

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONTRACT

35630

THIS CONTRACT is made and entered, in duplicate, as of November 12, 2019 for reference purposes only, pursuant to Resolution No. RES-19-0168, adopted by the City Council of the City of Long Beach at its meeting on November 5, 2019, by and between TELESOFT, LLC DBA MDSL, a Delaware limited liability company ("Contractor"), with a place of business at 5343 N. 16th Street, Suite 300, Phoenix, Arizona 85016, and the CITY OF LONG BEACH ("City"), a municipal corporation.

WHEREAS, the City requires subscription, maintenance and support, as well as a one-time upgrade, of the City's desk phone and mobile device inventory and billing management system; and

WHEREAS, City did by Resolution No. RES-19-0168 determine that the City's need for subscription, maintenance and support, as well as a one-time upgrade, of the City's desk phone and mobile device inventory and billing management system could only be met by Contractor and, by reason of the foregoing, no useful purpose would be served by advertising for bids, and to do so would constitute an idle and useless act and an unnecessary expenditure of public funds;

NOW, THEREFORE, in consideration of the mutual terms and conditions contained herein, the parties agree as follows:

1. Contractor shall sell, furnish and deliver to City maintenance, upgrade and support of the City's desk phone and mobile device inventory and billing management system, as well as a one-time upgrade to the current software version, attached hereto as Exhibit "A" and incorporated herein by reference, as authorized by Resolution No. RES-19-0168.

2. City shall pay Contractor in due course of payments, following receipt of an invoice from Contractor and upon acceptance from City, the prices shown in Exhibit "B", in an annual amount of Fifty-Six Thousand Two Hundred Thirty-One Dollars (\$56,231) with an annual contingency of Three Thousand Dollars (\$3,000) for additional services, for

1 a total annual amount not to exceed Fifty-Nine Thousand Two Hundred Thirty-One Dollars
2 (\$59,231) for a period of two (2) years, with the option to renew for three (3) additional one-
3 year periods, with an annual increase of up to five percent (5%), at the discretion of the
4 City Manager; and, a one-time upgrade to the current version in the amount of Fifteen
5 Thousand Dollars (\$15,000).

6 3. The term of this Contract in relation to maintenance shall commence
7 on May 18, 2019, and shall terminate at midnight on May 17, 2021 unless sooner terminate
8 as provided herein. The term of this Contract in relation to licensing shall commence on
9 November 15, 2019, and shall terminate at midnight on November 14, 2021 unless sooner
10 terminated as provided herein. City shall have the option to extend the term of this
11 Agreement for three (3) additional one-year periods, at the discretion of the City Manager.
12 The City may terminate this Contract by giving thirty (30) days prior notice of termination
13 to Contractor.

14 4. Neither this Contract nor any of the moneys that may become due to
15 Contractor hereunder may be assigned without the prior written consent of City.

16 5. Any notices required hereunder or desired to be given by either party
17 shall be in writing and personally delivered or deposited in the U.S. Postal Service, first
18 class postage prepaid, addressed to Contractor at the address stated herein, and to City
19 at 411 West Ocean Boulevard, Long Beach, California 90802 Attn: City Manager. Notice
20 shall be deemed given on the date personal delivery is made or on the date of deposit in
21 the mail, whichever first occurs.

22 6. City shall have the benefit of any warranty from the contractor on the
23 hardware and related accessories, and Contractor warrants that the hardware and related
24 accessories are in good working order and free from defect at the time of delivery.

25 7. The parties agree to abide by the Master Services Agreement, as
26 specified in Exhibit "C", attached hereto and incorporated herein by this reference.

27 ///

28 ///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IN WITNESS WHEREOF, the parties have signed this document with all the formalities required by law as of the date first stated above.

TELESOFT, LLC DBA MDSL, a Delaware limited liability company

Sept 14, 2020, 2019

By [Signature]
Name BRIAN BRADY
Title CEO

9/14/2020, 2019

By [Signature]
Name Charles Luque
Title CEO

"Contractor"

CITY OF LONG BEACH, a municipal corporation

September 24, 2019

By [Signature]
City Manager

EXECUTED PURSUANT TO SECTION 301 OF THE CITY CHARTER.

"City"

This Contract is approved as to form on September 23, 2020, 2019.

CHARLES PARKIN, City Attorney

By [Signature]
Deputy

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
411 West Ocean Boulevard, 9th Floor
Long Beach, CA 90802

EXHIBIT "A"

Attachment A

The logo for mdsl, featuring three vertical dots to the left of the lowercase letters 'mdsl'.

City of Long Beach

Change Order Request

Change Order Objectives: Server Migration

Services to be Provided

Subject to the terms and conditions of the original Agreement, any subsequent Amendments, and this Change Order, MDSL will make/facilitate the following change(s)

Activity Details:

Customer is moving the application and modules to a new server environment. MDSL's Support Analyst will need to migrate the applications' new environment. All vendor feeds and costing conversions will be included in this move. The upgrade entails:

1. An assessment of the current environment, processes and tools used for the MDSL application.
2. Development review of the current processes or tools that may need to be converted due to a server platform change. (Additional fees may be incurred based on development level of effort to convert the process or tool).
3. MDSL validates the new server meets the minimum environmental requirements.
4. MDSL validates a copy of the TelMaster folder is created on the new server.
5. MDSL validates the new server has connectivity to the database, polling units, PBX's and other data sources.
6. MDSL installs the application and makes necessary configuration changes due to platform change.
7. On go live day, MDSL will configure all data inputs and out puts to use the new server configuration.
8. MDSL validates the environment with the customer. (e.g., costing, vendor feeds, HR updates, FTP processes and/or any additional MDSL processes).
9. Four hours of remote training are included

Cost:

One time fee \$15,000

Monthly fee \$2,000 (36 months)

Server Migration Upgrade Checklist

Task	Owner
Project Kickoff	Customer/MDSL
Establish UAT Date	Customer/MDSL
Establish Pre-UAT Remote Training Date	Customer/MDSL
Provide Hardware/Software Requirements to Customer	MDSL
Audit Current MDSL Application Environment at Customer (Ticket Created)	MDSL
Convert Shell Scripts (if required)	MDSL
Convert Costing (if required)	MDSL
Feeds	MDSL
Costing	MDSL
Changes	MDSL

Custom Work	MDSL
Application Changes	MDSL
Provide destination to receive data	Customer/MDSL
Provide FTP connectivity for various data sources, including CDR or others.	MDSL
Validate new server meets minimum environmental requirements	MDSL
Install all binary required to run the MDSL application	MDSL
Provide copy of the entire Telmast directory from current Production server.	Customer
Provide a copy of the Production database (primary db and reporting db)	Customer
Install Application	MDSL
Revise DB schema to match application version	MDSL
Install Reporting	MDSL
Costing/Collection Process Modifications in Production (when applicable).	Customer/MDSL
Make necessary configuration changes (to reintegrate the product and database) to Test and Production Environments due to Platform Changes	MDSL
Testing/QA/UAT - MDSL will respond to any tickets created as a result of Customer UAT Testing	Customer
Pre-UAT Remote Training	Customer/MDSL
UAT	Customer/MDSL
To validate the upgrade/migration, Customer should test their daily, weekly and monthly processes to avoid possible issues when running the first time after upgrade/migration	Customer
Verify billing process and support	Customer
Upgrade thoroughly tested in Test/Dev Environment	Customer
Test UAT Accepted	Customer
Establish Production Upgrade Date	Customer/MDSL
Create Customer and MDSL Production Run Book	Customer/MDSL

Customer Responsibilities
Customer acknowledges and agrees to these responsibilities:

Customer agrees that any changes to the Scope of Work after Acceptance of the original business requirements and signed Change Order Request will constitute additional "out of scope" work. Services other than those expressly identified herein require a new Change Order Request.

Customer agrees that any changes or modifications to the scope or tasks associated with this project will require joint Customer/MDSL approval in writing. Changes may extend the duration of the engagement and/or require additional resources, resulting in additional cost to Customer.

Customer agrees that MDSL will not be responsible for missed deadlines due to items not in the control of MDSL that delay the project. This includes, but is not

limited to, availability of Customer resources, equipment and infrastructure provider services.

Payment Terms

Customer will be invoiced one hundred percent (100%) of the one-time fee upon SOW execution, the monthly fee to be billed once the environment is running.

Please indicate whether the existing P.O. will be modified to reflect this Change Order Request or if a new P.O. will be issued, by providing the P.O. number.

Use Existing P.O. # _____

Use a New P.O. # _____

The Customer agrees to pay invoice(s) within thirty (30) days from invoice date. This payment shall be subject to the payment terms set forth in this Change Order Request including, where applicable, late payment and additional expense charges.

Invoicing Procedures

Unless otherwise instructed by Customer in writing, MDSL shall send all invoices to:

TS-AcctsPay@longbeach.gov

Change Order Expiration

Customer agrees to utilize the Services within one (1) year of the executed Change Order Request or issuance of a Purchase Order, unless other arrangements are made by signed amendment to this Change Order Request; Otherwise, the Change Order Request will automatically expire, allowing MDSL to recognize the Services as complete. Fees paid by Customer for Services Customer failed to utilize will be non-refundable.

IN WITNESS WHEREOF, the Customer and MDSL have reviewed and agree to all of the terms and conditions of this Work Order. By signing the Work Order or issuing a Purchase Order against this Work Order, Customer expressly agrees to and consents to be bound by all assumptions as true in all material respects and the terms and conditions contained herein.

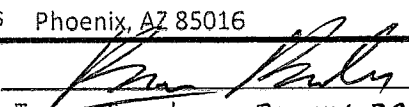
Customer Name:	
City of Long Beach	Telesoft LLC dba MDSL
Office Address for contact and notice purposes	Office Address 5343 North 16 th Street Suite 300 Phoenix, AZ 85016
Signature: _____	Signature: 
Name: _____	Name: Tamara Saunders BRIAN BRADY
Title: _____	Title: CFO
Effective Date: _____	Effective Date: _____

EXHIBIT “B”

Attachment B

Licenses:

Monthly licensing first 10,000 extensions) hosted \$2,000.

\$24,000/annual

Annual Software Maintenance (5-18-2019 to 5-17-2020):

SCHEDULE A – ITEMIZED LIST OF ITEMS COVERED UNDER MAINTENANCE

FOR

CITY OF LONG BEACH

ITEM #	DESCRIPTION	QTY	MAINT.
CITY OF LONG BEACH C873			
	TTS Call Accounting - First 10,000		
TTS 101	Extensions	1	\$ 9,859
TTS 103	TTS Tele Cop (Toll Fraud) - 1st PBX/Switch	1	\$ 1,078
TTS 103A	TTS Tele Cop (Toll Fraud) - per PBX/Switch	7	\$ 852
TTS 114	TTS Vendor Feed Format Conversion 1-5	4	\$ 9,004
TTS 124	General Ledger Journal File	1	\$ 1,849
TTS 124H	HR Journal File	1	\$ 1,849
SB 411 B	Micro Poll Polling Device w/Modem	8	\$ 4,560
	SUBTOTAL		\$ 29,051
ASTS 100A	CCMI RATE TABLE SUBSCRIPTION	2	\$ 3,180
	TOTAL ANNUAL SOFTWARE MAINTENANCE		\$ 32,231

EXHIBIT “C”

Master Services Agreement

SaaS

THIS MASTER SERVICES AGREEMENT (“MSA”) is made on 8/21/ 2020 (the “Effective Date”) by and between Telesoft, LLC (DBA MDSL), a Delaware limited liability company, with a principal place of business at 5343 N. 16th Street, Suite 300, Phoenix, AZ 85016 (together with any of its Affiliates providing services under this Agreement, the “Supplier”) and the City of Long Beach (“Customer”). Each of Customer and Supplier may individually be referred to as a “Party” and collectively as the “Parties.”

WHEREAS:

- A. Supplier develops, owns and distributes certain software products, applications, platforms and related services that, among other things, facilitate invoicing, auditing, processing and usage management for telecommunication, technology, and financial data services with Customer’s vendors, and
- B. Customer desires to license such software products, applications, platforms and related services from Supplier in accordance with the terms and conditions of this Agreement.

IT IS HEREBY AGREED:

In consideration of the payment of the Fees by the Customer to the Supplier, the Supplier will (i) grant access to the Customer to use the Software, and (ii) provide the Services to the Customer subject to the following terms and conditions:

1. DEFINITIONS

For the purposes of this MSA the following words shall have the following meanings respectively:

- 1.1 **Affiliates:** any entity controlled by, or controlling, or in common control with any party hereto, as the case may be. An entity shall be deemed to control another entity if the former entity possesses, directly or indirectly, the power to direct, or cause the direction of, the management and policies of the other entity whether through ownership of voting securities or partnership interests, representation on its board of directors or similar governing body, by contract or otherwise;
- 1.2 **Agreement:** means this MSA, the SOW and any amendments, schedules, annexes, exhibits or similar documents referenced by and incorporated into to this Agreement as agreed between the Parties in writing from time to time;
- 1.3 **Applicable Laws:** means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction applicable to the obligations of the Parties under this Agreement;
- 1.4 **Audit and Inventory Services:** certain professional consulting services that may be provided to Customer as detailed in the SOW;
- 1.5 **Client Device:** a personal computer, smart phone, tablet or other workstation or terminal device at the Customer’s site or used by Customer capable of connection to and operation of the Software situated at the Supplier’s ASP Facility;
- 1.6 **Client Device Software:** the client systems software such as, but not limited to, thin client applications (e.g. RDP client, Citrix ICA client), operating system, systems library, browser or browser component, network operating system and data communication software, which is specified by the Supplier as being required, and which is normally resident in the Client Device;
- 1.7 **Confidential Information:** data or information in any form disclosed by one Party to the other Party by any means, if and for so long as the data and information are protectable as trade secrets

by the disclosing party or are otherwise subject to legal rights that give the disclosing party, independent of agreement, a right to control use and/or disclosure of the data and information. As a non-exhaustive list of examples, Proprietary Information includes information regarding a Party's financial condition and financial projections, business and marketing plans, product plans, product and device prototypes, the results of product testing, research data, market intelligence, technical designs and specifications, secret methods, manufacturing processes, source code of proprietary software, the content of unpublished patent applications, customer lists, vendor lists, internal cost data, the terms of Agreements with employees and third parties, and information tending to embarrass the disclosing party or tending to tarnish its reputation or brand;

- 1.8 **Data:** means the data held in the Licensed Database and may include any data relating to the Customer operations, facilities, customers, clients and programs in whatever form that information may exist and whether entered into, stored in, generated by processed through or accessible as a result of the Services and Use of the Software;
- 1.9 **Database Server:** a server or servers on which the Licensed Database portion of the Software is located and accessed by Customer's users;
- 1.10 **Data Protection Laws:** means the European General Data Protection Regulation (GDPR) (Regulation (EU) 2016/6790, Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827), Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) and similar laws, rules and regulations relating to and governing the processing, collection, use and disclosure of personal data;
- 1.11 **Documentation:** any printed or online material relating to the Software including, but not limited to, user manuals, maintenance manuals, specifications, instructions, charts, diagrams and the like, which have been issued by the Supplier to the Customer during the Term of this Agreement;
- 1.12 **Fees:** the moneys payable by the Customer to the Supplier in exchange for access to the Software and/or the provision of the Services hereunder and as more fully described in the SOW;
- 1.13 **First Access Date:** the date of first access to the Software by the Customer as defined in Section 4 of this Agreement;
- 1.14 **Force Majeure Affected Party:** any Party to this Agreement who may be prevented from fully performing its obligations under this Agreement by the occurrence of a Force Majeure Event;
- 1.15 **Force Majeure Event:** the occurrence of any event or circumstance, beyond the control of the Force Majeure Affected Party, that could not be overcome using all commercially reasonable efforts and which makes it impossible for the Force Majeure Affected Party to fully perform its obligations under this Agreement, including (without limitation) any act of God or a public enemy, any terrorist, cyber or military attack, fire, flood, earthquake, storm or other like natural disaster, disruption or outage of communications, power or other utility, civil unrest, unavailability of supplies (provided no substitute supplies can reasonably be obtained), or any other cause similar to any of the foregoing;
- 1.16 **Host Software:** the systems software such as, but not limited to, operating system, database management system, systems library, network operating system and data communication software, which is specified by the Supplier as being required, and which is normally resident in the Supplier's ASP Facility and through which the Software must function;
- 1.17 **Implementation Services:** services associated with uploading and configuring client supplied data into the Software, including but not limited to project management, discovery, planning, data gathering, data cleansing, upload of data either electronic or paper, testing and documentation of the Software and training in the operational use of the Software as detailed in the SOW;
- 1.18 **Intellectual Property Rights** means any of the following: a) patents, trademarks, rights in designs, get-up, trade, business or domain names, copyrights including rights in computer

software and databases (including database rights) and topography rights (in each case whether registered or not and, where these rights can be registered, any applications to register or rights to apply for registration of any of them); and b) rights in inventions, know-how, trade secrets and other confidential information; and c) any other intellectual property rights which may exist at any time in any part of the world, including the rights to copy, publicly perform, publicly display, distribute, adapt, translate, modify and create derivative works of copyrighted subject matter.

- 1.19 **Managed Services** means additional services provided by the Supplier to the Customer as detailed in the SOW;
- 1.20 **Remote Desktop Access Method:** access to the Software utilizing either (i) thin-client remote desktop client software such as Microsoft Remote Desktop or Citrix Receiver, or (ii) a browser-based remote desktop library such as Guacamole, to connect to a remote desktop session server within Supplier's ASP Facility;
- 1.21 **Services:** the Implementation Services, Managed Services and/or Audit and Inventory Services to be performed by the Supplier in accordance with the terms and conditions of this Agreement as defined by the SOW;
- 1.22 **Service Level Objectives:** means, individually and collectively, the service level objectives that Supplier provides (including the terms and conditions that outline Supplier's responsibilities thereof) in connection with delivery and maintenance of the Software and Services by Supplier to Customer as expressly set forth in any SOW;
- 1.23 **Statement of Work or SOW:** means the document duly executed by the Parties, referencing and subject to the terms of this Agreement, specifying the Software, Services, Fees, Service Level Objectives and related terms and conditions;
- 1.24 **Software:** the computer program product or products specified in the SOW (Software Modules) which shall comprise the Supplier's own Software together with (if appropriate) software licensed from other sources to the Supplier including all updates, upgrades, additions, enhancements and improvements from time to time, in machine-readable or printed form and subject to Supplier's Software Release Policy set forth in Annex C attached hereto;
- 1.25 **Supplier's ASP Facility:** the computer system or network of computer systems, including Host Software in the form and configured as described in Annex A (Security Standards) to be accessed by the Customer to operate the application and database portions of the Software;
- 1.26 **Term:** the period of time during which the Supplier grants the License and/or provides the Services to the Customer, as more particularly defined in Section 12 or described in an SOW;
- 1.27 **Third Party Software:** means those computer programs supplied by the Supplier for Use by the Customer in accordance with the License rights in Clause 2;
- 1.28 **Use:** the copying of all or any portion of the Software from storage units or media into the Supplier's ASP Facility for processing and operation, the use of the Software in the course of operation including the use of the Software in printed form and/or the use of Documentation in support of the operation of the Software, provided always that any such use is always limited to the purposes for which the Software is designed as specified in the Documentation;
- 1.29 **Web Portal Access:** means access to the Software via the internet using an agreed standard web browser.

2. SOFTWARE LICENSE, USE, AND OWNERSHIP

- 2.1 During the Term, and subject to Customer's compliance with the terms and conditions of this Agreement, Supplier hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable license to access, use, and interact with (collectively, "Use") the Software for Customer's and Customer's Affiliates' internal business purposes (the "License"). The scope of

the License is defined by the terms and conditions of this Agreement, and the License is granted subject to those terms and conditions.

- 2.2 During the Term and subject to Customer's compliance with the terms and conditions of this Agreement, Supplier hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable license to copy and distribute the Documentation solely for internal use and to the extent necessary for Customer to incorporate portions of such Documentation into Customer's own documentation. Customer acknowledges that the Documentation is Supplier's Confidential Information, and Customer agrees to ensure that all proprietary notices placed on the original copies by Supplier, such as copyright notices, trademark notices, and confidentiality notices, are also included in the same manner on all copies. Customer may not modify or make derivative works of the Documentation.
- 2.3 Customer shall be the exclusive owner of all right, title and interest in and to the Customer Data. Notwithstanding the foregoing, Customer grants to Supplier and its licensors a worldwide, perpetual, royalty-free, fully-paid up, non-exclusive license and right to use, store, analyze and aggregate the Customer Data for the sole purpose of Supplier performing the Services for Customer hereunder. Subject to the limited license granted herein, Supplier acquires no right, title or interest from Customer or its licensors under this Agreement or in or to Customer Data.
- 2.4 Customer acknowledges that there are no additional licenses granted by implication under this Agreement. Supplier reserves all rights that are not expressly granted. Customer acknowledges that, as between the parties, Supplier owns all Intellectual Property Rights and any other proprietary interests that are embodied in, or practiced by, the Supplier Software and/or the Documentation.
- 2.5 Except as expressly permitted in this Agreement, Customer shall not: (i) use the Software in any manner that is inconsistent with the Documentation; (ii) sell, lease, assign, pledge, license, sublicense, rent, loan, resell or otherwise transfer, with or without consideration, the Software or Documentation; (iii) use the Software to operate the business of a third party, or to process data or content provided by a third party for the operation of a third party's business, or otherwise use the software on a third party's behalf, or act as a service bureau or provider of application services to any third party; (iv) reverse engineer, decrypt, decompile or disassemble the Software, or recreate any of the source code of the Software; (v) modify the Software, nor create derivative works based upon the Software, in whole or in part; (vi) copy or distribute the Software without Supplier's prior written authorization; (vii) attempt to gain unauthorized access to the Software or any related systems or networks; (viii) remove any proprietary notices or labels on the Software or Documentation; or (ix) use the Software to store or transmit Malicious Code.
- 2.6 Customer agrees to allow Supplier to monitor Customer's use of the Software for purposes of confirming that Customer remains in compliance with the Agreement. Supplier will treat non-public information obtained through any such review and examination as Customer's Proprietary Information.
- 2.7 Customer acknowledges and agrees that this Agreement grants no title or right of ownership in or to Supplier's Software, Documentation, products, software code, programs and tools, training or professional services materials, know how, techniques, technologies, methods and concepts, or any component thereof (collectively, the "Supplier Technology"), and that Supplier and its licensors retain all right, title and interest in and to such Supplier Technology, including, but not limited to: (i) patent, copyright, trade secret and similar Intellectual Property Rights in the underlying technology; (ii) all copies and derivative works thereof (by whomever produced) and (iii) the Documentation. Customer shall not, at any time, take or cause any action, which would be inconsistent with or tend to impair the rights of Supplier or its licensors in the Supplier Technology.
- 2.8 Customer hereby grants to Supplier a worldwide, perpetual, irrevocable, royalty-free, fully paid-up license and right to use, copy, display, modify, publish or create derivate works from any Customer feedback relating to the Software, Documentation and Services, including but not limited to, any information provided by Customer related to Customer's experience with the Software, Documentation and Services.

3. FEES AND PAYMENT

- 3.1 Customer shall pay the Fees to Supplier in the amounts and on the terms and conditions set forth in this Agreement and the SOW commencing upon the First Access Date or as otherwise agreed in the applicable SOW. Any Fees prepaid in advanced are non-refundable and will not be subject to terms and conditions relating to early termination fees or charges.
- 3.2 All Fees and other charges arising under this Agreement are exclusive of value added tax or other local taxes and such tax will (i) be added to the Fees in accordance with prevailing legislation at the time of invoice and (ii) itemized on the invoice in accordance with any relevant regulations.
- 3.3 Payment shall be due 30 days from receipt by the Customer of a valid written invoice. The Supplier reserves the right to charge interest on all undisputed invoices (except for that portion and only that portion which is the subject of a good faith dispute as notified by Customer) not settled in accordance with Clause 3.3 at a rate of 1.5% per month calculated daily and compounded monthly or, if lower, the highest rate permitted under Applicable Laws.
- 3.4 On each anniversary of the Effective Date after the Initial SOW Term of any applicable SOW, the Supplier reserves the right to increase the Fees by a percentage equivalent to the prevailing rate of the applicable retail price indexing published from time to time by the relevant authority in the jurisdiction in which the Customer is located (e.g., Consumer Price Index (United States) or The Office for National Statistics (United Kingdom) plus two percent (2%).

4. PROVISION OF ACCESS

- 4.1 Upon the Effective Date and in accordance with any applicable provisions of the SOW, the Supplier will commence installation and commissioning of the necessary Software in preparation for use by the Customer. The Supplier will also assist the Customer in testing of the connection to the Supplier's ASP Facility. The installation and commissioning of the Software does not include Implementation Services or Consulting Services.
- 4.2 Once the Software and Host Software has been commissioned and a connection from a Client Workstation has been tested to the satisfaction of Customer (acting reasonably), the Supplier will serve notice to the Customer by email that use of the Software may commence. The day this notice is served will be deemed to be the First Access Date.
- 4.3 In the case where a related proof of concept, product trial or similar pilot exercise ("POC") has been conducted in advance of or in connection with this Agreement, the execution of this Agreement will serve as acknowledgement of the successful completion of the POC and the date of this Agreement shall be the First Access Date.

5. SUPPLIER WARRANTIES AND OBLIGATIONS

- 5.1 The Supplier warrants that the Software will substantially conform to the functions specified in the Documentation.
- 5.2 The Supplier further warrants that it has a right to grant the Customer and its Affiliates a license to use the Software, Supplier's ASP Facility, Host Software, Database Server and Documentation without knowingly infringing or violating any third-party rights.
- 5.3 The Supplier further warrants that the Services shall be performed in compliance with all Applicable Laws and Supplier will use all commercially reasonable efforts to achieve any applicable Service Level Objectives.
- 5.4 The Supplier shall use all commercially reasonable efforts to ensure that no virus is introduced or transmitted by it to the Customer's computer system during the term of this Agreement.
- 5.5 The Software and Services are not fault-tolerant and are not guaranteed to be error free or to operate uninterrupted. Customer must not use the Software in any application or situation where the Software's failure could lead to personal injury property or environmental damage.

EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE SOFTWARE, SERVICES, DOCUMENTATION AND DATA OR DELIVERABLES PROVIDED BY SUPPLIER ARE PROVIDED "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS," AND SUPPLIER EXPRESSLY DISCLAIMS ALL OTHER REPRESENTATIONS AND WARRANTIES OF ANY KIND OR NATURE, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF OPERABILITY, CONDITION, TITLE, NON-INFRINGEMENT, NON-INTERFERENCE, QUIET ENJOYMENT, VALUE, ACCURACY OF DATA, OR QUALITY, AS WELL AS ANY WARRANTIES OF MERCHANTABILITY, SYSTEM INTEGRATION, SUITABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE ABSENCE OF ANY DEFECTS THEREIN, WHETHER LATENT OR PATENT.

6. CUSTOMER REPRESENTATIONS AND OBLIGATIONS

- 6.1 Customer represents that (i) it has full power to enter and perform this Agreement under applicable law and under its relevant governance documents; (ii) it has obtained any consent it requires from its management, its board of directors and any third parties to the extent consent is necessary to authorize it to enter and perform this Agreement; and (iii) it has had adequate opportunity to review and negotiate the terms of this Agreement and to seek the advice of counsel about its rights and duties under this Agreement.
- 6.2 The Customer shall make all commercially reasonable efforts to ensure that no virus or malware is introduced or transmitted by it to the Supplier's computer system during the term of this Agreement.
- 6.3 Customer shall make available to the Supplier any project management and technical personnel necessary to assist with configuration or services or troubleshooting operational issues where such configuration or troubleshooting requires knowledge of, or administrative access to, the Customer's network or operations, and ensure that such personnel are appropriately qualified and trained. The Customer acknowledges that failure to make available such resources within a reasonable timeframe will negatively affect issue resolution times, and therefore release the Supplier from any associated Service Level Objectives.
- 6.4 The Customer shall ensure that it can provide to its users the appropriate technical environment from which to access the Software, including Client Devices and Client Device Software, as specified in Annex B – Technical Prerequisites. These requirements shall be updated from time to time by Supplier in line with industry trends and new product releases. Supplier and Customer shall work together in good faith to ensure the technical measures are understood and can be properly implemented by Customer. Customer acknowledges that failure to provide a suitable technical environment may lead to degraded performance or availability of the Software, for which Supplier cannot be held liable.
- 6.5 Customer shall timely provide any and all consents, approvals, third-party information and documentation (including letters of authorization) required in order for Supplier to implement and deliver the Services or otherwise reasonably requested by Supplier (including any project implementation documentation with agreed deadlines or milestones).
- 6.6 Customer may not contact Supplier's subcontractors directly without express prior written permission from Supplier.

7. BACK-UPS

- 7.1 The Supplier will make regular back-ups, emergency and archival copies of the Licensed Database in machine-readable form, in accordance with the Security Standards and Supplier's Business Continuity Plan. The Supplier shall not distribute or otherwise relinquish possession of such back-up copies apart from providing copies of the Licensed Database to the Customer when formally requested in writing to do so by the Customer.
- 7.2 The Customer agrees neither to copy or print, nor to permit any person to copy or print, in whole or in part any of the Documentation without the Supplier's prior written consent, such consent not to be unreasonably withheld.

8. SOFTWARE PROTECTION

- 8.1 The Customer shall not provide or otherwise make available any part of the Software of the Supplier including but not limited to, flow charts, logic diagram and source codes, in any form to any person (other than such of the Customer's employees, Affiliates, or consultants who have a need to know the same) without the prior written consent of the Supplier and the Customer shall take appropriate action by instruction, agreement or otherwise to satisfy the Customer's obligations under this Agreement with respect to use, copying, modification, protection and security of the Software.
- 8.2 The Customer shall ensure that its employees and other persons permitted access to the Software or the confidential information of the Supplier are first made aware that such information is confidential and that they owe a duty of confidence to the Supplier and in the case of independent consultants who may from time to time render Services to the Customer in respect of the Software the Customer shall be liable for any such independent consultant breaching the above-mentioned duty of confidence.
- 8.3 The Customer is not permitted to allow access to the Supplier ASP Facility without the consent of the Supplier.
- 8.4 The Customer further agrees to the terms in Annex D - Use of Third-Party Software.

9. CONFIDENTIALITY

- 9.1 Each Party as "Recipient" may be given access to information (in hardcopy, electronic or other form) that is identified by the other as "Discloser" as Confidential Information. Confidential Information of Supplier shall include the Supplier Technology (defined below); and Confidential Information of Customer shall include the Customer Content. Recipient agrees not to disclose or permit access to the Discloser's Confidential Information, except to the Recipient's employees and agents who are informed of the confidential nature of the Confidential Information and who have agreed in writing or who are otherwise legally bound to treat the Discloser's Confidential Information in a manner consistent with Recipient's duties under this Agreement. Recipient will not use the Discloser's Confidential Information except (i) as necessary to perform Recipient's duties under this Agreement; and (ii) in any other manner that this Agreement expressly authorizes. Recipient shall use the same care to protect such Confidential Information as it uses to protect its own information of like kind, but in no event less than reasonable care, and will restrict access to such Confidential Information to those of its personnel engaged in a use permitted hereby. Notwithstanding the foregoing, either party may also disclose Confidential Information in confidence to its attorneys, accountants, professional advisors, and bankers in the ordinary course of business, as well as to current and potential investors in connection with a proposed financing transaction, and to other third parties in connection with a proposed transaction for the sale or acquisition of that party's business or assets. Confidential Information, including copies thereof, shall be returned or destroyed by Recipient upon the first to occur of (a) completion of the Services, (b) termination of this Agreement or (c) written request by the Discloser.
- 9.2 Nothing in this Agreement shall prohibit or limit Recipient's use of information (i) previously known to it without obligation of confidence, (ii) independently developed by it without use of or reference to Discloser's Confidential Information, (iii) acquired by it from a third party not under an obligation of confidence with respect to such information, or (iv) that is or becomes publicly available through no breach of this Agreement. Further, each party may disclose Confidential Information to the extent required by a court of competent jurisdiction, law enforcement officials or other governmental authority or otherwise as required by law. Unless prevented by law, the Recipient agrees to notify the Discloser as far in advance as reasonably possible before the Recipient delivers the Discloser's Confidential Information to any of those third parties. If requested by the Discloser, and if permitted by law, the Recipient will cooperate with the Discloser, at the Discloser's expense, in seeking to limit or eliminate legal requirements that compel disclosure, or in seeking confidential treatment by the applicable court, law enforcement officials and/or governmental agencies.
- 9.3 Recipient acknowledges that a breach of this section could cause Discloser irreparable harm and significant injury, which may be difficult to ascertain. Recipient agrees that Discloser will have the right to pursue any and all rights and remedies available at law and equity for such a breach.

10. INDEMNIFICATION

- 10.1 The Supplier will defend any action brought against the Customer or its Affiliates (each an "Indemnified Party") and will fully indemnify an Indemnified Party against any claim, action, demand, cost or expense (including for the avoidance of doubt, any professional or legal fees and disbursements) incurred by that Indemnified Party which is based on a claim that the Software, Documentation or Services used or performed within the scope of the License granted hereunder and otherwise in compliance with the terms and conditions of this Agreement infringes, whether actual or alleged, the proprietary rights (which term shall include, but not be limited to any patent, copyright, trade-mark, service-mark, design right, database rights, know-how etc.) of any third party, provided that:
- 10.1.1. the Indemnified Party notifies the Supplier promptly in writing of any action of which it is aware (provided however that Supplier's liability under this paragraph 10 shall only be reduced if, and in proportion to the extent that, any delay in notification on the part of the Indemnified Party materially prejudices Supplier's ability to defend any such action);
 - 10.1.2. the Supplier has sole control of the defense and all negotiations for the settlement or compromise of any action; and
 - 10.1.3. the alleged infringement arises by virtue of the Use of the Software alone in a manner authorized under this Agreement and not in combination with other software or equipment that has not been approved for such use by the Supplier.
- 10.2 If the Software, Documentation or Services become, or in the Supplier's opinion is likely to become, the subject of a claim for infringement of any person's proprietary right the Supplier may, at its option, secure the Customer's rights to continue using the Software, Documentation or Services, or replace or modify the Software, Documentation or Services to make them non-infringing (provided that such replacement or modification provides substantially the same level of service and functionality to Customer).
- 10.3 The foregoing states the entire liability of the Supplier with respect to infringement of any other person's proprietary rights by the Software, Documentation or Services.

11. LIMITS OF LIABILITY

- 11.1 Neither Party shall be entitled or seek to rely on any representation (other than fraudulent misrepresentation), statement or warranty concerning the Services, nor shall either Party be liable to the other Party for any loss or damage incurred or suffered by such reliance unless such representation, statement or warranty is specifically made in this Agreement or authorized in writing as a special term of this Agreement by a director of the Supplier and an authorized representative of the Customer.
- 11.2 EXCLUDING CONFIDENTIALITY AND INDEMNITY OBLIGATIONS HEREUNDER, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE PERFORMANCE OF THEIR RESPONSIBILITIES UNDER THIS AGREEMENT, EVEN IF THE PARTY CAUSING SUCH DAMAGES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, SUPPLIER'S MAXIMUM AGGREGATE LIABILITY (WHETHER IN CONTRACT OR IN TORT OR UNDER ANY OTHER FORM OF LIABILITY) FOR DAMAGES OR LOSS, HOWSOEVER ARISING OR CAUSED, SHALL IN NO EVENT EXCEED THE FEES PAID BY CUSTOMER TO SUPPLIER UNDER THE RELEVANT SOW. THE ALLOCATIONS OF LIABILITY IN THIS SECTION REPRESENT THE AGREED AND BARGAINED-FOR UNDERSTANDING OF THE PARTIES AND THE COMPENSATION FOR THE SERVICES REFLECTS SUCH ALLOCATIONS. THE LIMITED REMEDIES SET FORTH IN THIS AGREEMENT SHALL APPLY NOTWITHSTANDING THE FAILURE OF THEIR ESSENTIAL PURPOSE.

12. TERM AND TERMINATION

- 12.1 The term of this MSA shall commence on the Effective Date and, unless previously terminated as provided below, will remain in effect for so long as any Software or Services are being delivered by Supplier to Customer pursuant to any SOW. The term of any SOW shall be as specifically set forth in such SOW (the "SOW Term"). Termination of this MSA shall terminate any and all SOW's then in effect at the time of such termination.
- 12.2 Either Party may immediately terminate this MSA or any SOW by giving written notice of termination to the other party if:
- 12.2.1. That other Party shall breach or fail to perform any obligation under this Agreement and, if such breach or failure is capable of remedy, remedial action shall not have commenced, in the case of Customer's obligation to pay any Fees before the expiry of period of five (5) days after written notice thereof, and in all other cases before the expiry of period of thirty (30) days after written notice thereof; or
- 12.2.2. that other Party becomes insolvent or unable to pay its debts or has an administrative or other receiver appointed or passes a resolution for its winding-up or liquidation or has a court order made for winding up or declaration of insolvency or becomes subject to an administration order or enters into a voluntary arrangement with its creditors or ceases or threatens to cease to carry on business or takes or suffers any similar action in consequence of debt.
- 12.3 Within thirty (30) days after termination of this MSA:
- 12.3.1. the Customer shall either return the Documentation and all copies in the Customer's possession to the Supplier or (at the Supplier's option) take all reasonable steps to destroy the Documentation and all copies and furnish the Supplier proof of such steps at the request of Supplier; and
- 12.3.2. in accordance with Clause 9.6 above, the Supplier shall either deliver up the Data to Customer in a form which is accessible by Customer or destroy the Data (including all copies and backups thereof) at Customer's discretion.
- 12.4 Customer may terminate any SOW for convenience on no less than ninety (90) days prior written notice; however, in such case, or in case of Supplier's termination of any SOW or this MSA (resulting in the termination of any SOW) based on Customer's uncured material breach (including breach of any payment obligations), Customer shall pay Supplier an early termination charge equal to the sum of: (i) 100% of any unpaid, undisputed Fees accruing prior to the date of termination; (ii) 100% of any unpaid, undisputed Fees for months 1-15 of the SOW Term; and (iii) 50% of any unpaid, undisputed Fees for months 16 through the end of the SOW Term. For clarity, this Section 12.4 shall not apply to non-refundable prepaid Fees.

13. GENERAL

- 13.1 **Entire Agreement; Amendment.** This Agreement constitutes the entire agreement between the Parties and there are no understandings or agreements which are not fully expressed herein. No change, modification or amendment to this Agreement or any SOW shall be valid unless made in writing and signed by authorized representatives of both Parties. Either Party may request, in writing, changes to the Software, Services or Scope only in accordance with Supplier's change control procedure defined in Annex E attached hereto. Notwithstanding the foregoing, the Parties agree and acknowledge that Supplier may periodically update the Annexes by written notice to Customer to ensure the responsible, fair and reasonable use of the Services and Software (including updates to address Software updates, upgrades, additions, enhancements, and improvements from time to time), and to ensure compliance with Applicable Laws.
- 13.2 **Notices.** Any notice required or permitted by this Agreement shall be given to the recipient in writing by mail, hand delivery or telecopy to the address set forth in the signature page below, or to such other address as the recipient may designate by written notice. Further, Supplier may send operational notices related to the Services provided hereunder by electronic mail to Customer at the electronic mail address provided to Supplier. Any such notice shall be deemed to be received on the date delivered, telecopied or e-mailed, or five days after being mailed by registered or certified mail, return receipt requested, postage prepaid.

- 13.3 **Severability.** If any provision of this Agreement is declared or found to be illegal, unenforceable or void, then both parties shall be relieved of all obligations arising under such provision, but if such provision does not relate to the payments to be made to the Supplier by the Customer and if the remainder of this Agreement shall not be affected by such declaration or finding, then each provision not so affected shall continue to be valid and enforceable.
- 13.4 **Waiver.** No provision of right under this Agreement shall be deemed waived unless the waiver is in writing and signed by the waiving party. The failure of either Party to enforce compliance with a provision of this Agreement shall not be construed as a general waiver of such provision or any other provision.
- 13.5 **Signature Authority.** Each of the Supplier and the Customer represents and warrants to the other that: a) it has full power and authority to execute, deliver and comply with this Agreement; b) the execution, delivery and performance of this Agreement by it have been duly authorized by it; and c) this Agreement evidences a valid and binding obligation of it enforceable in accordance with its terms.
- 13.6 **Assignment.** Subject to the provision of this clause, this Agreement shall be binding on the Parties, their successors and assigns. Neither Party shall assign this Agreement or any of its rights hereunder, nor delegate any of its obligations hereunder, without the other Party's prior written consent, except that such consent shall not be required in the case of an assignment of this Agreement (but not of any individual rights or obligations hereunder) to: (i) a purchaser of or successor to substantially all of a Party's business (unless, in the case of Customer, such purchaser or successor is a software, data processing or computer services vendor that is a competitor of Supplier, its parent company or any of its subsidiaries or affiliates); or (ii) an Affiliate (provided, in the case of Customer, that the scope of each license granted under this Agreement does not change). Any assignment in breach of this Section shall be void.
- 13.7 **Headings.** The headings in this Agreement are for reference only and shall not affect the construction of this Agreement.
- 13.8 **Data Protection.** The Supplier agrees that it shall store or process Customer Data in accordance with all Applicable Laws, including without limitation the data protection principles as set out in any applicable Data Protection Laws.
- 13.9 **Publicity.** Supplier shall have the right to publicly announce or use Customer's name or logo for Supplier's promotion, publicity, marketing or advertising purposes.
- 13.10 **Agency.** Except as expressly permitted by this Agreement, neither Party shall in any circumstances hold itself out as being: (a) the servant or agent of the other Party; or (b) authorized to enter into any contract on behalf of the other Party or in any way to bind the other Party to the performance, variation, release or discharge of any obligations.
- 13.11 **Third Party Rights.** A person who is not a party to the Agreement shall not enforce any of its provisions as a third-party beneficiary, including under the Contracts (Rights of Third Parties) Act 1999.
- 13.12 **Force Majeure.** Upon the occurrence of a Force Majeure Event:
- 13.12.1 either Party shall notify the other Party in writing of the commencement of the Force Majeure Event. Where the notification is from the Force Majeure Affected Party, to the extent available to such Party, it should also provide details of the Force Majeure Event and a non-binding estimate of the extent and the expected duration of its inability to perform its obligations due to the Force Majeure Event; and
- 13.12.2 the obligations of both Parties under this Agreement will be suspended for the duration of the Force Majeure Event and neither Party shall be liable for, or be considered to be in breach of this Agreement due to, any failure to perform such obligations.
- 13.12.3 Whilst such Force Majeure Event is continuing, the Force Majeure Affected Party shall use all reasonable efforts to overcome the Force Majeure Event. Upon the Force Majeure Event being overcome or it ceasing to exist, both parties will, as soon as is reasonably practicable thereafter, resume full performance of their obligations under this Agreement (including, for the avoidance of doubt, any suspended obligations). Where a Force Majeure Event continues for a

period of fourteen (14) Business Days, either Party may, by written notice to the other Party, terminate this Agreement with immediate effect.

13.13 **Law and Jurisdiction.** This Agreement will be interpreted and construed in accordance with the laws of the State of California excluding that body of law applicable to choice of law. The Parties consent to exclusive jurisdiction in the state or federal courts located in California, and such venue shall not be challenged by the non-filing Party as improper or inappropriate due to, among other things, inconvenience under the doctrine of forum non-conveniens or other similar doctrines. Each Party also agrees not to bring any action or proceeding arising out of or relating to this Agreement in any other court.

SIGNATURES ON FOLLOWING PAGE

IN WITNESS WHEREOF the parties hereto have caused this Agreement to be signed and delivered by their duly authorized officers.

City of Long Beach

Telesoft, LLC dba MDSL

Address for contact and notice purposes:

Address for contact and notice purposes:

5343 N. 16th Street
Suite 300
Phoenix, AZ 85016
ATTN: Chief Financial Officer

Signature: *LINDA F. TATUM*
Name: *Linda F. Tatum*
Title: *ASST CITY MANAGER*
Date: *9/25/2020*

Signature: *Brian Brady*
Name: *BRIAN BRADY*
Title: *CFO*
Date: *8/21/20*

EXECUTED PURSUANT
TO SECTION 301 OF
THE CITY CHARTER.

APPROVED AS TO FORM

September 23, 2020
CHARLES PARKIN, City Attorney

By *[Signature]*
**ERIN WEESNER-MCKINLEY
DEPUTY CITY ATTORNEY**

Index of Annexes

Annex A: Security Standards (Connect)

Annex B: Technical Prerequisites (Connect)

Annex C: Software Release Policy

Annex D: Use of Third-Party Software

Annex E: Change Control Procedure

Annex A – Security Standards (Connect)

1. Overview

- 1.1 This Schedule defines the hosting & security standards implemented by MDSL as an Application Service Provider (ASP) and Software as a Service (SaaS) provider.
- 1.2 MDSL's security arrangements are constantly monitored and regularly audited and tested, thus the precise configuration is frequently updated to ensure that the system and services follow industry best practices.

2. Service Overview

- 2.1 MDSL provides enterprise technology expense management “Software as a Service” from its cloud hosting facilities, delivered via the public internet.
- 2.2 MDSL owns and operates a robust network of infrastructure servers co-located at multiple, diverse, enterprise-grade datacenter facilities (the “MDSL Cloud”).
- 2.3 The MDSL Cloud is physically and logically separated from the MDSL corporate network, ensuring customer data is kept secure in well-defined and controlled locations.
- 2.4 Beyond the environmental facilities (space, power, cooling) and public internet connectivity provided by our data center partners, MDSL is responsible for the selection, provisioning and maintenance of the software involved in delivering MDSL services.
- 2.5 Technical administration of the infrastructure services, logical access controls including user accounts, and operational monitoring is the responsibility of the MDSL ASP administration teams listed in Section 5 – Human Security. No third party has administrative access to any MDSL hosting system.
- 2.6 For a limited number of infrastructure services (such as public DNS and CDN), MDSL also makes use of “Public Cloud” services from recognized and certified providers including Oracle Cloud, Amazon Web Services and Microsoft Azure. Public Cloud services are used to provide global resilience and content acceleration.

3. Information Management System

- 3.1 MDSL maintains an Information Security Management System certified across the business to ISO/IEC 27001:2013 under Certificate No. IS 562188, awarded by BSI.
- 3.2 BSI and NDB audits the ISMS policies, processes and controls at least annually in compliance with the requirements of the standard. These audits cover processes for company-wide Security Incident Management, Business Continuity and Disaster Recovery, Change Management and Continuity Service Improvement.
- 3.3 MDSL employs a dedicated Information Security & Risk Manager, reporting to the Board of Directors, to oversee the global operation of Information Security, Risk Management and Business Continuity planning.
- 3.4 Independent auditors are engaged as needed to provide both internal and external audit functions to support and verify the ISMS.
- 3.5 MDSL publishes an Information Security Policy setting out our obligations to protect the Confidentiality, Integrity and Availability of business information. The Policy is approved by senior management and reviewed annually.
- 3.6 All MDSL staff receive induction awareness training on Information Security, Risk Management and Business Continuity shortly after beginning employment, with annual refresher courses, and must sign a ‘Computer Use Agreement’ which formalizes their responsibilities in regard to security and risk.
- 3.7 A global risk assessment framework has been established, approved by management and communicated to the appropriate stakeholders.

4. Physical & Environmental Controls

4.1 Corporate Offices

- 4.1.1. All MDSL offices adhere to the documented access control policies, including use of automated access control systems (key cards & fobs), and visitor sign-in where available. Access logs are maintained.

- 4.1.2. Primary MDSL office buildings are located in purpose-built office facilities with secure perimeters, and appropriate fire and theft protection systems, kept under maintenance contracts and tested annually.
- 4.1.3. MDSL corporate data rooms and communications cabinets are secured with additional access controls (key fob entry, locked racks etc.) and appropriately signed.
- 4.1.4. "Clean desk" and "clear screen" policies are in operation
- 4.1.5. MDSL policy is that customer data should not be stored for extended periods within corporate office facilities. Any customer data received at MDSL corporate offices should be securely uploaded directly to the SaaS hosting facilities for continued processing, and removed from local sites as soon as practicable.

4.2 SaaS Hosting facilities

- 4.2.1. The "MDSL Cloud" is provisioned from multiple enterprise-grade co-location hosting datacenters.
- 4.2.2. Colocation datacenter providers are assessed by MDSL's internal security officer for compliance against the information security standards of ISO 27001. Information security remains a key factor in partner selection and is reviewed as part of a standing agenda item at service reviews with data center partners.
- 4.2.3. Colocation datacenter providers provide the following minimum Physical Access Controls:
 - Strong physical perimeter walls, fences and doors
 - 24/7/365 Security monitoring including guards & CCTV
 - Unified, monitoring security-breach alarm systems
 - Visual verification of all persons entering the data floor.
 - Mandatory advanced visitor registration – access list of authorized engineers controlled by MDSL Infosec team.
 - Proximity card-reader access controls
 - Secure, managed delivery and loading areas
 - Dedicated, locked server racks
- 4.2.4. Colocation datacenter providers each provide the following minimum Environmental Controls:
 - Resilient Power & Cooling
 - Fully redundant and resilient power supplies, at a minimum of N+1
 - Maximum diversity and separation of UPS system and power distribution through dedicated A&B supplies
 - Back-up diesel generation at N+1 to support site load in the event of a failure of grid-power
 - Redundant HVAC units to guarantee temperature & humidity with at least N+1 resilience
 - Fire detection & suppression
 - Very Early Smoke Detection Apparatus (VESDA)
 - Two-stage detection systems (includes underfloor and ceiling void spaces) – smoke & heat
 - Advanced water mist or Firetrace fire suppression systems
- 4.2.5. Escorted site inspection visits of hosting datacenters are possible by pre-arrangement with the MDSL ASP Administration Team
- 4.3 MDSL maintains a central asset register and inventory for all corporate and hosting hardware, with associated asset tags.

5. Human Security

- 5.1 All MDSL staff are background-checked prior to employment (via 3rd party service) and trained to ensure compliance with the applicable security policies as part of ISO27001 policies.
- 5.2 All staff sign employment contracts and the Computer Use Agreement, ensuring they recognize their responsibilities with regard to non-disclosure, confidentiality, acceptable use and conduct, and the disciplinary process for non-compliance with these policies which can result in termination of employment for serious breach.
- 5.3 **Segregation of duties.** Where team sizes allow, MDSL separates operational duties between well-defined groups.

- 5.3.1. The **ASP Administration Team** administers and monitors the hosting platform including user account management, management of the web and remote access farms and DBA services for the database servers.
- 5.3.2. The **ASP Infrastructure Team** manages the underlying network infrastructure, servers, storage, and firewalls in addition to security management of users and roles. This team is restricted from accessing application source code or client databases.
- 5.3.3. The **ASP DBA Team** monitors and manages the client databases, including backups, performance and capacity management. This team has no access to manage the underlying network or security infrastructure. All access to client databases is audited.
- 5.3.4. The **ASP Operations Team** performs configuration management and deploys new software code to the ASP hosting platform. This team has no access to manage the underlying network or security infrastructure, and is not permitted to work on client databases without the client's authorization.
- 5.3.5. The **Helpdesk Team** manage client communications and application support (including audited user management), and can gain access to client data only when a ticket is entered by the customer asking for support that would require such access. For the avoidance of doubt, authorization to access client data is deemed to be implicitly granted if the customer asks for assistance with specific customer data or configuration issues.
- 5.3.6. The **MDSL Development Team** has no access to the SaaS hosting platform by default, with development environments separated from the SaaS hosting platform, with rights granted on a need-to-use basis through an audited online system. Senior development leads can request access rights to customer systems or infrastructure for detailed troubleshooting or emergency maintenance, only with authorization from customers or MDSL senior management acting on their behalf, and such access is fully audited.

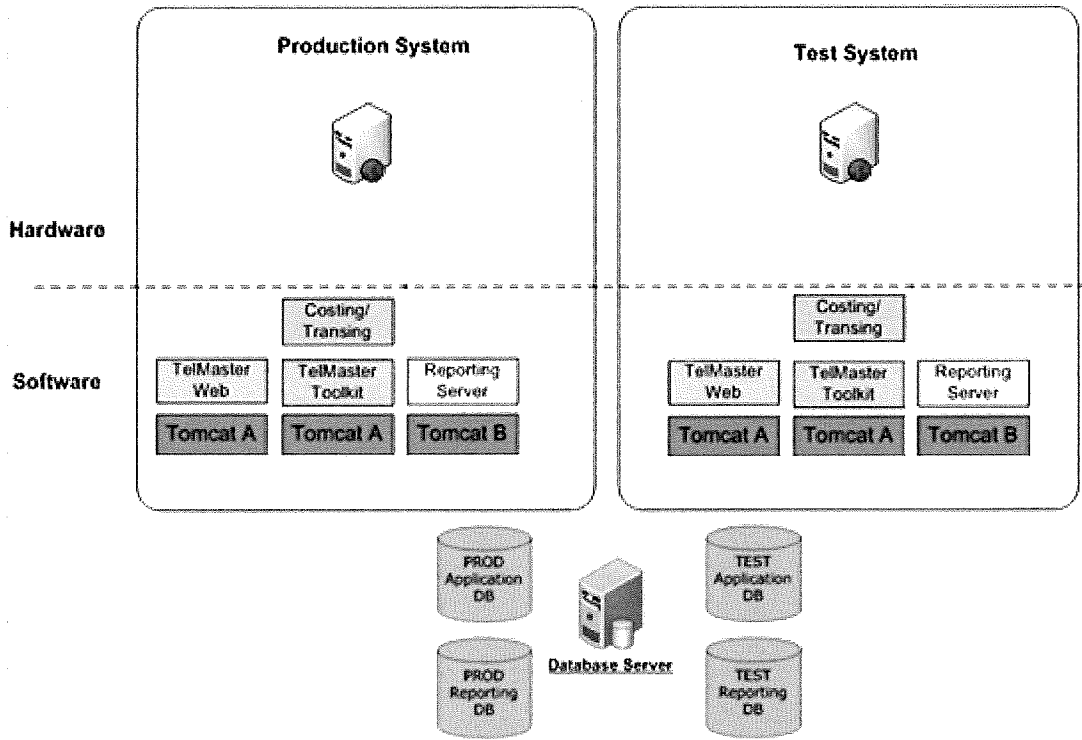
6. User Access Controls

- 6.1 User access controls policies are documented and included in staff training materials, including the MDSL Computer Use Agreement.
- 6.2 Users are provided with unique user IDs unless expressly requested by customer.
- 6.3 Users' access rights to scoped systems are granted according to their functional role, on a "minimum privilege" basis, after appropriate approval from application owner(s), and in alignment with defined ISMS task profiles.
- 6.4 User IDs and initial passwords are provided separately.
- 6.5 For users of MDSL's web products, MDSL supports and recommends the use of Single Sign On (SSO) via SAML 2.0 to mitigate password management concerns. Identity-Provider-Initiated (IdP) and Service-Provider-Redirect (SP) profiles are supported.
- 6.6 Passwords must adhere to minimum security requirements:
 - Passwords expire after 90 days
 - Passwords must meet complexity requirements (including at least 3 of: lowercase, uppercase, numeric, special)
 - Account is locked after 3 failed logon attempts
 - Password history is maintained, past 12 passwords are prohibited
 - Minimum password age to prevent rapid cycling
 - Passwords are not displayed when entered
 - Passwords are encrypted in transit and encrypted/hashed in storage
 - All account access logged and logs maintained for minimum of 3 months
- 6.7 Wherever possible when deploying new information systems, default administrative accounts are disabled, and default passwords are changed.
- 6.8 Customer administrators must be registered & pre-authorized through MDSL account managers prior to requesting changes to user rights.
- 6.9 Access rights are reviewed periodically or ad-hoc on change of user role or status.
- 6.10 Unused user accounts are reviewed on a monthly basis and suspended after 90 days of inactivity or as agreed by customer.
- 6.11 Users are required to log off or lock sessions when not in use.
- 6.12 All corporate MDSL systems are deployed with screensaver locks that activate after 15 minutes of inactivity.
- 6.13 MDSL reserve the right to disable user accounts or applications at any time pending investigation into a security incident. Such suspension will not count as 'Unscheduled Downtime'.

7. Communications & Network Security

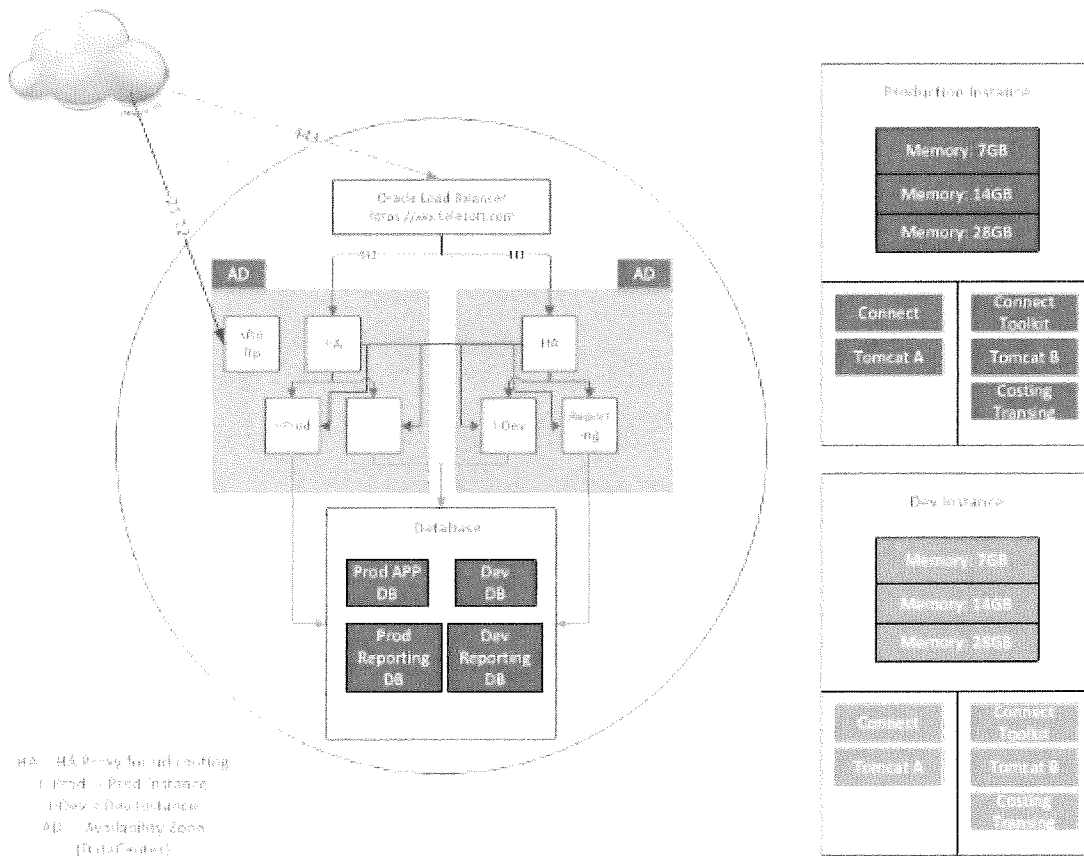
- 7.1 MDSL's networks are defended by redundant, appliance-based, 'stateful packet inspection' firewalls which are configured to permit only the services & protocols essential to the hosting environment.
- 7.2 MDSL maintain a multi-tier DMZ design, segregating internet-facing services from internal secure data segments, with inter-tier data flows protected by firewalls and VLANs.
- 7.3 All data is encrypted in transit to and from the hosting network.
 - 7.3.1. All web services are secured with HTTPS / TLS
 - 7.3.2. File transfers are enabled and protected by SFTP (SSH)
 - 7.3.3. Direct data connections protected by SSH (where configured) with optional client certificates
 - 7.3.4. Emails protected by opportunistic TLS (where configured)
- 7.4 Servers are built against documented security baselines, including VM templates
- 7.5 All network and server hardware is provisioned in resilient / redundant configurations to protect against individual component failure. This includes RAID mirroring for disk, redundant power supplies, SAN controllers, switches, network patching etc.
- 7.6 Systems utilize a common time synchronization service
- 7.7 Certain services interact with Public Cloud services from Amazon Web Services (for DNS via Route 53), Google (Google Maps for Business) and Azure (Bing Maps).
- 7.8 Wireless networking
 - 7.8.1. Wireless networking is not permitted in the MDSL Private Cloud hosting environment.
 - 7.8.2. Wireless networks are segregated in the MDSL corporate environment, and guest SSIDs are provided with no access to MDSL corporate networks.

8. Data Security



- 8.1 MDSL's core products are based on industry standard RDBMS systems, i.e. Microsoft SQL Server running on a Windows Active Directory enabled domain.
- 8.2 Database servers are built against documented security baselines, provisioned into a secure internal data VLAN and monitored by a dedicated DBA team.

- 8.3 Customers are provided with a dedicated production environment (which may include staging database(s)) in addition to one or more non-production environments for acceptance testing or other project purposes.
 - 8.3.1. Each customer environment is provisioned with its own **dedicated** SQL database(s), protected by dedicated Active Directory service accounts.
 - 8.3.2. No data is shared between customer databases in different environments except pre-production, UAT or STAGING copies of the production system, refreshed at the customer's request.
 - 8.3.3. As they do not share data or user accounts, there is a clear **separation of environments**, allowing granular and differentiated security and change control models to be applied within the client administrative user base and MDSL support teams.



- 8.4 Windows Integrated authentication is used for service accounts, ensuring maximum security, mitigating against password leakage concerns, and enabling centralized access control.
- 8.5 NTFS file permissions are used to secure file assets on the hosting domain.
- 8.6 Individual Customers are never granted 'SA' rights to database servers or control over shared resources.
- 8.7 Application Data Lifecycle
 - 8.7.1. Unless otherwise agreed in writing, MDSL solutions will keep up to 13 months of transactional data online and available for reporting.
 - 8.7.2. Older transactional data may be archived to 'near-line' storage.
 - 8.7.3. Data archived in this way can be retrieved on request for up to five years after creation.
- 8.8 Backups
 - 8.8.1. *Full* backups of core customer databases are taken weekly; *differential* backups are taken daily, and log backups taken at least every 15 minutes. In most cases this allows "point-in-time" recovery for at least one week.

- 8.8.2. Log backups are shipped to an alternate datacenter to enable rapid recovery with minimal data loss
- 8.8.3. Non-relational file data is backed up and replicated between datacenters at least daily.
- 8.8.4. Monthly backups are archived for up to seven years.
- 8.9 Virus and malware scanning software is deployed to all workstations and file servers, with definitions updated daily. On-access scanning supplements scheduled scans to ensure real-time security.
- 8.10 At the end of the data lifecycle, e.g. on termination of a client contract, decommissioning of servers or material past an archive retention threshold, MDSL follow a documented data disposal procedure that includes secure file deletion, paper shredding and/or certified physical media applicable. Data is securely destroyed at termination of contract as agreed with each customer and by agreed media
- 9. **Data Protection**
- 9.1 Where MDSL is processing Personal Data for Customer, MDSL will:
 - 9.1.1. only do so on documented Customer instructions and in accordance with applicable law, including with regard to transfers of personal data to a third country or an international organization, and the parties agree that this Agreement and the MDSL Privacy Policies constitute such documented instructions of the Customer; as applicable, MDSL also relies upon (i) MDSL's Privacy Shield certification and/or standard contractual clauses and/or consent for data transfer to the United States to MDSL, and (ii) standard contractual clauses for data transfers to countries outside the European Economic Area, the United States, or countries that do not have adequate levels of data protection as determined by the European Commission, and as such, Customer appoints MDSL as its agent for purposes of entering into any standard contractual clauses for such purposes on Customer's behalf;
 - 9.1.2. ensure that all MDSL personnel involved in the processing of Personal Data have committed themselves to confidentiality;
 - 9.1.3. make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (if applicable to the Customer) where such information is not otherwise available to Customer through its account and user areas or on MDSL websites, provided that Customer provides MDSL with at least 14 days' written notice of such an information request;
 - 9.1.4. promptly notify Customer of all requests received directly from a data subject of any of the Customer Data in respect of that data subject's Personal Data submitted through the Services;
 - 9.1.5. not store Customer Data (in a format that permits identification of relevant data subjects) for longer than is necessary for the purposes for which the data is processed save to the extent, required for legitimate business purposes (with respect to, for example, security and billing) in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes; and
 - 9.1.6. assist Customer as reasonably required (at Customer's expense) where Customer conducts a Data Protection Impact Assessment involving the Services.
- 10. **Application Security**
- 10.1 Software Development
 - 10.1.1. MDSL's applications are designed and developed with security in mind, with defensive coding techniques employed to mitigate threats such as SQL injection and cross site scripting. MDSL coding practices are aligned with OWASP standards and the SANS Web Application checklist.
 - 10.1.2. Both client- and server-side data validation is employed within the application.
 - 10.1.3. Developers do not have access to production data except with written client approval e.g. for resolution of issues raised through a trouble ticket, developing bespoke customer solutions, supporting customer-specific data implementations during a project, or while supporting a controlled infrastructure change.
 - 10.1.4. Sample data for initial software development & testing and pre-pilot client demonstrations is randomly generated from scratch or otherwise securely masked, unless clients have given permission for their data to be used e.g. for custom report, workflow or integration development.
 - 10.1.5. All MDSL source code is stored centrally in a Version Control System (Subversion).
 - 10.1.5.1. Each source code change is tracked against a specific user. Only authorized users are granted access to the source repository.

- 10.1.5.2. MDSL manage multiple branches of code to enable change control best practices (e.g. making emergency security releases of previous versions).
- 10.1.6. MDSL maintain corporate coding standards, standardized development patterns and practices and implement Unit Testing, Continuous Integration and Automated Regression Testing as part of our software build cycle. Each enhancement and defect is tracked in a centrally managed SDLC tracking tool, allowing all areas of the business to monitor status of development in progress.
- 10.1.7. Deployment of new product versions, patches and configuration is controlled through a specific change management process that enforces (a) automatic deployments where possible to increase repeatability and reduce human error and (b) staging guidelines (e.g. internal development → QA → UAT → production) with sign-off and rollback planning at each stage.
- 10.2 **Application Security Model**
 - 10.2.1. The application security model identifies two main types of users: administrative analysts, and web portal end-users. The administrative analysts (typically fewer in number) access the core database system through the IMS web interface and legacy desktop applications; the web portal end-users use a browser based interface for dashboard reporting and access to the self-service procurement portal. Both types of user can be managed from within the inventory application, and both types can be divided into roles and groups for simplified management and restriction.
 - 10.2.2. Role-based security defines (i) which features and objects can be accessed and (ii) which actions can be performed on different types of object
 - 10.2.3. The MDSL application concept of 'physical coverage' restricts data access to specified region(s) of the world for certain users. The Connect tool also employs cost center-based security to restrict data access on a user profile basis.

11. **Operations & Monitoring**

11.1 **Logs**

- 11.1.1. The MDSL applications automatically create audit logs, including server date & time, user ID (and impersonated application user, if applicable) and source application and process details for the following user events. Previous and new values are captured where possible.
 - login
 - lock-out
 - record creation
 - record update
 - record deletion
 - configuration change
 - ad-hoc query
- 11.1.2. Application logs are stored in the relevant customer database instance and are stored according to the retention schedule agreed with customers. By default, application security audit logs are retained indefinitely within application database instance unless archived on request.
- 11.1.3. Application logs and object journals are available from within the MDSL applications to customer's application administrators with appropriate user rights.
- 11.1.4. Infrastructure-wide logs are employed to ensure full audit coverage across the hosting networks. These include OS and Service logs, Firewall connection and IDS/IPS logs (including source IPs & protocol details) and are synchronized via Domain Time Services.
- 11.1.5. Infrastructure & Firewall Logs are centralized in an SIEM system, with access restricted to relevant MDSL Infrastructure team and internal audit staff, and retained for at least 90 days.

11.2 **Monitoring**

- 11.2.1. Critical hosting components are monitored internally and externally by automated systems, ensuring that system administrators are proactively alerted to warning and error conditions within the hosting network.
- 11.3 **Patching**. The ASP Infrastructure Team keeps up-to-date with patches across the system software of all network and server hardware and VMs in the MDSL hosting environment.
 - 11.3.1. A documented release procedure is followed that includes a staged roll-out to testing and final production deployment on a regular basis.

12. **Security Testing**

- 12.1 Security penetration tests are regularly carried out by accredited third parties, including automated weekly network vulnerability scans.
- 12.2 Customers may commission their own penetration and/or application security tests, under the following conditions:
 - 12.2.1. Customer will bear the entire cost of such testing, including, where applicable, 3rd party fees and management or set-up time from MDSL.
 - 12.2.2. Customer must agree with MDSL in advance the scope and timing of the test.
 - 12.2.3. Customer must ensure any testing third party is engaged with confidentiality provisions no less comprehensive than those in this agreement between MDSL and Customer.
 - 12.2.4. Customer will use only accredited information security testers.
 - 12.2.5. Testers will not exploit any vulnerabilities found.
 - 12.2.6. Customer will be liable for any damage caused to MDSL systems resulting from such testing activity.
 - 12.2.7. Results must be shared in full, solely with MDSL, and MDSL will have the right to use the test results for the benefit of all customers.
- 12.3 Issues raised through automated or manual security testing are captured on MDSL's ISO27001 CSIP process to ensure timely and effective resolution.
- 13. **Business Continuity**
 - 13.1 **Global Coverage.**
 - 13.1.1. MDSL maintain primary offices in multiple main time zones for 'follow-the-sun' coverage: GMT, EST, UTC, PST, and HKT.
 - 13.1.2. Each office retains customer support and managed service capability, ensuring service continuity even in the event of an office outage or local incident.
 - 13.1.3. Remote access policies ensure that users can access key corporate resources, and administer hosting services in the event of localized outages.
 - 13.2 **High Availability.** The Software and hosting services are designed and implemented with High Availability in mind (see above). Each provider, hardware and software component is assessed for resilience during service design and selected accordingly.
 - 13.3 **Disaster Recovery – Hosted Software Services**
 - 13.3.1. A "disaster" in relation to hosted Software services will be declared when a major service incident is reported which, after initial investigation, reveals a total datacenter outage, from which recovery is not reasonably expected within one business day.
 - 13.3.2. **Recovery Point Objective (RPO).** MDSL take daily differential backups of customer data, with database log backups every thirty minutes. In addition to supporting point-in-time recovery for local data corruption, these are replicated to alternate datacenters and restored to a 'warm' backup server on a regular schedule, no less frequently than every four hours. The RPO for production customer data is **four hours** – i.e. in the event of a disaster leading to a permanent site outage, customers would lose no more than four hours of transactional data.
 - 13.3.3. **Recovery Time Objective.** The objective of this Plan is to restore critical systems within 48 hours, and Essential systems within 1 week(s) of a disaster that disables any functional area and/or essential equipment supporting the systems or functions in that area.
- 14. **Organizational & Supply Chain Security**
 - 14.1 3rd party risk reviews
 - 14.1.1. Third party vendors and subcontractors are required to adhere to minimum security standards and flow-down data protection terms.
 - 14.1.2. MDSL is independently audited by both the British Standards Institute (BSI) and NDB auditors based in New York
 - 14.2 Legal & Regulatory requirements
 - 14.2.1. MDSL privacy policy is published at <http://www.mdsl.com/privacy-policy>
 - 14.2.2. MDSL is compliant to the General Data Protection Regulation (GDPR)
 - 14.2.3. MDSL is currently SOC 1 and SOC 2 Type 2 attested
 - 14.2.4. MDSL is ISO 27001:2013 certified under certificate No: 5881662
 - 14.2.5. MDSL is registered under the US-EU Privacy Shield Framework, with specific Privacy Shield Policy available at <http://www.mdsl.com/privacy-shield-policy>. To learn more about the Privacy Shield program, and to view the company's certification, please visit: <https://www.privacyshield.gov>

- 14.2.5.1. MDSL is subject to the authority in the US of the Federal Trade Commission (FTC). As such, the FTC has jurisdiction to hear any claims against MDSL regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy.
- 14.2.5.2. In the event that any dispute cannot be satisfactorily resolved by the party concerned and MDSL, MDSL is committed to cooperate with the data protection authorities (DPAs) located in the European Union and Switzerland or their authorized representatives in the investigation and resolution of complaints and will comply with any advice given by the DPAs on specific actions and remedial or compensatory measures required to ensure compliance with Privacy Shield Principles.
- 14.2.6. MDSL is registered with the ICO Data Protection Register under registration no. Z9225870 <https://ico.org.uk/ESDWebPages/DoSearch?reg=365150>

Annex B – Technical Prerequisites (Connect)

This document describes the requirements of the client's technical environment to use and access MDSL services.

These requirements will evolve regularly with new product releases, aligned with industry best practice, emerging technologies or security threats. Updated versions will be communicated to customers on a regular basis to allow forward planning and risk mitigation.

1. Environment

1.1. Internet Protocol Version

1.1.1. Connect requires Internet Protocol version 4 on the database server, web servers, costing server, and client machines.

1.1.2. Connect does not support native Internet Protocol version 6.

1.2. Virtual Environments

1.2.1. MDSL supports virtualized guest host machines for the Connect application, toolkit, reporting server, and costing server.

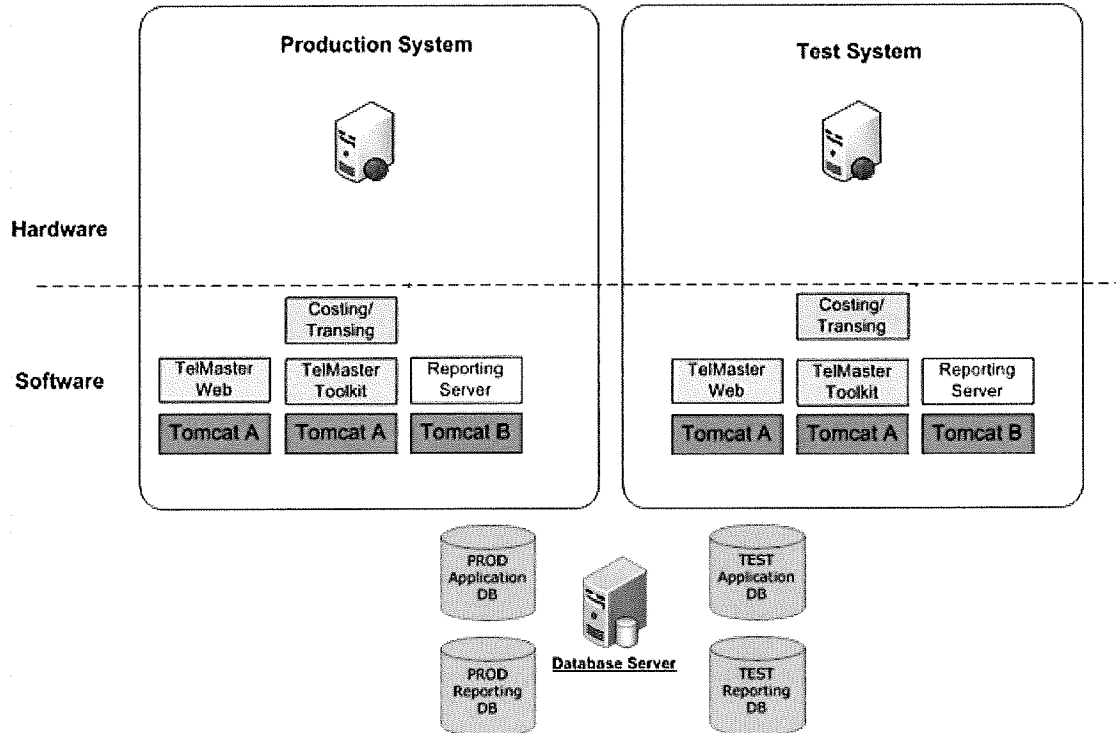
1.2.2. MDSL does not support virtualized guest host machines for the database tier.

1.2.3. VMWare® is fully supported as a virtualized technology.

1.2.4. Ensure that the RAM/CPU allocated to the virtual environment is reserved and dedicated rather than being over-allocated. If the RAM/CPU is over-allocated, those resources (at the levels required by Connect) might not always be available to the guest system. Additionally, JVMs will crash if the balloon driver is activated due to over allocation. VMWare® suggests disabling the balloon driver to prevent this from happening.

2. Recommended Server Configuration

2.1. The figure below shows the recommended hardware and software configuration for production and test systems.



3. Database Server Requirements

- 3.1. Connect requires two database instances: one for application data and another for reporting data. Use of the same database software is required, either Microsoft® SQL Server™ or Oracle®, for both instances.
- 3.2. MDSL must have full DDL and DML permissions to the database, and must be able to:
 - 3.2.1. Create, add, and modify table data.
 - 3.2.2. Create, add, and modify tables and data types.
- 3.3. For SQL Server, create a TELMAST user as the DBO for all database tables and objects in both instances.
 - 3.3.1. When using SQL Server, Connect requires a SQL Authentication account.
 - 3.3.2. To support internationalization, you must use one of the supported database character sets. See [this link](#) for more details.

	Minimum	Recommended	High-Load
Processor	Dual Core Intel® Xeon® or AMD® Opteron® 2 GHz or faster	Quad Core Intel® Xeon® or AMD® Opteron® 2.5 GHz or faster, 64-bit	2x Quad Core Intel® Xeon® 2.5 GHz or faster, 64-bit
Cache	2 MB Cache	4 MB Cache	12 MB Cache
Memory	8 GB 667MHz	16 GB 667MHz	64 GB 667MHz or more
Hard Drive	2x 500 GB 10K RPM 2x Disk Controllers (duplex configuration)	4x 500 GB 10K RPM 2x Disk Controllers (duplex configuration)	4x 750 GB 15K RPM 2x Disk Controllers (duplex configuration)
Storage	RAID 1	RAID 0+1	RAID 0+1
CD-ROM/ DVD-ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM
Ethernet Card	Dual Gigabit Ethernet Cards (minimum Gigabit connectivity to Costing and ToolKit Servers)	Dual Gigabit Ethernet Cards (minimum Gigabit connectivity to Costing and ToolKit Servers)	Dual Gigabit Ethernet Cards (minimum Gigabit connectivity to Costing and ToolKit Servers)
DR RS232 or Serial Ports	Need to be available for live call collection only	Need to be available for live call collection only	Need to be available for live call collection only
Operating System	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above
Database Software	Oracle12c, or SQL Server 2012 and above (Standard or Enterprise)	Oracle12c, or SQL Server 2012 and above (Standard or Enterprise)	Oracle12c, or SQL Server 2012 and above Enterprise
Oracle character encoding setting	Must be set to UTF-8/Unicode	Must be set to UTF-8/Unicode	Must be set to UTF-8/Unicode

- 3.4. Performance characteristics for a given database instance can vary greatly depending on the speed of the network, the configuration of the hardware, and the database engine setup. To ensure that the database instance will provide adequate performance for the Connect application, MDSL requires that each database instance be speed tested. The database must exhibit a performance characteristic of 10,000 update, read, and write operations in under 20 seconds. The test must be performed using the DatabasePerformanceTestProcessor in the Connect Toolkit and MDSL's Technical Support team will manage the process to run the tests.
4. Web Server/Reporting Server Hardware Requirements
 - 4.1. The Web server and the Reporting server must be set to the same time zone.
 - 4.2. Connect does not support the use of reverse proxies between client machines and host Web servers.
 - 4.3. If using a Windows system, Admin rights are required for installing Connect.
 - 4.4. If using a Unix-based system, root access is required for installing Connect.

	Minimum	Recommended	High-Load
--	---------	-------------	-----------

*Processor	Dual Core Intel® Xeon® or AMD® Opteron® 2 GHz or faster	Dual Core Intel® Xeon® or AMD® Opteron® 2.5 GHz or faster, 64-bit	Dual Core Intel® Xeon® or AMD® Opteron® 2.5 GHz or faster, 64-bit
Cache	2 MB Cache	4 MB Cache	4 MB Cache
Memory	10 GB 667MHz Dual Ranked DIMMs (2 GB allocated to each JVM instance)	20 GB 667MHz Dual Ranked DIMMs (4 GB allocated to each JVM instance)	32 GB 667MHz Dual Ranked DIMMs (8 GB allocated to each JVM instance)
Hard Drive	100 GB 10,000 RPM	100 GB 10,000 RPM	100 GB 10,000 RPM
Storage	NA	NA	NA
CD-ROM/ DVD-ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM
Ethernet Card	Dual Gigabit Ethernet Cards	Dual Gigabit Ethernet Cards	Dual Gigabit Ethernet Cards
DR RS232 or Serial Ports	Need to be available for live call collection only	Need to be available for live call collection only	Need to be available for live call collection only
Operating System	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above
JDK Version	1.8.0, 64-bit	1.8.0, 64-bit	1.8.0, 64-bit
**Web Service	Apache Tomcat™ 8.x	Apache Tomcat™ 8.x	Apache Tomcat™ 8.x

4.5. * Connect (v1.x) requires a 64-bit Web server for the application and toolkit. A 64-bit JVM (Java Virtual Machine) is not limited to the 2 GB memory allocation that applies to a 32-bit JVM.

4.6. ** The Connect installer deploys the required Tomcat Web server instance.

4.7. To successfully support licensed customers, MDSL needs Microsoft Excel, the Microsoft Excel viewer, or Open office installed on the Web Server to view and/or manipulate various files (example: vendor feeds).

5. Costing Server/Toolkit Server Hardware Requirements

	Minimum	Recommended	High-Load
Processor	Dual Core Intel® Xeon® or AMD® Opteron® 2 GHz or faster	Dual Core Intel® Xeon® or AMD® Opteron® 2.5 GHz or faster, 64-bit	Dual Core Intel® Xeon® or AMD® Opteron® 2.5 GHz or faster, 64-bit
Cache	2 MB Cache	4 MB Cache	4 MB Cache
Memory	10 GB 100MHz (2 GB allocated to each JVM instance)	10 GB 100MHz (4 GB allocated to each JVM instance)	32 GB 100MHz (8 GB allocated to each JVM instance)
Hard Drive	2x 250 GB 10K RPM 2x Disk Controllers (duplex configuration)	2x 500 GB 10K RPM 2x Disk Controllers (duplex configuration)	2x 750 GB 10K RPM 2x Disk Controllers (duplex configuration)
Storage	RAID 1	RAID 1	RAID 1
CD-ROM/ DVD-ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM	48x IDE Internal CD-RW/DVD ROM
Ethernet Card	Dual Gigabit Ethernet Cards	Dual Gigabit Ethernet Cards	Dual Gigabit Ethernet Cards
DR RS232 or Serial Ports	Need to be available for live call collection only	Need to be available for live call collection only	Need to be available for live call collection only
Operating System	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above	Windows Server® 2012, Ubuntu® 16.04 and above
JDK Version	1.8.0, 64-bit	1.8.0, 64-bit	1.8.0, 64-bit

5.1. To successfully support licensed customers, MDSL needs Microsoft Excel, the Microsoft Excel viewer, or Open office installed on the Web Server to view and/or manipulate various files (example: vendor feeds).

6. Client Hardware Requirements

	Minimum	Recommended	High-Load
Processor	1.5 GHz or faster	2.5 GHz or faster	2.5 GHz or faster
Cache	2 MB Cache	2 MB Cache	2 MB Cache
Memory	4 GB 100MHz	8 GB 100MHz	16 GB 100MHz
Hard Drive	100 GB 10K RPM	100 GB 10K RPM	100 GB 10K RPM

Ethernet Card	Gigabit Ethernet Card	Gigabit Ethernet Card	Gigabit Ethernet Card
Browser	Internet Explorer® 10x, 11.x, latest versions of Edge®, Chrome®	Internet Explorer® 11.x, latest versions of Edge®, Chrome®	Internet Explorer® 11.x, latest versions of Edge®, Chrome®
	Caution: Connect has been lightly tested against the most recent versions of Chrome and Firefox. You may use Chrome and Firefox, but official support is only provided for IE. MDSL will not troubleshoot or modify its application for issues related to non-supported browsers or versions.		
Screen Resolution	1152x864	1280x1024	1280x1024
Operating System	Windows® 7, Windows® 8, Windows® 10	Windows® 7, Windows® 8, Windows® 10	Windows® 7, Windows® 8, Windows® 10

7. Other

7.1. PDF Reader software is required for printing work orders.

7.2. Connect does not support the use of reverse proxies between client machines and host Web servers.

Annex C – Software Release Policy

This document outlines MDSL’s software release and associated technical support policy as updated March 2018.

1. **Monthly Release Cycle**

- 1.1 MDSL follows a monthly release cadence for its core products. By releasing monthly, MDSL can bring valuable enhancements to market more rapidly, in addition to providing more timely fixes to issues.
- 1.2 In order to ensure platform stability, new features will be hidden by default, and enabled only after the customer has accepted the new functionality as part of a User Acceptance Testing cycle.
- 1.3 Release notes will be provided online with each release.
- 1.4 Releases are numbered YYYY.MM after the year and month of release e.g. 2017.01 for the release made in January 2017. This convention allows customers to easily understand the age of a given release, and the associated support services available based on the Technical Support Policies below.

2. **Release Availability & Upgrades**

- 2.1 Because MDSL provides customers with a dedicated database instance, and to best comply with Customer’s change management procedures, Customers may choose when to implement a software release under advisement from Supplier.
- 2.2 Customers must be mindful of the Technical Support policies below and agree a regular upgrade schedule with their account managers to ensure their Software remains in ‘Active Support’.
- 2.3 MDSL account managers will provide advice on the upgrade process, encouraging upgrades to newer releases where appropriate to a customer’s needs.
- 2.4 The highly configurable nature of the Software means Customers should accept new product versions in a User Acceptance Testing (“UAT”) environment, made available by Supplier, before an upgrade to a Customer’s production environment proceeds.

3. **Technical Support & Patching Policy**

MDSL provides at least 12 months’ support for each release, on the following schedule:

3.1 **Active Support**

MDSL will provide “Active Support” on a regular monthly release for six months after the release date. During this time, MDSL will proactively provide patches, hot-fixes or workarounds to enable the Products to operate in substantial conformity with its then-current operating documentation.

3.2 **Extended Support**

Following the Full Support period, MDSL will provide six months of “Extended Support”. No enhancements will be made to releases under “Extended Support”, and customers will be advised to upgrade to more recent release to resolve all non-critical issues. Customer Support teams will apply existing patches or workarounds, where possible, on an ad-hoc basis for critical issues only. For the purposes of this policy, a “critical” issue is an issue that substantially increases the risk to the confidentiality, integrity or availability of client’s data, and for which no reasonable workaround is available.

3.3 **No Support**

Following the “Extended Support” period, a software release will receive no active technical support, but customers may continue to use the software at their own risk. No new enhancements, fixes or patches will be developed and customers should upgrade to a release in “Full Support” status at their earliest opportunity. Customer Support teams will direct

customers to upgrade to a more current version as a first step in resolving any operational problems.

3.4 End of Life

MDSL may “end of life” a product release, and the associated access & infrastructure, following the Extended Support period, by giving 6 months’ notice or as otherwise agreed with customers. At this time, access to “End of Life” products will terminate.

4. Enhancement Requests

4.1 MDSL encourages customers to submit enhancement requests at any time through their account manager or the online helpdesk.

4.2 Inclusion of enhancements into the MDSL product roadmap is at MDSL’s sole discretion.

4.3 New features and enhancements will be developed for release in future versions only. MDSL cannot make feature enhancements to already-released versions.

4.4 Specific project-based agreements can be made on a commercial basis to accelerate development of specific feature sets on a case by case basis.

Annex D – Use of Third-Party Software

1. The Supplier's Software includes software products ("Third-Party Components") produced and licensed to Supplier by third parties ("Supplier's Third-Party Suppliers").
2. Third-Party Components are protected by copyright and other intellectual property rights and elements thereof, including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Supplier's products, are owned by the Third-Party Suppliers. Customer shall not remove, modify or obscure any copyright trademark or other proprietary rights notices that are contained in or on the Third-Party Components. The Third-Party Components are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Customer's possession, access, or use of the Third-Party Components does not transfer any ownership of the Third-Party Components or any intellectual property rights to Customer.
3. Customer may not reverse engineer, decompile, or disassemble the Software (including any Third-Party Components), except and only to the extent that applicable law, notwithstanding this limitation, expressly permits such activity.
4. Customer acknowledges that Suppliers Third-Party Suppliers disclaim, to the extent permitted by applicable law, all warranties by them and any liability by Supplier's Third-Party Suppliers or their suppliers for any damages, whether direct, indirect, or consequential, arising from the Third-Party Components included in the Software.
5. Customer permits the disclosure by Supplier of software usage information to Supplier's Third-Party Suppliers as required under the agreement(s) between Supplier and Supplier's Third-Party Suppliers. Such disclosure is limited only to the Customer name, address.

Annex E - Change Control Procedure

The requesting party will submit and document all changes via a Change Request Form (see template below).

The Change Request shall detail:

- the proposed change(s);
- an analysis of the reasons why the change(s) are required;
- the proposed approach to implement the requested change(s); and
- the impact of the change(s) on project schedule, fees and expenses.

Upon written acceptance of the Change Request by both parties, the Software, Services or Scope will be modified and any fees or additional charges will be adjusted accordingly.

Supplier shall have no obligation to perform or schedule any work until the Change Request is approved and accepted in writing by both parties.

Change Request Form Template

Title of Change Request:

Customer Name:

Requester:

Date:

Overview of Current Situation and Requirement:

Reason for the Change:

Proposed Change:

Project Risks and Assumptions:

Proposed Timeline:

Changes to Fees and Expenses:

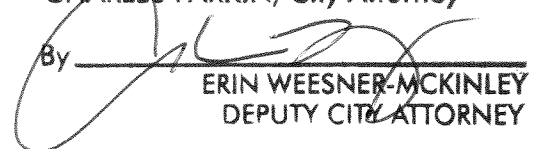
The parties agree to the above specifications and have executed this Change Request as of the date(s) set forth below.

APPROVED AS TO FORM

September 23, 2020

CHARLES PARKIN, City Attorney

By

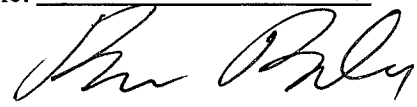


ERIN WEESNER-MCKINLEY
DEPUTY CITY ATTORNEY

MDSL

Customer

Name: BRIAN BRADY



Title: CFO

Date: 8/21/20

Name: _____

Title: _____

Date: _____