arising out of a breach by the data importer or his sub-processor of any

of their obligations referred to in Clause 3 of in Clause 11, because the data exporter has factually —

disappeared or ceased to exist in law or lias become insolvent, the data Importer agrees that the

data subject may Issue a claim against the data importer as if it were the data exporter, unless any

successor entity has assumed the entire legal obligations of the data exporter by contract of by

operation of law, in which case the data subject can enforce its rights against such entity.

41

Data Transfer Agreement, for the transfer of personal data to Data Processors in third

countries

( Standard contractual clauses from C(2010) 593 )

The data iraporter may not rely on a breach by a sub-processor of its oblizations in order to avoid

its own liabilities, \_

3. Ifa data subject is not able to bring a claim against the data exporter or the data importer

referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their

Obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data

importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-

processor agrees that the data subject may issue a claim agalnst the data sub-processor with regard

to its own processing operations under the Clauses as If it were the data exporter or the data

importer, unless any successor entity has assumed the entire legal obligations of the data exporter

or data importer by contract or by operation of law, in which case'the data subject can enforce its

\_ fights against such entity. The liability of the sub-processor shall be limited to its own processing

' Operations under the Clauses,

Clause 7

Mediation and jurisdiction

1, The data importer agrees that {f the data subject invokes against It third-party beneficiary

tights and/or claims compensation for damages under the Clauses, the data importer will accept -

the decision of the data sublect:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the

Supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established,

2. The parties agres that the choice made by the data subject will not prejudice its substantive or

procedural rights to seek remedies in accordance with other provisions of national or international

law,

Clause 8

Cooperation with supervisory authorities -

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it

80 requests-or if such deposit Is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data

importer, and of any sub-processor, which has the same scope and is subject. to the same ~

conditions ay would apply to an audit of thé data exporter under the applicable data protection

law.

3, The data importer shall promptly inform the data exporter about the existence of of lepletetion

applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or

any sub-processot, pursuant to paragraph 2, In such a case.the data exporter shall be entitled to

take the measures foreseen in Clause 3(b).

Clause 9

Governing law

The Clauses shali be governed by the law of the Member State in which the data exporter is

established, namely

anesderssveoee eoemnancat canes nee oe cananra ave fama pacanees 4 pvassdunrebevereres earmeacnarpens OPrereccacrDorarcognehbannnever?: As eh non0an dee, oer bunae ehgebqeersen

42

() This requirement may be satisfied by the sub-processor co-signing the contract entered Into between the date exporter and the data

Importer under this Derision. .

Data Transfer Agreement, for the transfer of personal data to Data Processors in third

countries

( Standard contractual clauses from C(2010)'593 )

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses, This does not preclude the parties from

adding clauses on business related issues where required as long as they do not contradict the

Clause, ,

, Clause 11

Sub-processing

1. The data importer shall not subcontract any of {ts processing operations performed on behalf

of the data exporter under the Clauses without the prior written consent of the data exporter,

Where the data Importer subcontracts its obligations under the Clauses, with the consent of the

data exporter, it shall do so only by way of a written agreement with the sub-processor which

imposes the same obligations on the sub-processor as are imposed on the data importer under the

Clauses ( 1 ). Where the sub-processor fails to fulfill its data protection obligations under such

written agreement the data importer shall remain fully liable to the data exporter for the

performance of the sub-processor’s obligations under such agreement,

2, ‘The prior written contract between the data importer and the sub-processor shall also provide

for a third-party beneficlary clase as laid down in Clause 3 for cases where the data subject is not

able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data

exporter or the data Importer because they have factually disappeared or have ceased to exist in

law or have become insolvent and no successor entity has assumed the entire legal obligations of

the data exporter or data importer by contract or by operation of law. Such third-party liabllity of

the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred

to in paragraph 1 shall be governed by the law of the Membor State in which the data. exporter is

established, namely ...oreorssoessssssvccseersonrspesesneses

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses

and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a

year. The list shall be available to the data exporter’s data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

\_1, The parties agree that on the termination of the provision of data-processing services, the data

importer and the sub-processor shall, at the choice of the data exporter, retumn all the personal data

transferred and the copies thereof to the data exporter or shall desttoy all the personal data and

certify to the data exporter that it has done so, uniess legislation imposed upon the data importer

prevents it from returning or destroying all or part of the personal data transferred, In that case,

the data importer warrants that it will guarantee the confidentiality of the personal data transferred

and will not actively process the personal data transferred anymore,

2. ‘The data importer and the sub-processor warrant that upon request of the data exporter and/or .:

of the supervisory authorlty, it will submit its data-processing facilities for an audlt of the

measures referred to in paragraph 1.

——\_—\_ 43

(") This cequiroment may be salisfled by the sub-processor co-signing [ho contract entered Into between the data oxporter and the data

importor under this Deolsian, .

\_On behalf of the data exporter:

Name (written out in

full:

Position:

Address: \

Other information necessary in

order for the contract to be

binding (if any):

Signature

oot

ef \

( ) (stamp of organization)

\

\*

Se nseent

On behalf of the data importer:

Name (written out in

full);

Position:

Address:

Other information necessary

in order for the contract to be

binding (if any):

Signature

a

( ) (stamp of organization) -

Sac

44

C) This requiromont may be satisfied by the sub-procossor co-signing the contract entered into botween the data exporter and the data importer

under this Decision,

Appendix I

to the Standard Contractual Clauses

This Appendix forms part of the Clanses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary

information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data tmporter

The data importer is (please specify briefly activities relevant to the transfer);

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Categories of data

The personal d data transferred concem the following categories of data (please specify):

Special categories of data Gf appropriate)

The personal data transferred concern the following special categories of data (please specify);

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

45

(') This requirement may be satisfied by the sub-processor co-siguing tle contract entered into between the data exporter and the data Importer

under this Decision.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data

importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other

party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge,

damages, expenses or loss it has incurred, ,

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and

- settlement of the claim (').

46

(') This raquiremént may be satisfied by the aub-processor co-signing the contract entered Into between tho date oxporter and tho data importer .

under this Decision.

Schedule C-2

SAFE HARBOR CERTIFICATION

1.1 Service Provider. hereby certifies (and continues to certify during the term of this Agreement)

that it adheres to the Safe Harbor Agreement between the U.S. Department of Commerce and the

Buropean Commission with respect to personally identifiable information that is transferred ftom the

European Economic Area to the United States (the “Safe Harbor”), and that, as a result, the Patties are not

required by law to execute the Data Processing Agreement set forth in Schedule C-1,

1.2 Service Provider represents, warrants and undertakes that during the term of this Agreement

and thereafter for so long as it retains any SSBT Personal Data:

(a)

(1) itis and will remain a certified participant in the Safe Harbor scheme overseen by the

US Department of Commetce and recognized by the European Commission as

providing adequate protection for personal data pursuant to its Decision of 26 July

2000 on the adequacy of the protection provided by the Safe Harbor Privacy

Principles and related Frequently Asked Questions issued by the US Department of

Commerce (2000/520/EC) (the “Safe Harbor Decision”) and that such certification is

and will continue to apply to all the categories or types of personally identifiable data

and/or sensitive personal information contained within the SSBT Personal Data that

is transferred from the European Economic Area to the United States under this

Agreement; or

(2) if Service Provider ceases to remain a certified participant in the Safe Harbor scheme

or its ‘certification ceases to apply to any of the categories or types of personally

identifiable information transferred from the European Economic Area made

available to if under this Agreement or the European Commission amends or revokes

the Safe Harbor Decision such that Service Provider’s compliance with the Safe

Harbor scheme would no longer be regarded as providing adequate protection for

personal data for the purposes of Article 26(1) of Directive 95/46/EC of the European

Parliament and of the Council of 24 Ootober 1995 on the protection of individuals

with regard to the processing of personal data and on the free movement of such data,

then, it will enter into a data processor agreement under the standard contractual

‘clausés for data processors established in third countries approved by the European

Commission in its Decision of 27 December 2001 on standard contractual clauses for

the transfer of personal data to processors established in third countries, under

Directive 95/46/EC (or such other standard contractual clauses as the Enropean

Commission may have formally approved since the date of this Agreement) (the

“Data Processing Agreement”);

(by it will comply with the Safe Harbor’s requirements and principles published by the U.S.

Department of Commerce, with respect to all SSBT Personal Data transferred to Service Provider

from the European Economic Area or any other jutisdiction and will publicly declare that it does

so, including by providing a timely anual reaffirmation to the Departnient of Commerce of its

self-certification of adherence to the Safe Harbor’s requitements; and

(c) if it intends to transfer or give access to any SSBT Personal Data to any-of its affiliates,

subsidiaries or subcontractors, it will ensure that these affiliates, subsidiaries or subcontractors

first enter into appropriate contractual arrangements with the Service Provider and/or SSBT

47

and/or one of its Related Companies on terms no less restrictive that the terms-herein and that

replicate the provisions of the Safe Harbor requirements or the terms of the European

Commission’s standard contractual clauses for the transfer of personal data referred to in Section

1.2 above, .

13 If Service Provider is in breach of Section 1.2 above at any titie during the term of this

Agreement or any subsequent period in which Service Provider retains any SSBT Personal Data then

Service Provider will, promptly on request by SSBT, destroy all SSBT Personal Data in its possession

and cease any further access to SSBT Personal Data (provided that Service Provider shall not destroy arty

original records of SSBT Personal Data without SSBT’s consent).

1.4 Upon the reasonable request of SSBT or one of its Related Companies, Service Provider shall! (i)

enter into good faith discussions regarding its entering into mutually agreeable additional data processing

agreements; (ii) use reasonable efforts to cooperate in connection with.the preparation of the additional

mutually agreeable data processing agreements and any required annexes to such agreements, including

providing any additional information required thereunder within the pertod of time specified therein, or, if

no tine period is specified therein, within a reasonable time; and (ili) upon SSBT’s direction, at all times

during the negotiations referenced herein not send, receive or hold any SSBT Personal Data. SSBT

Personal Data in the hands of the Service Provider at the time these negotiations are initiated shall be

removed or return as determined by SSBT in compliance with the terms of the Agreement,

48

Schedule D

Security Schedule

All capitalized terms not defined heréin shall have the meanings ascribed to them in the Master Services Agreement

executed by and between MetticStream, Inc, (“Service Provider”) and State Street Bank and Trust Company

(“SSBT”) as may be amended from time to time (the “Agresment”). As of the effective date of the Agreement or

such other data as the parties agree in writing, Service Provider shall have implemented, and shall thereafter

maintain cutrerit, a comprehensive security policy or policies (“Security Policy”) that satisfies the requirements set

forth below. Service Provider agrees that it shall not make any change(s) to its Security Policy that effectively

’ reduces or limits the rights or protections offered to SSBT under this Schedule or the Agreement generally.

Consistent with Section 5.3 ofthe Agreement, Service Provider shall secure and protect State Street Data, as defined

below, by using at least the same degree of care as the Service Provider uses to secure and protect its own

Confidential Information but-in no event any less than reasonable care; provided, however, that with respect to those

‘jurisdictions which do not recognize a reasonable standard of care Service Provider shall be obligated to use best

efforts,

Service Provider agrees to participate in State Street’s Vendor Management Program including completing SSBT’s

Vendor Risk Assessment Questionnaire(s) when requested by SSBT. Requests by SSBT will be no more frequent

than once in any twelve (12) month period for any Services described Ina Statement of Work. Service Provider also

agtees to make appropriate resources available for follow-up phone review(s) of the questionnaire or, if requestéd by

SSBT, for an onsite visit.

Service Provider shall not delegate any Services to be performed under this Agreement -or provide any access to

State Street Data or its network fo a subcontractor or other third party except to an Approved Subcontractor who’

compliss with the security measures at least as stringent as those described in this Schedule.

With respect to any Service Provider Personnel whio no longer requires, or is no longer authorized for whatever

reason to, access to State Street Data, where access is managed by SSBT, Service Provider shall so notify SSBT in

writing at least twenty-four (24) hours prior to the date on which such access is no longer required: unless such .

access is removed under exigent circumstances such that twenty-four (24) hours prior notice is not possible in which

case Service Provider shall notify SSBT immediately upon knowledge that such access shall be removed.

Qbiectives - Service Provider shall implement data security. measures that are consistent with banking industry best

practices and standards such that Service Provider: :

1, Protects the privacy, confidentiatity, integrity, and availability of all data, information, text, visual, audio ot

graphic representations and other materials in any medium or format, either electronic, or tangible which is

disclosed by or on behalf of SSBT and/or SSBT’s Related Companies to, or otherwise comes into the

possession of, the Service Provider, its Related Companies or Pexsonnel in connection with the Agreement,

(including but not limited to SSBT’s Confidential Information (collectively, “State Street Data”);

2, Protects against accidental, unauthorized, unauthenticated, or unlawful access, copying, use, processing,

disclosure, alteration, transfer, loss or destruction of the State Street Data including, but not. limited to,

identity thet: .

3. Complies with all applicable laws, rules, regulations, directives and decisions (each, to the extent having

the force of law) that are relevant to the handling, processing and use of State Street Data by SSBT or

Service Provider, on SSBT’s behalf, in accordance with this Agreement; and

4, Ensures security measures and procedures include (but shal] not be limited to) appropriate administative,

physical, technical, procedural and organizational safeguards:

1. Risk Assessments

A. Risk Assessment - Service. Provider shall perform regular, at least annually, robust, coinprehensive risk

assessments which identify the State Street Data or business assets (e.g., fiicilities, equipment, devices,

49

etc,), the threats against those asséts (both internal and external), the likelihood of those threats occurring

and the impact upon the organization to determine an appropriate level of Information Security safeguards.

Risk Mitigation ~ The Service Provider shall manage, control and remediate any threats identified in the

Risk Assessment that could result in unauthorized access, copying, use, processing, disclosure, alteration,

transfer, loss or destruction of any State Street Data, including without limitation, explicit protection

against identity theft, so as to achieve the Objectives stated above, commensurate with the sensitivity of the

State Street Data, as well as the complexity and scope of the activities of the Service Provider pursuant to

the Agreement:

Risk Assessment Suramary ~ Service Provider shall provide SSBT with the written (high level summary)

results of the Risk Assessment upon request, If SSBT believes vulnerabilities or threats identified in the

Risk Assessment have not been successfully remediated, Service Provider shall promptly employ a

mutually agreed, independent third party expert to perform a follow up assessment, Service Provider

agrees to remediate any risk findings other than those properly designated as medium or low risk (“High

Risk Findings") from the follow up assessment that could potentially affect SSBT at Service Provider

expense.

2, Security Policy

A.

Security Policy - Upon request by SSBT on an annual basis, the Service Provider shall provide SSBT’s ~

Chief Information Security Officer or his designee with a copy of its then current Security Policy and an

opportunity to discuss Service Provider's security measures with a qualified IT management member of

Service Provider. The Security Policy must reflegt security measures added as a result of risk assessment

findings.

Security Polley Review ~ Service Provider shall review its Security Policy regularly, and particularly

following any changes in applicable law, advances in technology or changes to the Service Provider's

information systems, in order to verify that the Security Policy and controls set out therein remain accurate,

comprehensive and up to date.

3. Organizational Security

A.

B.

Responsibility - Service Provider shall assign responsibility for information security management to

"appropriate skilled and senior Personnel only.

‘Need to Know’ Access - Service Provider shall restrict access to information systems used in connection

with this Agreement and/or to State Street Data to only those Personnel who are reliable, have sufficient

technical expertise for the role assigned and know his or her obligations and the. consequences of any

security breach.

Confldentiallty - Service Provider Personne! who have accessed or otherwise been made known of State

Street Data, shall maintain the cdnfidentiality of such information for the duration of such individuals

employment with Service Provider and for a perlod of three (3) years thereafter. No less frequently than

annually, all Setvice Provider Personnel that may have access to State Street Data will be required to

certify that such individual has read‘and complied with the confidentiality and non-dfsolosure duties in this

schedule. SSBT reserves the right to inspect this certification.

4, Asset Management

A.

B.

Data Sensitivity - Service Provider acknowledges that it understands the sensitivity of the State Street

Data. ‘

Data Control - Unless otherwise agreed to in writing by SSBT, Service Provider and its Personnel shall

not copy, download, transmit (to or from), or store State Street Data on any desktop, laptop, server, portable

or other device at any location, unless directly related to the delivery of service pursuant in the Agreement,

No Public Cloud Computing - Service Provider represents and warrants that it does not and shall not rely

upon public cloud computing to perform the Services, including without limitation, the processing or

storage of State Strest Data, unless SSBT has specifically approved such use in writing. For purposes of

50

this Schedule, public cloud computing refers to a model for enabling convenient, on-demand network

access to a shared pool of configurable computing resources (e.g,, networks, servers, storage, applications

and servers) via the Internet that can be rapidly provisioned and released with minimal management effort

or service provider interaotion.

5. Security Training

6.

7

A.

c,

General - Service Provider, prior to making any State Street Data available shall institute an appropriate

training and education program to ensure that its Personnel are appropriately trained regarding their

" responsibilities under the Seourity Policy and with respect to the confidentiality and non-distlosure duties

including, without limitation, any special requirements relating to State Street Data.

Privileged Aceass Users - In addition to its training obligations in‘the Agreement generally, Service

Provider shall make available specific security training to all Personnel granted privileged access (e.g,

root, dba, network admin, superuser level access, support, etc.) to systems which handle or hold State Street

Data and/or are used to provide Services.

Developer - Service Provider also shall make available to development teams associated with development

efforts impacting SSBT, specific training focused on well defined, seoure coding standards,

Physical Security

A.

Securlng Physical Faellities . Service Provider shall maintain all systems hosting State Street Data and/or

providing Services on behalf of SSBT in a physically secure environment that restricts access to only

authorized individuals, and detects any unauthorized access or access attempts. A secure environment

includes 24 x 7 security Personnel or equivalent means of monitoring at all relevant locations (including,

without limitation, buildings, computer facilities, and-records storage facilities).

. Physical Security of Media - Service Provider shat] prevent the unauthorized viewing, copying, alteration

or removal of any media containing State Street Data, wherever located. Removable media on which State

Street Data is stored (including thumb drives, CDs, and DVDs, but excluding laptops, and PDAS by

Service Provider must be encrypted using at least 256 bit AES (or equivalent) and may not be used or re-

used by Service Provider to store data of any other customer or to deliver data to any third party unless

prior to such use or re-use the State Strect Data is securely erased,

Media Destruction - Service Provider shall destroy removable media and any mobile device (such as

discs, USB drives, DVDs, back-up tapes, printers, laptops and PDAs) containing State Street Data or render

State Street Data on such physical media unintelligible and not capable of reconstruction by any technical

means prior to any reuse of the media, ifrequested by SSBT or if such media or mobile device is no longer

intended to be used.

. Paper Destruction - Service Provider shall cross shred all paper waste and dispose in a sécure ‘and

confidential manner so as to render all paper waste unteadable.

Secure Physical Processing Locations ~ Service Provider shal) keep an upto-ate record of the location of

each data center used in connection with the provisions of Services and the owner of such data center and

shall provide such record to SSBT upon request. Further Service Provider shall promptly notify SSBT of

any transfer or relocation of material portions of State Street Data.

Communications and Operations Management

Ae

Network Penetration Testing - Service Provider shall, on at least an annual basis, contract with an

independent third. party to conduct a network penetration test on information systems and network having

access to ot holding or containing State Street Data, Service Provider witl provide SSBT with a high level

summary of the test results including the scope and methodology of the test and confirmation that High

Risk Findings have been remediated or a plan (including time frame) is in place to remediate.

. Data Encryption ~ Service Provider shall encrypt or protect by other technical means State Street Data in

Service Provider's possession or centro] so that it cannot be read, copied, changed or deleted by

unauthorized persons while in storage, including when saved on removable media,

51

Data Protection During Transmission or Transit - Service Provider shall encrypt and protect State Street

Data in Service Provider’s possession or control so that it cannot be read, copied, changed or deleted by

unauthorized persons during transmission or transit inside or outside of Service Provider's internal

network.

. Data Loss Preverition - Service Provider shall implement a comprehensive data leakage solution that

identifies, detects, monitors, documents and either alerts or prevents said State Street Data from leaving the,

Service Provider control without authorization in place.

Data Destruction ~ Service Provider shall agree at the request of SSBT to (i) promptly return to SSBT, in

the format and on the media reasonably requested by SSBT, all or any part of State Street Datn; (il) erase or

destroy all or any part of State Street Data in Service Provider’s possession, in each case to the extent so

requested by SSBT; and (iii) provide letter of attestation that data has been successfully erased or

’ destroyed.

Network Ports - Service Provider shall restrict unauthorized network traffic affecting State Street Data,

Malicious Code - Service Provider shall detect the introduction or intrusion of malicious code on

information systems handling or holding State Street Data.and al no additional charge to SSBT prevent the

unauthorized access, disclosure or loss of Integrity of any State Street Data and remove and eliminate any

effects,

8, Access Controls

A.

Authorized Access - Service Provider shall maintain the logical separation such that access to all systems

hosting State Street Data and/or being used to provide services to SSBT will uniquely identify each -

individual requiring access, grant access only to authorized individuals based on the pringiple of least.

privileges, and prevent unauthorized access to State Street Data,

User Access Inventory - Service Provider shall maintain an accurate and up to date list of ail Personnel

who have access to the State Street Data and will have # process to promptly disable within twenty-four

(24) hours of trarisfer or termination access by any individual Personnel,

Password Management - Service Provider shall communicate new passwords to users in a secure mamner,

with an appropriate proof of identity check of the intended users, Passwords shall not be stored or

transmitted in readable form,

Logging & Monitoring - Service Provider shall log and monitor all access to the information systems

containing State Street Data for additions, alterations, deletions, and copying of State Street Data, The

Service Provider agrees to malniain full records or system or applicable access attempts, both successful

and failed and ypon roquest will make available to SSBT, all logs andrecords, Security administration logs

‘will be retained for a- minimum of sixty (60) days and financlal transactions logs will be retained for a

minimum of six (6) months.

Multl-Factor Authentication for Remote Access ~ Service Provider shal] use multi factor authentication

and a secure tunnel when accessing systems containing SSBT data remotely,

Wireless » Service Provider shall ensure use of WIFI (aka 802,11) network traffic is encrypted using

WPA2 with the ABS encryption algorithm option provides for non-broadcast SSID and mutual

authentication between the server and the end devices when accessing systems containing State Street Data.

9, Use of Laptop and Mobile Devices in connection with the Agreement

A.

B.

Eneryption Requirements - Service Provider shall encrypt the State Street Data on any laptops or mobile

devices (¢.g,, Blackberries, PDAs) used by Service Provider's Personnel using at least 256° bit encryption

AES (or equivalent).

Secure ‘Storage - Service Provider shall require that all laptops and mobile devices be seomly stored

whenever out of the Personnel’s immediate possession and, in the event of a Jost or stolen laptop or other

52

mobile device containing State Street Data, Service Provider shall immediately notify SSBT‘s Chief

Information Security. Officer or his designee.

C. Network/ Systems Password Storage - Service Provider shall prohibit use of laptops or other mobile

devices (e.g,, Blackberries, PDAs) to store network or system passwords that enable access to SSBT

systems or other systems that handle or hold State Street Data, unless such passwords are encrypted. -

D, Remote Wipe/Inactivity Timeout - Service Provider shall employ access and password controls as well as

inactivity timeouts of no longer than thirty (30) minutes on all laptops, desktops and mobile devices used

by Service Provider’s Personnel and maintain the ability to immediately upon knowledge remotely remove

data from any deyice lost, stolen or in possession of a terminated employee.

BE. Laptops/Mobile Devices - Service Provider shall prohibit access to State Street Data on laptops or mobile

devices where above requirements cannot be met.

10. Information Systems Acquisition Development and Maintenance

A. Application Penetration Testing - Service Provider shall, on at least an annual basis, contract with an

Independent third patty to condyct an application penetration test application used in association with this

agreement. Service Provider will provide SSBT with a high level summary of the test results Including the

scope and methodology of the test and confirmation that High Risk Findings haye been réemediated or a

plan (inclnding time frame) is in place to remediate.

B. State Street Data - Must be used by the Service Provider solely for the purposes specified in this

Agreement, Additionally:

J. No production data shall be used for any other purpose (¢.¢., QA testing, development testing, User

Acceptance Test areas (UAT), training, demonstration, etc.).

II, In instances where production data is copied to other environments as authorized by SSBT in

writing, data must be copied in a secured mamer and meet the controls specified within this

document. State Street Data must be protected to the same level as is applied to the production data

or as otherwise authorized by SSBT (e.g. masked or obfuscated data).

IIL Production environment must be a separate environment ftom any other non-production

environment (development, UAT, etc.).

C, Software Patching - Service Provider shall regularly update and patch ofall computer software on systems

fiat handle or hold State Street Data, with patching for vulnerabilities rated ‘critical’ or ‘high’ applied

within thirty (30) days of patch availability, unless othe controls have been applied that mitigate the

vulnerability.

D. Virus Management - Service Provider shall provide antivirus and spyware software protection to Service

Provider's systems that handle or hold State Strect Data (includes laptops and mobile devices), using the

most recently distributed version of software including virus signatures Updated at least every tventy-four

(24) hours. .

11, Incident Event aud Communications Management

A. Incident Managemenit/Notification of Breach - Service Provider shall develop and implement an

approved incident response plan that specifies actions to be taken when the Service Provider, one of its

subcontractors or SSBT suspects or detects that a party has gained unauthorized access to State Street Data

or systems or applications containing any State Street Data (the “Response Plan”). Such Response Plan

shall, include;

I. Escalation Procedures - An escalation procedure to senior managers and appropriate reporting to

regulatory and law enforcement agencies. The Service Provider shall immediately report to SSBT’s

Chief Information Security Officer or his designee via telephone or email (and provide a

confirmatory notice in writing as soon as practicable but in any event within qventy-four (24) hours)

all incidents that may in any way affect-the operation of SSBT or the confidentiality, availability or

integrity of State Street Data (lacluding backed up data), including but not limited to, any successful

or. attempted unauthorized access to systems or networks which contafn or provide access to the

53

State Street Data; provided that the foregoing notice obligation Is excused for such perlod of time as

Service Provider is prohibited by law enforcement agencies to notify SSBT.

Wf, Incident Reporting - Service Provider will promptly furnish to the SSBT full details that the

Service Provider has or may obtain regarding the general circumstances and extent of stich

unauthorized access, including without limitation, the categories of personal data and the number

and/or identities of the data subjects affected, as well as any steps taken to secure the State Street

Data and preserve information for any necessary investigation.

IIL Investigation & Prevention - Service Provider shall use reasonable efforts to assist SSBT in

investigating or preventing the reoccurrence of any such access and shall: (i) cooperate with the

SSBT in its efforts to comply with statutory notice or other legal obligations applicable to SSBT or

its clients arising out of unauthorized access or use and to seek injunctive or other equitable relief;

(ii) cooperate with the SSBT In any litigation and investigation against third parties deemed

reasonably necessary by SSBT to protect its proprietary rlghts; and (iil) promptly take all reasonable

actions necessary to prevent a reoccurrence of and mitigate against loss from any such authorized

access,

IV, Personnel Training & Confidentiality - Service Provider shall ensure that all Personnel fully

\_ understand the process and conditions ynder which they are required to invoke the appropriaté

incident response. Service Provider shall maintain absolute confidentiality regarting actual or

suspected authorized possession, use or knowledge of State Street's Data or any other failure of

Service Provider’s security measures or non-compliance with its security policies or procedures.

Service Provider agrees (0 itomediately discontinue use of and access to State Street’s Data, if

requested, for any security reasons cited by SSBT.

11. “Special” Personal Data Processing - Service Provider shall provide enhanced controls for “special”

categories of Personal Data when requested by SSBT, including but not Hmited to encryption at rest and during

. transinission.

12, Limited Access - From time to time, SSBT grants Service Provider Personne] access to SSBT facilities subject .

to, the terms of the Agreement, iri order to perform the Services, With respect to those engageinents where Service

Provider and its Personnel do not require and shall not access State Street Data to fulfill its Service obligations to

SSBT except while on SSBT fucilities, the terms and conditions of this Schedule apply except that the following

provisions shall replace Sections 1 througli 11 above:

A. Service Provider shall provide SSBT with information regarding such security measures designed to protect

the privacy of State Street Data upon the reasonable request of SSBT; promptly provide SSBT with

information regarding any failure of such security measures or any security breach related to State Street

Data; and maintain absolute confidentiality regarding any such failure of such security measures or any

security,

B. Notwithstanding anything to the contrary contain in this Schedule or the Agreement generally, if at any

\_ time Service Provider is required to copy (in print, electronic or other form), transport, transmit, transfer or

otherwise move any State Street Data to catry out its obligations under this Agreement, it shall only do so if

such printed or moved State Street Data remains on SSBT’s premises, and within SSBT’s network, as

‘applicable, at all tines, In no event shall any State Street Data be removed from SSBT’s premises or its

network. For purposes of this Agreement, any and all Informetion residing with the SSBT network or

accessed while on SSBT premises shall be considered to be State Street Data,

C. Service Provider, prior to making any State Street Data available shall institute an appropriate training and

education program to ensure that its Personnel are appropriately trained regarding thelr responsibilitles

under the Secutity Policy and with respect to the confidentiality and non-disclosure duties including,

without limitation, any special requirements relating to State Street Data.

54