January 26, 2026

Lake County Managed services in OCI

Firm Fixed Price Services Exhibit A
DLT Quote #: 5398429
Offer Valid through: March 31, 2026

Project Team

Data Intensity: JR Mariottini, Sales Account Manager, jmariottini@dataintensity.com, (630) 841-5129:

Customer: DLT Solutions (Part of TD SYNNEX Public Sector) ("Customer") OBO Lake County, Jessica Marino, Team Lead Enterprise Applications, jessica.marino@dlt.com, (703) 773-9262

Data Intensity reserves the right to make changes to the project team member(s) herein. Customer may also request changes to the project team, and Data Intensity will make best efforts to change any project team member(s) as requested and use its best efforts to minimize impact to the project schedule and project estimated hours. Any Customer changes to the project team member(s) that impact the project scheduled or estimated hours shall require a written change order between the parties, to reflect any required adjustments, prior to any such change being implemented. **This Exhibit A ("Exhibit A," "Order Form," or "OF"), and the offer and terms herein shall, unless executed, expire thirty (30) days from 23-Jan-26.**

Therefore, the parties agree:

MANAGED SERVICES

► DELIVERABLES:

Managed services deliverables are as set forth in, and in accordance with, the applicable Exhibit B.

► SCOPE OF SERVICES:

The services included as in-scope under this OF are as set forth in, and in accordance with, the applicable Exhibit B.

► SLA(s):

The services provided herein shall be delivered in accordance with the Service Level Agreement(s), as set forth in the applicable Exhibit B.

► IN-SCOPE ENVIRONMENTS/INFRASTRUCTURE:

In-Scope Environments/Infrastructure Inventory List is as set forth in, and in accordance with, the applicable Exhibit C.

► CUSTOMER ROLES AND RESPONSIBLITIES:

In order for Data Intensity to provide the Services, Customer agrees to the following:

- Cooperation – Customer agrees to assist Data Intensity in its efforts, and to exercise due diligence in responding to requests for information, or other assistance, in a timely manner.
- Support Agreements – Customer will maintain current original software vendor support on all Data Intensity managed workloads: software, applications or hardware.
- Verification of Support Levels - Customer agrees to allow Data Intensity to verify support types and support levels for all managed workloads.

- Lack of original software vendor support, and/or use of third-party support services, reduces all applicable Service Level Agreements to reasonable efforts and may expose Customer to additional charges for the elongated response times caused by the aforementioned.
- Activity Disclosure – Customer will inform Data Intensity of any activities that may impact Customer's Environment and Data Intensity's ability to perform the Services. Data Intensity will not be held responsible for any issues or service loss resulting from any tasks performed by Customer's personnel, or third-party vendors, on the Customer Environment without prior written notification and mutual acceptance should change affect the ability for DI to provision the contracted Services hereunder. This includes administrative password changes or anything significantly affecting the Customer Environment.
- Connectivity – Within three (3) business days from the Effective Date, Customer will assist in providing Data Intensity with a VPN connection between Customer site and the Data Intensity network. In addition, Customer will assist in maintaining such VPN connection during any term under this OF.
- Access - Customer will provide Data Intensity the necessary access and information to implement applicable monitoring systems.
- Kick-off Meeting - Data Intensity will schedule a meeting between Customer and network provider to coordinate the technical infrastructure for the implementation.
- Systems Documentation - Data Intensity shall have the right to document the hardware, hosting, operating system, database software, and applications software of the Customer Environment.
- Passwords - Customer will provide Data Intensity with all required administrative passwords to access and support the Customer Environment.
- Ticketing System – Customer will use Data Intensity's ticketing system to issue requests regarding the Services herein.

► ACCEPTANCE PROCESS:

The deliverables will be subject to the following acceptance process:
The deliverables are considered complete when delivered to Customer for review. After submission of the deliverable(s) by Data Intensity, Customer shall, within seven (7) days (the "Acceptance Period"), review and evaluate the deliverable to determine whether the deliverables satisfy the acceptance criteria in all material respects. "Acceptance Criteria" means the deliverable materially conforms to the contract specifications or would pass within the industry unrejected. If the deliverables satisfy the Acceptance Criteria, prior to the end of the Acceptance Period, Customer may provide a written acceptance to Data Intensity. If Customer fails to notify Data Intensity of rejection of a deliverable within the Acceptance Period, then the deliverable(s) shall be deemed accepted.

For any deliverables not accepted, due to nonconformity, Customer will notify Data Intensity in writing, within the Acceptance Period, of the rejected deliverable(s) with sufficient details (a "Rejection Notice") to allow Data Intensity to revise the deliverables into conformance. Thereafter, Data Intensity will resubmit the modified deliverable to Customer.

Resubmitted deliverables will be subject to the Acceptance Period. Customer will limit its review of the resubmitted deliverable(s) to determine whether Data Intensity has corrected the nonconformance. In the event Data Intensity has not cured such nonconformance within thirty (30) days of written notice from Customer, Customer may terminate this Exhibit A in accordance with the MSA.

FEES

For the Services provided herein, Customer agrees to pay Data Intensity the following fees in accordance with the applicable Section(s) below:

1.1 Fee Structure

1.1.1 Managed Services Total Ops Management ("TOM"):

a. Renewal Term: Twelve (12) months. The Term shall commence in accordance with Section 1.1.1 (c) herein ("Term Start Date").
b. Termination Rights: No termination for convenience. For further clarification and the avoidance of doubt, except as otherwise stated herein, Customer may not reduce the quantity of services purchased hereunder, in whole or in part, during the Term set forth herein.

The TOM Services under this Exhibit A are considered a:

a. Renewal Order: The Renewal Term under this Exhibit A will begin on May 29, 2026 ("Renewal Term Start Date") which represents a monthly increase of $2,069.74 from $18,567.00 to $20,636.74.

TOM Fee Structure:

Item	Description	Quantity	Unit Price	Monthly
RMS- Total Operations Mgmt Services				
OCI-INFRA-TENMGT-TOM	Numbe of OCI Tenancy(s)	1	$469.52	$469.52
RMS-APPS-EBS-TOMMC	Critical Medium EBS instance - DR	1	$951.17	$951.17
RMS-APPS-EBS-TOMMC	Critical Medium EBS instance	1	$2,140.11	$2,140.11
RMS-APPS-EBS-TOMMNC	Non Critical Medium EBS instance	5	$1,426.70	$7,133.50
RMS-APPS-WLS-TOMSC	Critical Small OLM instance	1	$581.70	$581.70
RMS-APPS-WLS-TOMSNC	Non Critical Small OLM instance	1	$436.86	$436.86
RMS-DB-ORCL-TOMMC	Critical Medium database instance (Oracle)	1	$697.23	$697.23
RMS-DB-ORCL-TOMMC	Critical Medium database instance (DR Oracle)	1	$309.89	$309.89
RMS-DB-ORCL-TOMMNC	Non Critical Medium database instance (Oracle)	5	$464.36	$2,321.80
RMS-ENT-EBS-DBCONETASK	E-Business Suite Clone Service Task # per month	35	$23.19	$811.65
RMS-ENT-ORCL-DRTEST	The number of hours DR tests per annum (Oracle)	1	$327.66	$327.66
RMS-ENT-ORCL-TOMCRAQTR	Total Ops Management CRA Quarterly Entitlement	30	$84.26	$2,527.80
RMS-INFRA-LIN-TOMC	Critical infrastructure instance	18	$70.21	$1,263.78
RMS-INFRA-LIN-TOMNC	Non Critical infrastructure instance	11	$60.37	$664.07
RMS-ENT-ORCL-DRPHYSTAND	DR Standby Type - Physical Standby (Oracle)	1	$0.00	$0.00
Transition Fees and/or Overage Rates				
OCI-INFRA-LIN-TOMOVER	Overage rate $205.00	1		
OCI-INFRA-TENMGT-TOMOVER	Overage rate 205.00	1		
RMS-DB-ORCL-TOMOVER	Overage rate (Oracle) $220.00	1		
RMS-ENT-EBS-TOMOVER	Total Ops Management Overage $220.00	1		
		Total in USD		$20,636.74

1.2 Invoicing:

1.2.1

Terms of Payment: Invoices for applicable: (i) ***Managed Services*** (which may include, but is not limited to: a. Total Ops Management ("TOM"); b. Functional Support Desk ("FSD"); c. Client Request Account ("CRA") hours; d. License Management as a Service ("LMaaS"); e. and/or g. Subscription Fees, collectively referred to as Monthly Recurring Fees ("MRF")); and (ii) Overages, shall be submitted in accordance with the Term, service type, and pricing listed within Section 1.1, this Section 1.2, and as detailed in Exhibit B if applicable, throughout the Term. Invoicing for applicable one-time connection/set-up/service transition fees will occur upon execution of this Exhibit A. All invoiced amounts are due and payable net thirty (30) days from the date of invoice. A late payment interest charge of 1.5% per month (18% per annum) will be assessed on invoices not paid when due. Except for Customer's obligation to make payments under this Exhibit A, neither party will be liable for any failure or delay in its performance due to any unusual cause beyond its reasonable control, including, but not limited to, acts of war, or acts of God.

1.2.2

Managed Services MRF: Except as otherwise stated herein, invoicing for the MRF, for those Entitlements as applicable and detailed herein, will commence in accordance with Section 1.1.1. (c) herein. The initial MRF shall be prorated for the initial month based on the number or remaining days in the month. Thereafter, invoices shall be submitted monthly in advance.

1.2.3

CRA hours: Invoicing for the minimum monthly amount of CRA hours, as applicable and detailed herein, will commence upon the earlier of either the execution of this Exhibit A or the Term Start Date, whichever date allows Customer access to the CRA hours, and shall be prorated for the initial month based on the number of remaining days in the month. Thereafter, charges for CRA hours shall be included in the regular monthly invoices and shall be submitted monthly in advance, in accordance with the applicable Exhibit B. Time will be deducted from the allotted CRA hours in minimum increments of thirty (30) minutes to reflect time actually worked, rounded up based on total hours booked to each individual ticket per calendar month. Any CRA hours consumed beyond the required minimum monthly amount listed herein will be invoiced as overages, quarterly in arrears. The rates herein are based upon a global rate. All CRA support will be provided in English and by personnel with the requisite skills and qualifications. For further clarity and the avoidance of doubt, any unused allotted minimum monthly CRA hours shall expire at the end of that given quarter and cannot be carried over or borrowed against. Any rolled over hours that are unused at the end of the roll over period for that shall expire at the end of that given calendar quarter.

1.2.4

Overages: With the exception of CRA hours, any overages of the Services shall be invoiced monthly in arrears at the established overage rate, as detailed and applicable herein, in accordance with the applicable Exhibit B.

1.2.5

Additional Compensation / Out of Scope Fees: Data Intensity shall not be responsible for providing any services that are not expressly set forth in this Exhibit A. Any such additional or out of scope work shall be in accordance with the applicable Exhibit B either i) through a mutually agreed upon written change order or amendment; or ii) under separate agreement, as applicable. All fees charged by Data Intensity are exclusive of tax. In the event Data Intensity is required to collect such tax, the respective amounts will be added to the invoice and will be payable by Customer along with the fee for Services. For further clarification and the avoidance of doubt, Customer is responsible for all taxes, including sales and use taxes, as well as VAT, as applicable, on all services provided by Data Intensity along with the fee for Services. In addition to the foregoing, the fees herein do not include reasonable travel and expense ("T&E") of Data Intensity's consultants and any such T&E will be invoiced separately, due net thirty (30) days from date of invoice, provided Customer preapproves

such expenses in advance.

ACCEPTANCE OF ORDER

CUSTOMER ACKNOWLEDGES IT HAS FULLY AND COMPLETELY READ THIS EXHIBIT A, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS. FURTHER, CUSTOMER AGREES THAT THIS EXHIBIT A, ALONG WITH THE MSA AND THE APPLICABLE EXHIBITS B AND C, SIGNED BY BOTH PARTIES (COLLECTIVELY REFERRED TO HEREIN AS THE "AGREEMENT"), CONSTITUTES THE ENTIRE AGREEMENT BETWEEN THE PARTIES WITH RESPECT TO THE SUBJECT MATTER HEREOF, AND SUPERSEDE ANY AND ALL OTHER AGREEMENTS, UNDERSTANDINGS, AND UNDERTAKINGS, WHETHER WRITTEN OR ORAL, BETWEEN THE PARTIES IN RELATION TO THIS SUBJECT MATTER. IN THE EVENT OF A CONFLICT BETWEEN THE PROVISIONS OF THIS EXHIBIT A AND THE AGREEMENT, THE DOCUMENTS WHICH COMPRISE THE AGREEMENT SHALL GOVERN IN THE FOLLOWING DECREASING ORDER OF PRECEDENCE: A) EXHIBIT A; B) THE APPLICABLE EXHIBIT B; C) THE APPLICABLE EXHIBIT C; AND D) THE MSA.

CUSTOMER PURCHASE ORDER IS DUE AT TIME OF EXECUTION IN ORDER TO PROCEED HOWEVER, IN NO EVENT SHALL ANY PRE-PRINTED TERMS AND CONDITIONS OR OTHER PROVISIONS SET FORTH IN ANY ADDITIONAL DOCUMENTS, INCLUDING BUT NOT LIMITED TO A CUSTOMER'S PURCHASE ORDER, OR ANY RESTRICTIVE ENDORSEMENT ON ANY CHECK OR ANY INSTRUMENT OF PAYMENT, BE CONSTRUED TO MODIFY, AMEND OR ADD TO THE TERMS OF THE AGREEMENT, REGARDLESS OF ANY SUCH TERMS DATE OF ISSUE, NOW OR IN THE FUTURE, UNLESS SPECIFICALLY AGREED TO IN WRITING BY BOTH PARTIES. ANY SUCH ADDITIONAL TERMS SHALL BE VOID AND OF NO FORCE OR EFFECT.

EXECUTED AS AN INSTRUMENT UNDER SEAL AND AGREED TO AS OF May 26, 2026 (THE "EFFECTIVE DATE").

LAKE COUNTY	**DLT SOLUTIONS**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

January 26, 2026

Lake County

Data Intensity Total Ops Management Services - Exhibit B
DLT Quote: 5398429
Offer Valid through: March 31, 2026

A: SUPPORTED CAPABILITIES

Table A:

	Capability	Applicable Scope
☒	Managed Services (DSP)	Current vendor supported versions of **Oracle Database** DB Supported Products ("DSP"). All in-scope instances will be entered in the Data Intensity Configuration Management Database ("CMDB") system (see Exhibit C).
☒	Managed Services (TASP)	Current vendor supported versions of **Oracle EBS, OLM** Technical Application Supported Products ("TASP"). DSP Services are required in order to select TASP as in-scope. All in-scope instances will be entered in the Data Intensity CMDB system (see Exhibit C).
☐	Managed Services License Management as a Service ("LMaaS")	LMaaS provides the Customer with a service to protect their license position to avoid economic impacts of an audit. In-scope vendor(s) and environments are defined in Exhibit C. **Should Customer choose to opt-out of LMaaS Customer affirmatively acknowledges they are solely liable and exclusively responsible, without limitation, for their entire licensing position.**
☒	Managed Services (CCMSP)	Public cloud vendor(s) **OCI** Tenancy Management Supported Platform(s) ("**TMSP**"). All in-scope subscriptions will be entered in the Data Intensity Configuration Management Database ("CMDB") system (see Exhibit C). This includes: a. **Primary Tenancy Administration:** Provide primary public cloud portal and tenant administrator rights and roles management as well as cloud provider dashboard management; b. **Tenancy Policy Management:** Provide initial policy setup, access control and architecture consumption policies, firewall policy management, and ongoing VLAN networks service management; c. **Cloud Inventory Resource Visibility:** Provide ongoing visualization, through Customer Portal, of deployed resources by tagging group; d. **Capacity Management and Threshold Monitoring:** Provide ongoing resource monitoring and threshold management against environment consumption for compute, network, and storage services; e. **Monthly Cost Utilization:** Provide visibility of real-time data within the Customer portal, through reports available via ticket requests, depicting consumption patterns for existing and new resource consumption; f. **Cloud Architecture Governance:** Based on best practices for design, network services and security groups, tagging strategies, and **annual** review of architecture for best practices and consumption optimization; g. **High Availability Recommendations:** Provide **annual** review of changes to ensure that fault-tolerance is effective based on contracted managed services. Provide recommendations to improve costs and ensure proper high availability best practices are recommended (additional fees may apply); h. **Basic Security Management:** Based on best practices, and Customer agreed upon implemented access and control policy, provide **quarterly** implementation (via ticket request) and ongoing management of cloud vendor native tools (e.g., OCI Cloud Guard); and i. **Configuration Management Bundle:** Includes **ten (10)** Move, Add, Change, Delete ("MACD") changes per month. This provides the facility to undertake MACD of tenancy setting and configuration (e.g., VM configuration changes, region changes, and Firewall ("FW") rule changes)

☒	Managed Services (OSSP)	Current vendor supported versions of **Linux (all variants)** Operating System Supported Products ("OSSP"). All in-scope instances will be entered in the Data Intensity CMDB system (see Exhibit C).

B: ENTITLEMENTS: BASELINE MANAGED SERVICES PACKAGE

The Managed Services as listed within Table B below are considered in-scope and are provided for supported DSP, CCMSP, TASP, OSSP as selected, and detailed, in Table A and Exhibit C.

***Table B:**

Service Capability	Business as Usual ("BAU") Managed Service for in-scope DSP, CCMSP, TASP, OSSP
Incident Management	Receive, acknowledge, classify, and manage incidents in accordance with the mutually agreed upon Service Level Agreement ("SLA(s)"). Data Intensity manages all the aspects of a major incident, including resources and communication, through Major Incident Management ("MIM") (e.g., If it is an incident, a change driven by an incident, or a problem record generated from an incident, except as otherwise detailed in Table D, it is included in TOM).
Major Incident Management ("MIM")	Major incidents are those for which the degree of impact on the Customer's business/organization is extreme. Incidents for which the timescale of disruption – to even a relatively small percentage of users – becomes excessive should also be regarded as major incidents. Priority 1 status is used to identify major incidents. Shorter timescales and greater urgency, is used for major incidents. Where necessary, MIM includes the dynamic establishment of a separate major incident team, under the direct leadership of the Data Intensity incident manager. The major incident team is formulated to concentrate on the major incident alone, and to ensure that adequate resources and focus are provided for finding a fast resolution. MIM manages all aspects of a major incident, including resources and communication. Within seventy-two (72) hours after the restoration of the major incident (as detailed herein, see Table I), a Root Cause Analysis ("RCA") investigation will be undertaken. Either the RCA will be provided or, if this cannot be identified at the time, a problem record will be created.
Change Management	Receive, acknowledge, classify, and manage changes in accordance with the mutually agreed upon SLA(s) for incident-driven changes based upon monitoring services. Data Intensity will work with the Customer-designated responsible authority to determine commercial impact to the Managed Service and to facilitate timely, accurate, and efficient environment changes to limit disruption of use/ system, with traceability and proper controls for auditing purposes, in accordance with the terms herein (for Customer generated change, see Table D).
Service Request Management (for in-scope services)	Receive, acknowledge, classify, and manage service requests in accordance with the terms herein and the mutually agreed upon SLA(s). Data Intensity will work with the Customer-designated responsible authority to determine commercial impact and to facilitate timely, accurate and efficient environment implementation of the service request to limit disruption of use/system, with traceability and proper controls for auditing purposes in accordance with the terms herein (for Customer generated/out of scope Service Request, see Table D).
Patch Management	System critical break-fix/bug patches to resolve an incident are included as part of the Managed Service hereunder. Data Intensity will ensure proper planning for successful deployment, and possible back-out procedures, of patches as defined by the manufacturer. Bug-Fix/Break fix for Managed Service: Included as needed and covered by incident management

Backup Management	For BAU/existing systems as part of Managed Service where Data Intensity is managing Customer data backups schedules and data restoration activities, schedules, and Recovery Time Objective ("RTO")/Recovery Point Objective ("RPO") levels (see Exhibit C), will be reviewed to ensure compliance with the Customers backup/retention policies and compliance. These will be captured, reviewed, and documented as part of the AIS process (as defined herein) for the Customer's backup schedule and retention requirements. For Data Intensity managed backups, failures will be managed via incident management services. Backups will be routinely validated on a twice yearly basis or after any changes that may have impacted the backup routines.
Capacity Management	Where Data Intensity is providing monitoring services of the end-to-end service, Data Intensity will analysis and determine whether to establish, implement, and monitor mutually agreed upon capacity thresholds for CPU, memory, disk and network connectivity and report on these monthly. Should Data Intensity become aware of any actual or suspected occurrences of breach, Data Intensity will promptly notify Customer, and identify and forecast possible issues by analyzing the changes going into a service. One of the prime objectives of capacity management is monitoring components to ensure that sufficient capacity is on hand to perform the respective functions to the Customer's BAU/existing systems optimally (for future planning of capacity, trends, or projections, which is not included in Managed Service support, see Table D).
Access Management	Manage access to environments for role-based access definitions ***for Data Intensity users***, password management rules, and recovery utilities.

Performance Management	Analyze performance-related incidents for in-scope DSP, CCMSP, TASP, OSSP supported environments, instances, and/or subscriptions as selected, and detailed, in Table A and Exhibit C. Manage configurations within Data Intensity's control to maximize performance of production environments. Performance baselines will be determined by the Customer through performance testing, and the baselines established from the evidence based repeatable testing will be shared, and mutually agreed to, between the parties (each party acting reasonably and in good faith) such that performance management can be measured. Data Intensity will capture an overall system performance baseline for the in-scope DSP, CCMSP, TASP, OSSP supported environments, instances, and/or subscriptions herein in order to determine and monitor deterioration of performance against the established baseline and apply preventative measures (for Performance tuning of code, which is not included in Managed Service support, see Table D). In the event the Customer reports a performance issue and custom code is being executed, the Customer must be able to demonstrate that the same custom code remains performant and functional in a comparable environment. Data Intensity will investigate the technical aspects of the issue within the scope of the Managed Service. If issue is caused by Customer's code, then Data Intensity is: a) absolved of any liability, b) SLAs revert to reasonable efforts; and c) if Data Intensity is called upon to remediate Customer's Code issue, that task is out of scope and separately chargeable at Data Intensity then current rates. Where Archive environment support has been selected, the following applies: In a standard transactional production system, Databases are optimized for continual and regular usage, through caches and indexes to ensure efficient and effective performance. However, in an archive environment, the usage is infrequent, and the reporting is ad hoc, therefore bypassing the standard optimization routes as used in a standard transactional production system. The Customer is aware and acknowledges that the performance of an archive environment will not be comparable to the performance of a standard transactional production environment. Any performance tuning work requested on an Archive environment will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.
Problem Management	Analyze, and classify as problems, recurring incidents that result in outages or service interruptions within Customer's in-scope DSP CCMSP, TASP, OSSP supported environments, instances, and/or subscriptions herein. Work with Customer to define and implement mutually agreed upon solutions and/or work-arounds to mitigate problems and report on RCA.

Monitoring	In accordance with the Assumptions listed herein, Data Intensity shall install and configure tools that enable monitoring, administration and management capabilities, initiate incidents based on monitored threshold breaches to serve the needs of ensuring that incidents can be identified and dealt with reactively and proactively. Assumptions for Data Intensity's monitoring service are as follows: • Monitoring is offered on the basis that all monitoring tools / utilities are Data Intensity tools and will be installed on Data Intensity infrastructure. • Customer shall provide service accounts with appropriate access to all in scope systems to ensure full monitoring capabilities. • If Customer configuration prevents implementation or successful operation of monitoring environment, it may be necessary for the Customer to provide infrastructure to host the monitoring solution. • Data Intensity will not be held responsible for SLA, or system failures, until the monitoring solution is in place and accepted into service.
Configuration Management	Establish baseline configuration state, maintain version information, validate, and document all requested configuration changes.
Continuous Service Improvement Process ("CSIP")	CSIP is an incremental service development process, which stimulates bottom-up improvement idea creation and self-directed implementation in a transparent and engaging way. This governance and communication process is included with Managed Services (for any recommendations that come out of the CSIP process/any mutually agreed upon actions to be taken, which is not included in Managed Service support, see Table D.
Service Management	Data Intensity's IT Service Management Platform is provided via a Service Now portal and will serve as the system of record for operational SLA reporting and ticket management governing all Data Intensity delivered services.
Availability Management	With the exception of CCMSP, availability management looks at services from an overall uptime perspective. A SLA measure is provided on a per application basis within each encompassing in-scope DSP, TASP, OSSP supported environments, instances, and/or subscriptions herein. This is offered on Critical (production) Environment (as defined herein, Section H), or Disaster Recovery ("DR") environments (if selected/included herein), that meet Data Intensity's requirements. SLA(s) surrounding CCMSP, if applicable, are between the Customer and the public cloud vendor.
Service Level Agreement ("SLA")	A service-level agreement ("SLA") is a formal commitment between Data Intensity and the Customer where particular aspects of the service – quality, availability, responsibilities – are offered and mutually agreed between the parties.
Service Level Objective ("SLO")	A service-level objective ("SLO") is a key element of a service-level agreement (SLA) between Data Intensity and the Customer. SLOs are agreed upon as a means of measuring the performance of Data Intensity and are outlined as a way of avoiding disputes between the two parties based on misunderstanding.

***All Entitlements as detailed in Table B will be reported and tracked through Data Intensity's Service Now ticketing system and are included in the Monthly Recurring Fee ("MRF") as detailed within Exhibit A.**

C: ADD-ON ENTITLEMENTS

The following Managed Services are available to add to the Customers Baseline Managed Services Package (Table B), based on each individual Customers' needs, if selected below. The Customer may select to have the following selected Managed Services included within their MRF or billed against their established Client Request Account ("CRA") hours/overage rate as detailed within Exhibit A.

Unless selected at the time of initial order/execution, the following Managed Services are considered out of scope of this Exhibit B. The addition of any of any the following items, after placement of the initial Order/execution, may require a Request For Change ("RFC")/Change Order Request ("COR") in accordance with the terms herein.

***Table C (for in-scope DSP, TMSP, CCFOMSP, TASP, OSSP; see Table A and Exhibit C):**

Select to Include	Service Capability	Included in MRF	Bill against CRA	Details
☐	Vulnerability Monitoring	☐	☐	If selected enter detail
☐	Service LINQ	☐	☐	If selected enter detail
☐	Supply and Management of a Trusted Code Signing Certificate (CSC)	☐	N/A	The supply of certificate management service whereas; Data Intensity will procure and install a trusted CSC once per annum throughout the term of the applicable Exhibit A. Thereafter, Data Intensity will manage the expiration of each CSC and notify the Customer a month in advance of any such upcoming CSC expiration. If the certificate management is not renewed, a new certificate will not be procured or installed as of the expiration date. Customer may acquire their own CSC to replace the Data Intensity supplied CSC at any time throughout the term of the Exhibit A. Any such replacement requests shall be performed by Data Intensity and will be billed against the established CRA hours and/or the overage rate as detailed within Exhibit A. Please note, this is strictly for the management of the CSC and requires that the Customer's application and architecture is already configured to use such certificates. Any requests to reconfigure the Customer's application(s) will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

☐	Supply and management of a Trusted Transport Layer Certificate (TLS/SSL)	☐	N/A	The supply of certificate management service whereas; Data Intensity will procure and install a trusted TLS/SSL certificate once per annum throughout the term of the applicable Exhibit A. Thereafter, Data Intensity will manage the expiration of each TLS/SSL certificate and notify the Customer a month in advance of any such upcoming TLS/SSL certificate expiration. If the certificate management is not renewed, a new certificate will not be procured or installed as of the expiration date. Customer may acquire their own TLS/SSL certificate to replace the Data Intensity supplied TLS/SSL certificate at any time throughout the term of the Exhibit A. Any such replacement requests shall be performed by Data Intensity and will be billed against the established CRA hours and/or the overage rate as detailed within Exhibit A. Please note, this is strictly for the management of the TLS/SSL certificate and requires that the Customer's application and architecture is already configured to use such certificates. Any requests to reconfigure the Customer's application(s) will be billed against the established CRA hours and/or the overage rate as detailed within Exhibit A.
☐	Geographic Resource Restriction	☐	☐	If selected enter detail

☐	Use of Customer's Monitoring Tools	☐	☐	**Where Data Intensity *is providing* monitoring services, utilizing the *Customer's* monitoring tools**, Data Intensity will work with the Customer to integrate monitoring events into the Data Intensity ITSM ticketing system.
				• Where Customers monitoring tools are utilized;
				  ○ No usage or integration is included for Customer monitoring tools.
				  ○ The Customer is responsible for monitoring connectivity, functionality, and performance of the tools;
				  ○ The Customer is required to inform Data Intensity prior to any changes or blackouts on their monitoring tools;
				  ○ Data Intensity will not be held responsible for SLA(s) or system failures, due to: i) gaps or failures in Customers monitoring; or ii) Customer rejection, or delay in implementation, of any metric or threshold modification requested by Data Intensity throughout the Term.
				  ▪ Notwithstanding anything contrary herein, in the event that Data Intensity receives an increase in the number of alerts/events due to changes, lack of changes, or failures, resulting from the Customer monitoring tools, additional charges may be applicable and will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

☐	Additional Patch Service:	☐	☐	Additional patch management (i.e. ad hoc). If selected enter detail
☐	Mutually agreed upon SLA modification	☐	☐	Select from below the Section from herein that mutually agreed upon SLA modification is applicable to: ☐ Section H ☐ Section I ☐ Section J ☐ Section K Enter detailed explanation of mutually agreed upon applicable SLA modification
☒	Additional Customer Specific Entitlements not otherwise listed in this Table C	☒	☐	Specific to SKU: RMS-ENT-ORCL-DBCLONETASK Data Intensity will provide (1) DB clone per business day, not to exceed (20) per calendar month which will include, customer specific automation development and provisioning of infrastructure resources and post-clone steps to ensure accuracy. Automation development activities will include up to (3) iterations of post clone development changes to refine the automation process. The fixed price is for the daily clone refresh, from PROD (LKCOEBSPRD) to the following target environment(s) (LKCOEBSDLY), any clones outside of these are out of scope of this fixed price cloning. Execution of additional cloning will be charged separately. In the event of a failed clone, DI will work to rectify the failed clone and will not count against the customer's daily/monthly count limit unless a mutually agreed upon root cause analysis reveals that customer-created change caused the failure. In the event that the customer exceeds the limits set forth, each additional clone will be charged on a flat-fee basis set forth in the pricing table located in Exhibit A, section 1.1.1.
☒	CRA; for services in accordance with Section E herein	☒	N/A	Billed monthly in advance: Thirty (30) hours
☒	Disaster Recovery Management	☒	☐	If selected, Data Intensity shall: • Monitor network connectivity between the primary and DR sites within the in-scope supported capabilities; • Work with the Customer network team to remediate any network connectivity issue between the primary and DR sites within the in-scope supported capabilities; and • Assist as needed, with any planned or unplanned failover to the DR site within the in-scope supported capabilities. The Customer is responsible for the DR process. Data Intensity is a resource within the DR process providing the management of the DR architecture and configuration. Selection of this Add-on Entitlement would provide support for one (1) DR test per annum. Any additional DR tests requested will be charged against the

				established CRA hours and/or the overage rate as detailed and applicable within Exhibit A. DR Management service is in support of the RTO and RPO objectives (see Exhibit C), as tested and proven prior to AIS (as defined herein, Section G). Please note: In order to for DR Management to be successful, the capacity of the DR infrastructure is required to equal the size of the production environment for which the DR infrastructure is expected to provide coverage at the time of enacting. In the event that the DR is not equal to the coinciding production environment, any resizing needed will be included in the RTO target. Data Intensity will not be liable for non-performance due to lack of capacity. Any Services resulting from any such incidents will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A. Data Intensity may raise a request to invoke DR as an action to resolve an Infrastructure, Application Availability, or Incident Management SLA. The Customer will approve / reject any such request by Data Intensity within fifteen (15) minutes of any such request. If the Customer rejects any reasonable Data Intensity DR request or fails to respond within fifteen (15) minutes, then the SLA resolution and SLA availability clocks will be stopped. One (1) DR test will be mandatory at the point of AIS (as defined herein, Section G) and once per annum thereafter. In the event that the DR test fails, any DR enactment or support will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A. Any additional DR tests will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A. In-scope DR testing is non-destructive. Destructive DR testing is not included as in-scope and, if requested, will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A or may require a new Order. In the event of DR being invoked as a result of a primary site non-recoverable failure (e.g. critical failure in an availability zone, where the restoration from backups is not possible, and some or all of the DR capability has been lost), re-instatement/rebuild of the DR capability will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A or may require a new Order, where any hardware or software installation or reconfiguration is required. A prerequisite of AIS (as defined herein, Section G), of

				DR support, is that a runbook for DR including detail command level, step by step detail, with screen shots that detail how the failover and failback of a DR environment should occur, be available. The runbook will also be used for the execution of a DR test. If a runbook is not available, or it used and found to be incomplete, inconsistent, or incorrect, any resulting build or rework will be charged against the CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

***All Customer specific Entitlements selected and/or requested from within Table C will be initiated, reported, tracked, and closed through Data Intensity's Service Now ticketing system and will be billed by Data Intensity, as selected above, either as part of the MRF or against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.**

D: OUT OF SCOPE

Unless otherwise selected as Add-on Entitlements in Table C above, the following services are considered out of scope, and are not provided, as Entitlements under this Exhibit B. Customer requested out of scope services, for Customer in-scope supported capabilities, and in-scope environments, as selected, and detailed, in Table A and Exhibit C, will be billed by Data Intensity against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A. Should the Customer request any of any the following services to capabilities or environments not selected and detailed within Table A and Exhibit C, a new Order will be required.

Table D:

Service Capability	Technology Management
Change Management	All non-incident related Customer generated change (e.g., a change request to resolve an incident, would not be charged separately (as an example, If Data Intensity needs to apply a patch to resolve a DB incident, or if a patch is requested to correct an EBS functional issue, this would be charged separately. Based on the existing scope, anything new (i.e., outside of the current model) would be considered a project or coverage).
Service Request Management (for out of scope services)	All Customer generated service requests for out of scope services/outside of the Customers Baseline Managed Service Package.
Patch Management	All Customer driven patching and related pre patch analysis ("PPA")
Additional / Non Scheduled Backup or Restore activities	All Customer requested non-incident related restores or ad hoc backups where Data Intensity is providing managed backup services for the Customer.
Capacity Planning	The analysis of the Customers projected growth/contraction and real capacity data to identify trends and projections where individual components will exceed their operating tolerances/capacities, therefore requiring further tuning techniques or additional components
Access Management	Manage access to environments for role-based access definitions ***for any non-Data Intensity users***, password management rules and recovery utilities
Security and Compliance Management	The supply of services to provide Security and Compliance management includes: • Vulnerability testing support • Penetration testing support
Performance Tuning	The support and investigation of code performance related issues
CSIP Action Items	Mutually agreed upon actions to be taken, from recommendations resulting from the CSIP process

Exit Management	Exit Management is a bespoke process to fit each Customer's needs. In the event that a transition away from Data Intensity's Managed Service is required, Data Intensity is able to offer this exit management governance process. This facilitates a smooth, effective transition of services, with minimum disruption of ongoing delivery, and efficient completion of all mutually agreed upon obligations. Data Intensity is able to provide documentation of general applicability, detailing the Customer's systems,11 configurations, infrastructure and backup locations where applicable services are being delivered by Data Intensity.
Oracle GoldenGate ("GG") Incident Management	Incidents as detailed above are included within the TOM services (see Table B). Notwithstanding the foregoing, and for further clarification and the avoidance of doubt, the following types of incidents are considered out of scope of the entitlements under the TOM services herein: a. Where an incident: i. Has occurred previously and has been previously reported to the Customer, along with a recommended course of action to resolve the incident, but the Customer had declined proceeding with the recommended resolution, Customer will be notified, and Customer acknowledges and agrees that, as applicable and at Data Intensity's sole discretion, it will be billed for all work to resolve these such incidents against the established CRA hours and/or the overage rate, as detailed and applicable within Exhibit A, until the recommended course of action has been completed. ii. Has been identified as the Customer, or a Customers third-party's, action or inaction as the cause of the incident, Customer will be notified, and Customer acknowledges and agrees that, as applicable and at Data Intensity's sole discretion, it will be billed for all work to resolve these such incidents against the established CRA hours and/or the overage rate, as detailed and applicable within Exhibit A. iii. Has not been seen before, but a recommended course of action to prevent such incidents was made to the Customer, which the Customer declined proceeding with such recommended preventative action, Customer will be notified, and Customer acknowledges and agrees that, as applicable and at Data Intensity's sole discretion, it will be billed for all work to resolve these such incidents against the established CRA hours and/or the overage rate, as detailed and applicable within Exhibit A, until the recommended course of action has been completed. iv. Is related to an existing, known, issue that was identified from the AIS process, Customer will be notified, and Customer acknowledges and agrees that, as applicable and at Data Intensity's sole discretion, it will be billed for all work to resolve these such incidents against the established CRA hours and/or the overage rate, as detailed and applicable within Exhibit A, until the recommended course of action has been completed. b. Specific to Oracle GoldenGate incidents: i. Support of any GG Data Conflict Errors is not included within the scope of this Exhibit B. Any impact on Replicats failing due to GG Data Conflict Errors resulting in, but not limited to, Data Intensity having to restart Replicats, is the responsibility of the Customer and will require the Customer to address the design errors directly with the responsible third-party. Customer acknowledges and agrees that it will be billed by Data Intensity against the established CRA hours and/or the overage rate, as detailed and applicable within Exhibit A, for any efforts by Data Intensity resulting from such impacts. ii. Resolution of GG Abend errors, arising due to infrastructure, configuration, or recent changes of Customer and/or third-party, are outside the control of Data Intensity and therefore are not included within the scope of this Exhibit B. Whilst DI will investigate and restart the process where any GG Abend errors occur, the Customer will be notified, and Customer acknowledges and agrees that, as applicable and at Data Intensity's sole discretion, it will be billed for all work to resolve the Abend error against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

E: CUSTOMER REQUEST ACCOUNT ("CRA"): OUT OF SCOPE SERVICES

The CRA is a pre-purchased number of minimum monthly support hours at a global rate, for use by the Customer toward out of scope Managed Services for Customer in-scope supported capabilities, and in-scope environments, as selected and detailed, in Table A and Exhibit C, or against project-based services including but not limited to the below. For further clarity and the avoidance of doubt, the monthly number of CRA hours shall expire at the end of each month and cannot be carried over or borrowed against.

- Installations and Upgrades
- Analysis & Tuning
- Security & Object Administration
- Ad-hoc Cloning

Standard Inclusions and Caveats:

- Customer approves CRA spend through initiation of request for services;
- CRA is billed in minimum increments of 30-minute;
- Standard service request SLA's will apply to all CRA work (e.g. Ad hoc backup/restore requests); and
- Project based CRA tasks will require a minimum of two weeks' notice.
- Upon Customer's request, the Customer and Data Intensity agree to review the number of pre-paid CRA hours each quarter to determine whether additional hours should be added going forward.

Overages:

Any work requested a) which exceeds the Customer's allotted CRA hours; or b) for services exceeding entitlements, or for In-Scope project-based work, but for which there is no CRA in place, will be billed against the established overage rate as detailed and applicable within Exhibit A. The addition, or increase, of CRA hours after placement of the initial Order/execution, may require a RFC or COR in accordance with the terms herein. Any Customer support requests for Capabilities outside of those listed within Table A, and/or environments not included within Exhibit C, will be addressed through a separate Exhibit B.

F. STANDARD OPERATING HOURS

Multiple Geographic location or time zone:

Table F:

Standard Hours of operation	Hours	Days
Follow the sun	24 hours	7 days

G. Service Transition

Customer Onboarding Process

This Section G applies to new and/or changed environments transitioning into Data Intensity's TOM support.

Data Intensity's Customer On-Boarding Process is designed to ensure precision and speed relative to integrating the Customer's people, processes and tools into Data Intensity's Service Management Platform and integrate support operations between Customer and Data Intensity. Onboarding will require the Customer to provide designated contacts to provide system access, networking support, vendor support agreement information and monitoring support.

Unless otherwise stated herein, all new and/or changed environments transitioning into Data Intensity's Managed Service shall meet Data Intensity's Acceptance into Service ("AIS") criteria as follows:

- No open (P1, P2) incidents
- No existing problem records
- No recurring incidents (last 12 months) that have not been resolved
- Sufficient capacity to run operations for a minimum of 12 months
- Are at the latest patch levels
- Where DR is selected, a runbook must be present and to the standards defined in table C

Environments not meeting Data Intensity's above AIS requirements will be documented and excluded from in-scope supported environments, and from SLA calculations, under this Exhibit B. These excluded environments will require Data Intensity Remediation and Standardization ("RaS") Services which are designed to improve/uplift the in-scope supported environments, current Patching, and Maintenance & Configuration levels to meet Data Intensity's AIS requirements herein. Any such work required, on out of scope environments, will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A, until resolved.

In addition to the above requirements, where archive environment support has been selected, the following also applies:

For an environment to be suitable for archive support the following must be met:

- The environment is used for the sole purpose to preserve data
- The environment will have no transactions in the system;
- The environment cannot have data growth (beyond logging of user activity);
- The environment cannot be a configured target of replication;
- The environment cannot have changes implemented outside of agreed patching; and
- The environment cannot be used as any part of a DR or Business Continuity solution.

Archive environments not meeting Data Intensity's above requirements will be documented and excluded from archive supported environments under this Exhibit B. Any such excluded environments will be categorized as standard support environments, under either Critical/Non-Critical and S, M, L sizing, and will require a Change Order.

Customer acknowledges and hereby agrees that there will be a thirty (30) day stabilization period during which Data Intensity will work with Customer to document their system and implement the appropriate monitoring tools to meet the SLA. This stabilization period is necessary to ensure that the monitoring tools are performing appropriately and that the thresholds and e-mail notifications are working properly. Data Intensity and Customer will both certify the conclusion of the stabilization period. From this point, Data Intensity will be responsible for meeting the proposed SLA. Any changes to the Customer Environment will necessitate a commensurate stabilization period for the additional systems.

H: INCIDENT SERVICE

Critical Environment Incident Level Definitions:

Critical Environment: Environments that are essential to the survival of the Customer's business with a very low tolerance for unplanned down-time.

Table H-1:

Priority	Service Level Criteria	*Incident Response Time	SLA
1	Whole or critical part of system or service unavailable or unusable, or causing major impact, loss of revenue or damage to reputation.	15 Min	95%
2	Important, but not immediately critical part of the system or service unavailable or unusable or causes significant business impact.	1 Hour	95%
3	Service failure has a low business/financial impact and/or impacts an isolated number of users.	4 Hours	95%
4	Non-urgent issues and/or issues with acceptable workarounds immediately available.	8 Hours	95%

Incident Resolution Level Definitions

The following is only offered for Critical (production) Environment (as detailed herein), or Critical DR environments (if applicable), that meet Data Intensity's requirements:

Table H-2:

Priority	Service Level Criteria	Incident Resolution Time	SLO
1	Whole or critical part of system or service unavailable or unusable, or causing major impact, loss of revenue or damage to reputation.	8 Hours	95%
2	Important, but not immediately critical part of the system or service unavailable or unusable or causes significant business impact.	16 Hours	90%
3	Service failure has a low business/financial impact and/or impacts an isolated number of users.	24 Hours	85%
4	Non-urgent issues and/or issues with acceptable workarounds immediately available.	48 Hours	80%

Non-Critical Environment Incident Level Definitions:
Non-Critical Environment – Environments that are not mission critical but still require service for operational stability.

Table H-3:

Priority	Service Level Criteria	*Incident Response Time	SLO
1	Whole or critical part of system or service unavailable or unusable, or causing major impact, loss of revenue or damage to reputation.	30 Min	90%
2	Important, but not immediately critical part of the system or service unavailable or unusable or causes some business impact.	2 Hour	90%
3	Service failure has a low business/financial impact and/or impacts an isolated number of users.	6 Hours	90%
4	Non-urgent issues and/or issues with acceptable workarounds immediately available.	10 Hours	90%

Archive Environment Incident Level Definitions:
Archive Environment – Environments that are not mission critical but still require service for operational stability.

Table H-4:

Priority	Service Level Criteria	*Incident Response Time	SLO
1	Whole or critical part of system or service unavailable or unusable, or causing major impact, loss of revenue or damage to reputation.	4 Hours	90%
2	Important, but not immediately critical part of the system or service unavailable or unusable or causes some business impact.	8 Hours	90%
3	Service failure has a low business/financial impact and/or impacts an isolated number of users.	12 Hours	90%
4	Non-urgent issues and/or issues with acceptable workarounds immediately available.	18 Hours	90%

Incident Closure Process
The Customer will confirm the resolution of the incident. This can be done by a phone call with the Service Desk, a reply to an automatic notification from the ticketing application or via a web- based application within forty-eight (48) hours of incident having been resolved. This is the second important step in Data Intensity's two-step incident closure. After the Customer confirmation, an incident record can safely be put into "Closed" status. The Customer will be notified upon closure. If for any reason Customer confirmation is not received within the forty-eight (48) hour period of the incident having been resolved, the incident shall automatically be closed within Data Intensity's ITSM tool.

Standard Inclusions and Caveats:
Incident Response:

- *Incident response time is defined as the time from incident notification to the assignment of the incident to a Data Intensity engineer through Data Intensity's ITSM tool.
- Where Customers monitoring tools are utilized;
    - The Customer is responsible for monitoring connectivity, functionality, and performance of the tools;
    - The Customer is required to inform Data Intensity prior to any changes or blackouts on their monitoring tools;
    - Data Intensity will not be held responsible for SLA(s) or system failures, due to: i) gaps or failures in Customers monitoring; or ii) Customer rejection, or delay in implementation, of any metric or threshold modification requested by Data Intensity throughout the Term.
- Notwithstanding anything contrary herein, in the event that Data Intensity receives an increase in the number of alerts/events due to changes, lack of changes, or failures, resulting from the Customer monitoring tools, additional charges may be applicable and will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

Incident Resolution:
Incident resolution is defined as the time from the assignment of the incident to a Data Intensity engineer to the restoration of service, in accordance with the terms and caveats herein.

The following may be subject to factors outside of Data Intensity's control and the following exceptions will result in the resolution time clock being stopped while the exception is being dealt with:

- Notwithstanding anything herein, any outage, the cause of which is outside the control of Data Intensity, will result in the immediate suspension of any affected Service Level Agreements. Moreover, upon Customer request, Data Intensity will make commercially reasonable efforts to assist the Customer to mitigate the effects of the outage at the then current, but separately chargeable rates;
- Where the incident has not been resolved, but the service has been restored, this will achieve the resolution SLO;
- In the event that the incident causing the outage was caused by the Customer action or non-scheduled change;
- Environment downtime due to Customer-initiated changes whether implemented by the Customer or the Supplier on behalf of the Customer (provided that the Supplier notified the Customer of the impact of such changes beforehand);
- Environment downtime caused as a result of unplanned and unannounced increase in capacity usage by the Customer;
- Environment downtime due to problems caused by Customer-supplied content or software (e.g., faulty third-party applications used by the Customer);
- Environment downtime due to Customer failure to adhere to the change management procedure;
- Where Data Intensity has made at least two (2) reasonable written requests, each for the same reason to the Customer, without reaching agreement for necessary planned works to proceed or implement a reasonable alternative solution, and an incident occurs due to this planned work not having been undertaken;
- Where connectivity to the internet is disrupted because of a routing issue outside of the network and is outside Data Intensity's control;
- Restoration for failures where the cause of the failure is due to the actions or omissions of a third party (excluding any Data Intensity subcontractors);
- If a restoration plan is agreed between the parties that has a restoration time in excess of the relevant restoration target;

- Where Change Access for a Managed Service component is requested by the Customer (and granted by Data Intensity), restoration time service levels for that environment shall not apply during the agreed window within which that Change Access is in place;
- Restoration time service levels shall not apply where an incident arises following, and due to, changes made by a third party (excluding any Data Intensity subcontractors) as a result of its Change Access. Services provided by Data Intensity that are required to resolve such incidents shall be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A; and
- Monitoring is offered on the basis that all monitoring tools/utilities are Data Intensity tools however, where Customers monitoring tools are utilized:
    - The Customer is responsible for monitoring connectivity, functionality, and performance of the tools;
    - The Customer is required to inform Data Intensity prior to any changes or blackouts on their monitoring tools;
    - Data Intensity will not be held responsible for SLA(s) or system failures, due to: i) gaps or failures in Customers monitoring; or ii) Customer rejection, or delay in implementation, of any metric or threshold modification requested by Data Intensity throughout the Term.
  - Notwithstanding anything contrary herein, in the event that Data Intensity receives an increase in the number of alerts/events due to changes, lack of changes, or failures, resulting from the Customer monitoring tools, additional charges may be applicable and will be billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A

I. Change Service

Incident generated change is included within the MRF for the Managed Services provided for under Table B. All other changes not included as Entitlements will be executed and billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

Change Request Policy:
A change request requires authorization by the Customer's Change Advisory Board ("CAB") – A change request might involve a significant change to the service of infrastructure. A RFC may be submitted by the Customer or Data Intensity. RFC(s) are required and must be approved by both parties prior to being implemented.

All changes will be executed within a reasonable time frame, and all contracted SLA's will be suspended for the duration to implement the applicable change.

There are three types of changes (as detailed in Table I), two of which require approval:

Category	**Approval**
Emergency/Critical	ECAB
Normal	CAB
Standard	Preapproved

All times that follow are within Data Intensity's operating hours only. Any requested activity outside of these hours is considered out of scope of this Exhibit B and would be processed from the start of the next business day, or as a separately chargeable item, billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

Change Categorizing:

Table I:

Categorization	Description	Response Time	Minimum Lead Time	SLO
Emergency	An accelerated authorization and planning procedure must be performed in the case of an Emergency Change, where CRITICAL system(s) are currently experiencing significant impact or impending impact. The emergency change order board ("ECAB") is responsible for the authorization and scheduling of this kind of change.	4 hrs	N/A	90%
Normal – Major	A High Risk – High Impact change. This type of change is deemed to impose major risk to the business, and a major impact should issues be encountered. A normal major change requires collaborative efforts to scope, tests, and resource, and therefore requires a longer minimum lead time to fulfil.	8 hrs	14 days	90%
Normal – Significant	Medium Risk – Medium Impact. This type of change is deemed to impose significant risk to the business, and a significant impact should issues be encountered. A normal Significant change requires efforts to scope, tests, and resource.	8 hrs	7 days	90%
Normal – Minor	Low Risk – Low Impact This type of change is deemed to impose Minor risk to the business, and a Minor impact should issues be encountered. A normal Minor change is well understood and relatively easy to test and resource	8 hrs	3 days	90%
Standard	A Standard change is a pre-approved change, with an accepted and tested procedure, and deemed to be a low risk. These will be requested via the Service Request process	8 hrs	3 days	90%

Standard Inclusions and Caveats:

- Change response is defined as the time from change request submission to the assignment of the change request to an engineer within Data Intensity's ITSM tool.
- If a change fails to meet the definition of Emergency, as defined above (Table I), however, and Customer requires that such change is treated as an Emergency, Data Intensity shall either: a) discuss re-prioritization with Customer; or if unsuccessful b) charge a premium (double the established CRA and/or overage rate within Exhibit A as applicable) to treat the change as an Emergency, with appropriate SLO targets.
- The timeline for execution/commencement of a change will be dependent on the availability of a window from the Customer, whether approval is received, and whether sufficient planning can be completed. In this event, where the resultant commencement time is in excess of the SLO, the SLO does not apply.

J. Service Request

Service requests are by default not included as in-scope under this Exhibit B however, where their frequency and effort can be estimated, then specific service requests can be included as in-scope.

All other requests, unless otherwise stated herein, are not included as in-scope under this Exhibit B, are not included as Entitlements, and will be executed and billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A.

Service Request Policy:
A service request is a request to change or execute an operational task. RFC(s) are not required to implement service requests.

Service Request Change for a Standard Change:
Service requests for Standard Change typically have the following characteristics:

1. Approval is automatically granted by the Customer;
2. The requested tasks are well known, documented, and proven;
3. Authority is effectively given in advance for the change;
4. The request is included as part of the BAU service offering; and
5. The risk is unusually low and well understood.

Service Request Definitions
All times that follow are within operating hours only, any requested activity outside of these hours is not included and would be processed from the start of the next business day, or as a separately chargeable item.

Table J:

Categorization	Description	Response Time	Minimum Lead Time	SLO
Standard	A Standard change is a pre-approved change, with an accepted and tested procedure, and deemed to be a low risk.	8 hrs	3 days	90%

Standard Inclusions and Caveats:

- Service request response time is defined as the time from service request submission to the assignment of the service request to an engineer in Data Intensity's ITSM tool.
- Data Intensity shall charge a premium (double the established CRA and/or overage rate within Exhibit A as applicable) if Customer requires, and Data Intensity agrees, to a service request being completed in advance of the established minimum lead time

K. Availability SLA

In accordance with the terms herein, availability management looks at services from an overall uptime perspective. Data Intensity are able to offer availability measures on a per application/environment basis within the encompassing environment.

Availability is calculated based on the operating hours and the level of availability offered.

Availability % = (Operating Hours – Unplanned downtime) / Operating hours x 100

Table K:

Environment Type	SLA
Critical	99.9%
Non-Critical	N/A

Availability SLA's are offered on: a) only Critical (production) Environments and Critical DR environments; and b) where the environments meet Data Intensity's AIS minimum levels for patching, maintenance, and configuration.

Where an environment does not meet these levels/expectations, then this will require Data Intensity Remediation and Standardization ("RaS") Services. RaS services are designed to improve/uplift the environments current patching, maintenance, and configuration levels to meet Data Intensity's minimum AIS requirements and are billed against the established CRA hours and/or the overage rate as detailed and applicable within Exhibit A, as the work is performed.

Standard inclusions and caveats:

- Critical production/Critical DR environments only, based on high availability architecture and DR to be setup as Active/Active.
- Application availability is calculated by measuring the total number of hours the application was up and running and are subject to "limitations outside of Data Intensity's control" – see below; dividing by the total actual hours in a given month.
- Planned downtime is any predetermined downtime during which the applications may be unavailable and, as mutually agreed between Data Intensity and Customer via standard Customer change management procedures, for the purpose of upgrades, maintenance, or for any other mutually agreed upon reason or purpose.

Illustrative Limitations outside of Data Intensity control include

- A failure or degradation of performance or malfunction resulting from scripts, data, applications, equipment, infrastructure, software, penetration testing, performance testing, or monitoring agents directed or provided or performed by Customer, or third party of Customer, provided it was the Customer/third party provided code that caused such outage;
- Planned outages/downtime, scheduled, and announced maintenance or maintenance windows, or outages initiated by Data Intensity at the request or direction of Customer for maintenance, activation of configurations, backups or other purposes that require the service to be temporarily taken offline;
- Unavailability of Customer management, auxiliary or administration services, including administration tools, reporting services, utilities, third party software components or services not within the sole control of Data Intensity, or other services supporting core transaction processing;
- Outages occurring as a result of any actions or omissions taken by Data Intensity at the request or direction of Customer;
- Outages resulting from Customer equipment, or third-party equipment or software components, not within the sole control of Data Intensity;
- Events resulting from an interruption or shut down of the services due to circumstances reasonably believed by Data Intensity to be a significant threat to the normal operation of the services, the operating infrastructure, the facility from which the services are provided, access to, or the integrity of Customer data (e.g., a hacker or malware attack). Customer will be notified in accordance with the P1 incident response time (see Table H1);
- Outages due to system administration, commands, or file transfers performed by or on behalf of Customer or its representatives;

- Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties, and other force majeure events;
- Outages, or other inability to access the services, due to Customer's conduct, including negligence or breach of Customer, material obligations under the agreement, or by other circumstances outside of Data Intensity's control;
- Lack of availability, or untimely response time, of Customer to respond to incidents that require Customer participation for source identification and/or resolution, including meeting Customer responsibilities for any services;
- Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to Customer conduct or circumstances outside of Data Intensity's control;
- Hardware/Cloud failures that are not attributed to Data Intensity's management of the environments; and
- Performance problems that are impacted by the Customer, or third party, changing the system, either load or functionality changes, without prior notification to Data Intensity, therefore not allowing Data Intensity to proactively respond to the requested change.
- SLA(s) surrounding CCMSP, if applicable, are between the Customer and the public cloud vendor.
- Notwithstanding anything contrary herein, any outage, the cause of which is outside the control of Data Intensity, will result in the immediate suspension of any affected Service Level Agreements. Moreover, upon Customer request, Data Intensity, recognizing the exigent circumstances, will make commercially reasonable efforts to assist the Customer to mitigate the effects of the outage at the then current, but separately chargeable rates and Customer agrees to pay for all services provided. Customer's request for any such services shall be understood as official authorization to invoice in place of a Customer Purchase Order.

L. Acceptance of Order

CUSTOMER ACKNOWLEDGES IT HAS FULLY AND COMPLETELY READ THIS EXHIBIT B, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS. FURTHER, CUSTOMER AGREES THAT THIS EXHIBIT B, ALONG WITH THE MSA AND EXHIBITS A AND C (COLLECTIVELY REFERRED TO HEREIN AS THE "AGREEMENT"), SIGNED BY BOTH PARTIES, CONSTITUTES THE ENTIRE AGREEMENT BETWEEN THE PARTIES WITH RESPECT TO THE SUBJECT MATTER HEREOF, AND SUPERSEDE ANY AND ALL OTHER AGREEMENTS, UNDERSTANDINGS, AND UNDERTAKINGS, WHETHER WRITTEN OR ORAL, BETWEEN THE PARTIES IN RELATION TO THIS SUBJECT MATTER. IN THE EVENT OF A CONFLICT BETWEEN THE PROVISIONS OF THIS EXHIBIT B, AND THE AGREEMENT, THE DOCUMENTS WHICH COMPRISE THE AGREEMENT SHALL GOVERN IN THE FOLLOWING DECREASING ORDER OF PRECEDENCE: A) EXHIBIT A; B) EXHIBIT B; C) EXHIBIT C; AND D) THE MSA.

CUSTOMER PURCHASE ORDER IS DUE AT TIME OF EXECUTION IN ORDER TO PROCEED HOWEVER, IN NO EVENT SHALL ANY PRE-PRINTED TERMS AND CONDITIONS OR OTHER PROVISIONS SET FORTH IN ANY ADDITIONAL DOCUMENTS, INCLUDING BUT NOT LIMITED TO A CUSTOMER'S PURCHASE ORDER, OR ANY RESTRICTIVE ENDORSEMENT ON ANY CHECK OR ANY INSTRUMENT OF PAYMENT, BE CONSTRUED TO MODIFY, AMEND OR ADD TO THE TERMS OF THE DOCUMENT, REGARDLESS OF ANY SUCH TERMS DATE OF ISSUE, NOW OR IN THE FUTURE, UNLESS SPECIFICALLY AGREED TO IN WRITING BY BOTH PARTIES. ANY SUCH ADDITIONAL TERMS SHALL BE VOID AND OF NO FORCE OR EFFECT.

EXECUTED AS AN INSTRUMENT UNDER SEAL AND AGREED TO AS OF April 1, 2026 ("EFFECTIVE DATE").

DLT SOLUTIONS	**LAKE COUNTY**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

January 26, 2026

Data Intensity Total Ops Management Services

Exhibit C
DLT Quote: 5398429

Notwithstanding anything contrary hereto, Customer agrees to use reasonable best efforts to "right size" their environment based upon the term of this Order Form. Data Intensity reserves the right to re-negotiate fees based upon any significant changes to the Customer Environment or changes to the assumption of capacity deployed.

For DSP:

List of environments that will be in support (Server, Database, Database Version, Database Type, and RTO/RPO (if applicable), Critical, Non-Critical or Archive as well as the S/M/L size definition for Critical and Non-Critical):

Instance name	Instance [redacted]
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

DSP GLOSSARY

Tech	Small	Medium	Large
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	
[redacted]		[redacted]	[redacted]

For TASP:

List of environments that will be in support (Server, Application, Application Node, Description, and RTO/RPO (if applicable), Critical, Non-Critical or Archive as well as the S/M/L size definition for Critical and Non-Critical):

Instance name	Instance type
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

TASP GLOSSARY

Tech	Small	Medium	Large
[redacted]	[redacted] [redacted] [redacted]	[redacted] [redacted] [redacted]	[redacted] [redacted] [redacted]
[redacted]	[redacted] [redacted]	[redacted] [redacted]	[redacted] [redacted]
[redacted]	[redacted] [redacted] [redacted]	[redacted] [redacted] [redacted]	[redacted] [redacted] [redacted]
[redacted]	[redacted] [redacted]	[redacted] [redacted]	[redacted] [redacted]
[redacted]	[redacted] [redacted]	[redacted] [redacted]	[redacted] [redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted] Managed servers 3 - 5

Number of Managed servers > 5

For TMSP:
List of the cloud platform that will be in support:

[redacted]

For OSSP:

List of environments that will be in support (Server, OS, OS Version, and RTO/RPO (if applicable), Critical, Non-Critical or Archive):

OCI Region	Environment	Server			
[redacted]					
us-phoenix-1	OMCS-SHARED	PHX-AD1-LKCO-WEBPROXY-PVTMT001	RUNNING	Oracle Linux	Oracle-Linux-7.8-2020.06.30-0