Service Description - HCL Commerce on HCL Now

This Service Description (“Service Description”) describes the HCL Commerce on HCL Now Service (“HCL Commerce on Now” or “HCL Commerce Now” or “Service”). Additional terms governing the HCL Commerce on HCL Now service are set forth in the HCL Master License Agreement (“MLA”) and the HCL Now Master License Agreement Addendum (the “Addendum”), available at https://www.hcltechsw.com/wps/portal/resources/master-agreements. This Service Description, any applicable Attachments, order(s) (“Order Schedule”), MLA and Addendum are the complete agreement regarding transactions under the Addendum (collectively, the "Agreement"). Any capitalized terms used but not defined in this Service Description shall have the meanings given to such terms in the Addendum or other applicable documents of the Agreement.

1 HCL Commerce on HCL Now

HCL Commerce on HCL Now is an e-commerce Hosting and Managed Service that enables digital selling for business-to-consumer (B2C), business-to-business (B2B), indirectly through channel partners, or all of these simultaneously. HCL manages the Application (APIs, search, database, network, storage and compute resources), applies fixes to the application, provisions and maintains the infrastructure and applicable security and privacy controls. The Service is designed to enable the customer (“Customer”) to implement Extensions to meet Customer's unique business requirements.

HCL Commerce on HCL Now consists of hosting of and associated managed services for the Customer’s licensed instance of HCL Commerce Software program and includes:

- HCL Now Infrastructure Service
- HCL Now Managed Service

1.1 HCL Commerce Software

A separate license entitlement for HCL Commerce Enterprise software is necessary for use of the HCL Now Service.

1.2 HCL Now Infrastructure Service

HCL Now Infrastructure Service is the hosting environment and infrastructure on which the Commerce application runs. The exact provisioning and configuration of the infrastructure will be determined by the HCL Now team. It consists of the following:

- (1) Production environments
- (1) Pre-Production (Staging) Environment
- (1) Development/Test Environment
- Content Delivery Network (CDN) and CDN Egress Traffic
- (2) Virtual Private Networks (VPNs)
- Environment Storage Backup and Restore
- (5) Monitoring Pages
- (1) Monitoring Transaction
- (10) Administrative Two-Factor Authentication Accounts
- Server Security Protection
- Data Storage
- Direct Traffic Egress
- Disaster Recovery

- Networking (Firewalls, Load Balancers)

1.3 HCL Now Managed Service

HCL Now Managed Service provides ongoing management and support of the software and hosting environment to ensure it is functional, reliable, secure and performant. It consists of the following:

- Service Level Agreement (SLA)
- Support Services
- Environment Setup
- Infrastructure and Application Health Monitoring
- Infrastructure Security monitoring and remediation
- Online Service Management Tooling
- Environment Upgrades
- HCL Software Product Upgrades
- Promotion of Customer Extensions to the Production Environment
- Business Continuity Planning and Execution for the HCL Now platform in the event of Disaster Recovery events

1.4 HCL Now Infrastructure Capacity

HCL Commerce on HCL Now can scale on-demand, however understanding peak loads in advance is important to ensuring the service can perform as desired during peak events. The Order Schedule will contain metrics for peak order lines per hour. If these metrics are exceeded, the performance of the Service may degrade and SLAs shall no longer apply.

In the event Customer exceeds the peak order lines per hour metric in two consecutive months, Customer agrees to review the purchase of additional infrastructure capacity and managed services with the HCL Now team.

1.5 HCL Now Infrastructure Usage Components

HCL Now Infrastructure includes components which are charged based on usage. The maximum amount of these components that a Customer can consume on a monthly or annual basis will be listed in the Order Schedule. Usage beyond the allowances will be invoiced based on HCL price or publicly available cloud service provider price list at that time.

The following items or events have allowances:

- CDN Egress Capacity – TB per Region
- Network Egress or Ingress – TB per Region
- Database Data Storage – TB per Region
- Asset Data Storage – TB per Region
- Environments
- Virtual Private Networks (VPNs)
- Custom Transaction or Page Monitors (HCL provided)
- Cloud Identity Access Management (CIAM) User Accounts (HCL provided)

2 Service Features – HCL Now Infrastructure

2.1 Environments

The Service provides the functional infrastructure for running the software for which HCL provides the support and necessary network, hardware and system patches. As part of the HCL Now Infrastructure part, HCL provides some or all of the following environments based on the Service as specified in the Order Schedule. Additional environments, or standalone environments are available upon request and for an additional charge.

2.1.1 Production Environment

The final resting point for all "Run" software in the Service lifecycle management. The production environment ("Production Environment") comprises the Application, systems, and supporting systems infrastructure, that the end users and the Customers of an organization access and use on an operational basis to execute its business processes and transactions. Administrative access to this system is restricted to HCL personnel or authorized users only after Customer Operational Acceptance ("COA").

2.1.2 Pre-Production Environment

Provides a limited production replica for deployment and Customer's acceptance testing of the configurations of the final Application with any Extensions ("Pre-Production Environment"). The Pre-Production Environment is maintained to production operational and compliance standards at all times but is not covered as part of the Service Level Agreement. Administrative access to this system is restricted to HCL personnel or authorized users only after COA. This is the primary location for Customer conducted user acceptance testing and the final performance evaluation/testing prior to going live in Production Environment. Additional Pre-Production Environments are available upon request and for an additional charge.

2.1.3 Development/Test Environment

Provides a single, functionally equivalent instance of Production and the supporting infrastructure used for development testing, quality assurance, and functional testing of the new Service, including the Application and any Extensions. Additional Development/Test Environments are available upon request and for an additional charge.

2.2 Storage Backup and Restore

As part of the base Service, HCL provides storage snapshot backups for data protection of file systems. Storage snapshot backups include supporting data availability, configuring snapshot and replication schedules, and facilitating restore of data from snapshots. Daily snapshots are retained for a number of days and to a maximum capacity defined in the Order Schedule. Storage snapshot backups provide the ability to restore retained data to any day within the backup period. Longer backup durations and additional backup capacity are available upon request and for an additional charge.

2.3 Service Integration

The following capabilities are provided as part of the Service. Only secure transmission protocols and methods are allowed.

- Application Program Interface (API) - A set of routines, protocols, and tools for building software and applications.
- Messaging - Provides for inter-process communication (IPC), or for inter-thread communication within the same process. This permits the Service to be an endpoint for networks, or point-to-point communications. The Service does not provide an inbound connection point, nor routing between two (2) or more endpoints which are not part of the Service.

- Secure File Transfer Protocol (SFTP) or SSH File Transfer Protocol - A network protocol that provides file access, file transfer, and file management over a secure and reliable data stream. The Service provides a SFTP server for inbound file transfers destined to be consumed by the Extensions. Outbound transfer from the Service of data, and reports, can be accomplished through a java-based SFTP client, imbedded in the Application or Extensions. SFTP transfers require file-level encryption to protect the data at rest.

2.4 Network Integration

The following are the supported methods for integrating with Customer networks. Only secure transmission protocols and methods are allowed. Such supported methods apply solely to HCL Now integrations and not to customer-side network integrations. Customer is responsible for its internet connection and its VPN endpoint.

- Allow List Connections over the Internet - Limits access to the Service, or parts of the Service, to specific internet public addresses. The limit access provides the flexibility to limit access to Customer designated locations. Allow listing is included in the Service.
- Virtual Private Network (VPN) through the Internet. Additional VPN connections are available are available upon request and for an additional charge.
- In order to manage throughput to the servers, no more than 10% of the catalog delta updates or product inventory updates may be transmitted to the servers within a 15-minute period.

2.5 Security Features and Responsibilities

Security monitoring and incident response is provided by 24/7 365 Security Operations Center. HCL Commerce on HCL Now also implements the following security features:

- Data encryption in transit - The Service does encrypt content using the most current, stable and secure encryption protocols during data transmission between the cloud infrastructure and the endpoint networks or machines depending on the protocol used. Customer is responsible for ensuring transfer of content is via a secure protocol (as an example SFTP) while transmitting data.
- Data encryption at rest – HCL Commerce's database is fully encrypted at rest. All the passwords on all the files are encrypted. Other files are secured using the disk encryption of cloud provider.
- Anti-Virus & Malware Protection - Next generation anti-virus and malware software is installed and managed on HCL managed operating system software.
- Firewall - HCL creates initial firewall policies to restrict all unnecessary and unauthorized access to the Service Environments, and tests firewalls and networking components. The service is available in a high availability virtualized, standalone single hardware platform or high-availability dual hardware platform configuration.
- Two-factor authentication is required for Customers and HCL authorized system administrators who retain server administrative access to the Service Environments. HCL provides licensing, installation, and proactive monitoring and management for two-factor authentication alerts for the Service. The number of two-factor users provided is listed in the Order Schedule.
- Network Based Intrusion Detection & Prevention - HCL implements network-based intrusion prevention, monitors the systems, responds to intrusion prevention system alerts and performs event correlation. A standard intrusion preventions system (IDS & IPS) policy will be applied to the Service.
- Host Based Intrusion Detection - provides intrusion prevention on host endpoints that utilize standard intrusion prevention policies to monitor for malicious activities and will respond to the intrusion prevention system alerts.
- File Integrity Monitoring - HCL implements file integrity monitoring by validating the integrity of operating system and application software files using an automated verification method between the current file state and a known baseline.

2.6 Disaster Recovery

In the event of an HCL declared Disaster, HCL will communicate with Customer on an hourly basis as to the status of the recovery process, including progress regarding the Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO"). The defined RPO/RTO duration is 2 hours RPO, 4 hours RTO.

HCL provides the ability to failover a full copy of Customer data to a designated standby environment at a geographically disperse DR location within the defined RPO and RTO. HCL manages storage disaster recovery utilizing a replication of storage snapshots to achieve the required RPO/RTO. Storage snapshots provide a point-in-time capture of Customer data using the HCL managed storage infrastructure. Differential data changes between snapshots are replicated to offsite storage for maintaining synchronization of the Customer data. Snapshot and replication frequency is determined by the defined RPO/RTO. Storage capacity is allocated per Gigabyte as necessary to meet the Customer contracted disaster recovery requirements. Disaster Recovery capability not automatically provided for customers with volumes below 100,000 order lines per annum, but is available upon request and for an additional charge.

2.7 Content Delivery Network (CDN)

The Service includes a Content Delivery Network (CDN). The CDN is a required component of the Service and enhances site performance to the consumer. The CDN capacity is defined in the Order Schedule. Additional CDN capacity is available upon request and for an additional charge.

2.8 Transactional Emails

The Service includes an email gateway for administrative emails and notifications. This gateway cannot be used for Customer facing transactional emails to consumers. Transactional emails must flow through an external SMTP gateway service provided by the Customer or Customer's preferred email service provider.

3 Service Features – HCL Now Managed Service

3.1 Service Level Agreement ("SLA")

HCL provides the following availability service level agreement ("SLA") for the Service. The SLA is not a warranty and is Customer's sole and exclusive remedy. The SLA is available only to Customer and applies only to use in Production Environments.

3.2 Managed Services Support

English language managed services support is provided for the Service by the HCL Now Managed Services Team. Incidents are categorized using Priority levels as described below:

3.2.1 Priority Definition, Response Time, Coverage

Priority	Prority Definition	Response Time Objectives	Response Time Coverage
P1 (Critical)	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a Production Environment and indicates an inability to access services resulting in a critical impact on operations. This	Within 15 minutes	24/7

	condition requires an immediate solution.		
P2 (High)	Significant business impact: A service business feature or function of the service is severely restricted in its use or Customer is in jeopardy of missing business deadlines.	Within 1 business hour	24/7
P3 (Moderate)	Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours
P4 (Low)	Minimal business impact: An inquiry or non-technical request.	Within 1 business day	M-F business hours

HCL Now Support applies to the hosted environment and associated managed services. HCL Now Support differs from product technical support for the underlying software product and product features. Technical support for the products hosted on HCL Now shall be as set forth in the HCL Support Guide located at: https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0010420. Cases raised with the HCL Now Support team that require product technical support will be transferred to the product technical support team and such cases shall be addressed pursuant to the HCL Technical Support Guide and response objectives.

- Customer will ensure that a resource is assigned to work with HCL to provide information or verification on an ongoing basis, until the issue is resolved.
- In the event of multiple reported Errors being worked concurrently, unless otherwise requested by Customer, HCL will prioritize based on Priority starting with Critical (P1) and then on the time the Error was reported starting with the oldest. The SLA will apply to the top two Errors being worked based on this Priority.
- In the event HCL response time to an Error is negatively impacted due to Customer's delayed response to HCL request for additional information to correct an Error, the response times provided above will be extended by an amount of time proportionate to such delay.
- Both parties may agree that due to technical dependencies and other factors, certain Errors classified as Medium and Low may be resolved in an appropriate scheduled maintenance window. Customer acknowledges that HCL does not and cannot guarantee that all Errors can or will be corrected.
- System changes for upgrades or patches will be applied during Scheduled Maintenance unless the change is required to restore system availability.
- Business Days are Monday through Friday excluding national Holidays of the country from where the service is provided.

3.2.2 Availability Credits

An HCL Now support case for failure to meet an SLA must be submitted within 3 business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Service based on the duration of time during which Production Environment processing for the Service is not available ("Downtime"). Downtime is measured from the time Customer reports the event or external monitors report service unavailability, until the time the Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond HCL's or the selected Cloud Platform provider's control; problems with Customer or third-party content or technology, designs or instructions; unsupported system configurations and platforms or other Customer errors; or Customer-caused security incident or Customer security testing. HCL will apply the highest applicable compensation based on the cumulative availability of the Service during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 10 percent of one twelfth (1/12th)

of the annual charge for the HCL Now Managed Service part. Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

3.2.3 Service Levels

Availability of the Service during a contracted month:

Availability during a contracted month	Compensation (% of monthly HCL Now Managed Service part fee* for contracted month that is the subject of a claim)
Less than 99.9%	2%
Less than 99%	5%
Less than 95%	10%

*The service credit will be applied to the invoice of the contracting party for the applicable month in which the outage occurred.

3.2.4 Incident Priority Levels by Environment

Incident Priority level is dependent on the environment in which the incident occurs. See section 3.2.1 for Priority Definition, Response Time and Coverage.

Environment	Incident Priority Levels by Environment
Development/Test	Any incidents submitted are treated as Priority 3
Pre-Production	Any incidents submitted are treated as Priority 3
Production	Priority 1/2/3/4 depending on incident
Disaster Recovery	Priority 1/2/3/4 depending on incident

3.3 Monitoring

3.3.1 HCL Software Product and Environment Monitoring

The following monitoring will be performed as part of the HCL Now Managed Service:

Environment	Level of Monitoring
Development/Test	Basic server and cluster health. Database monitoring.
Pre-Production	Application performance data available but not monitored. Basic server health and database monitoring.
Production	Infrastructure and cluster health, application health, database health
Disaster Recovery	As per production when DR is activated. Data synchronization health.

3.3.2 External Monitoring for Production Environments

HCL will provide monitoring, alerting and reporting from a provisioned environment outside of the customers deployed environment as part of the base Service in the form of:

- External Monitor – Page – Monitor a single page (such as home page, product page) for specific response strings, at 5-minute intervals; and
- External Monitor – Transaction – Monitor a series of up to 10 pages in a process (such as search results, add to cart) at 5-minute intervals.
- Custom Transaction Monitor - can be deployed as an additional transaction monitor and may incur an additional cost.

External monitors originate from outside a customer's cloud Production Environment to monitor the Service through an automated method of simulating the click-paths of a given user experience. HCL will work with Customer to develop

synthetic use-cases and will monitor and open appropriate support case based on the impact to the Service and begin triage of the issue. The quantity of monitors will be specified in the Order Schedule, and additional External Page Monitors, External Transaction Monitors and Custom Transaction Monitors can be added to the entitlement.

3.4 Provisioning of Environments

HCL will provision the environments as part of the Service in three phases. Billing for the Hosting Service may vary in each phase, and will be outlined in the Order Schedule:

- Phase 1 – Development/Test environments will be provisioned.
- Phase 2 – Pre-Production and Production Environments will be provisioned.
- Phase 3 – The site will go live and Production SLA will come into effect.

3.5 Customer Extensions

Extensions (also known as customizations) ("Extensions") permit the Customer to configure the Service to meet Customer's business requirements by creating software extensions to the Service Application. Extensions are content provided by customers and/or their agents in the use of the Service and are not part of the Service. Customer is responsible for the development, performance, management, maintenance and support of all Extensions in all Environments. Customer may contract separately with HCL or a third-party contractor specifically authorized in writing by HCL to create Extensions. Customer is responsible for ensuring that Customer and any third-party contractor complies with these terms.

Customer-created Extensions are subject to the following additional terms and conditions:

(1) HCL will have the right to review and approve or reject the design documents, testing plans, test results and object code for Extensions for compliance with the terms of the Agreement.

(2) HCL may require Customer to perform performance tests specified by HCL. Customer shall provide such design documents, testing plans and results, and object code to HCL for review a reasonable time in advance of the Service going live or updates applied and shall co-operate with HCL in resolving issues identified by HCL. Customer is responsible for troubleshooting any performance issues related to Customer Extensions.

(3) Customer agrees to have in place and maintain a program to prevent malware, including viruses, Trojan horses, denial-of-service and other disruptive and covert technologies from being included in the Extensions.

(4) HCL may monitor and scan Extensions for security vulnerabilities and/or malware. HCL may remove the Extensions from any Service environment or suspend the Service until the security vulnerability or malware issue is resolved.

(5) Extensions will not include or add any third-party commercial or packaged software product that operates independently of the Service, and the addition of any such third-party commercial or packaged software is prohibited.

(6) Customer is responsible to train and maintain staff with an appropriate knowledge and skill level to work with the Service and Extensions during the term of the agreement. Any training or educational assistance that is required is at the Customer's expense. Should it be determined by HCL that the Customer is not able to perform its required tasks with reasonable assistance, HCL, at its sole discretion, may require that Customer engage in hands-on knowledge transfer activities with HCL

professional services personnel. Such knowledge transfer activities shall be, unless between HCL and its affiliates, at the Customer's expense. HCL will provide such training to Customer upon Customer's request for an additional charge.

(7) Customer, or their licensors retain all right, title, and interest or license in and to the Extensions provided to HCL for hosting with the Service. Customer represents and warrants to HCL that Customer has all rights necessary to provide the Customer Extensions to HCL for the purpose of hosting with the Service and that neither the Customer Extensions nor the hosting by HCL with the Service violate any third-party patent or copyright.

(8) Customer grants to HCL, on a world-wide, royalty-free, fully paid, revocable, sub-licensable basis, all rights and licenses to, and agrees to promptly obtain and keep in effect Required Consents for all Extensions, necessary for HCL and its subcontractors to host the Extensions and otherwise perform its obligations. Upon request, Customer will provide to HCL evidence of any such rights, licenses, or Required Consents. HCL will be relieved of its obligations to the extent that they are affected by Customer's failure to promptly obtain and provide to HCL any such rights, licenses, or Required Consents. In this paragraph, "Required Consents" means any consents, licenses or approvals required to give HCL and its subcontractors the right or license to access, use and/or modify in electronic form and in other forms solely as necessary to perform under this Service Description, including making derivative works, the Extensions, without infringing the ownership or intellectual property rights of the providers, licensors, or owners of such Extensions.

(9) Customer will ensure code, data and other artifacts introduced by Customer through the Extensions, do not increase the security risk, or require additional certification requirements unless expressly agreed to by HCL through an amendment or addendum to this Service Description. Without limiting any of the foregoing, Customer will: (a) perform web application and static code vulnerability scans on all Extensions to identify any security exposures; and (b) disclose to HCL in writing the existence of any exposures that were identified by a vulnerability scan that are included in or is provided in connection with the Extensions.

(10) Prior to Customer Operational Acceptance (COA), Customer deploys Extensions to Development/Test, Pre-Production, and Production Environments as applicable. After Customer Operational Acceptance, HCL will deploy Extensions to Pre-Production and Production Environments as applicable through an HCL support case management tool request. Extensions are required to be deployed and validated in a Pre-production environment prior to deployment to Production.

(11) Any additional work to be performed by HCL in support of Extensions, such as creation of Extensions or activation of other integrated components, may be described in a separate statement of work between HCL and Customer, and will be subject to separate fees invoiced in accordance with the terms and fees contained in such a statement of work.

(12) As part of the Service the HCL team will provide case management involving issues with the Service ("Support Case Triage") through the Customer. As part of Support Case Triage, HCL will investigate the issue through diagnostic tasks. If the cause is determined to be related to the Service, HCL supported Extensions (for which Customer has contracted with HCL under a separate agreement) or infrastructure, then HCL will manage the case through to problem resolution. If the solution must be provided from an area of Customer responsibility, HCL will provide any relevant diagnosis

uncovered in the triage process to assist the Customer, or their Authorized third-party, in problem resolution and continue to provide case management through case management tools.

3.6 Customer Operational Acceptance

Customer Operational Acceptance (COA) occurs after HCL has provisioned the Production Environment, and the Customer has completed the initial deployment of the Extensions onto the Production Environment, and is the process through which HCL and the Customer determine that:

- The Service has been installed, applied Extensions and data loads, functionally tested, performance tested and accepted in writing by Customer;
- HCL has documented and audited environment controls for devices and configuration to verify operational readiness;
- HCL has applied quality assurance methodology to the environment including redundancy testing and automated startup/shutdown procedures for applications;
- Post Go-Live support services begin; and
- The SLAs go into effect.

In preparation for COA Customer must:

- Provide an access list of persons authorized for access, opening Support cases, scheduling maintenance, and requesting changes;
- Identify those employees authorized to request modifications to the access list;
- Provide timely access to and participation of Customer personnel during implementation activities, in accordance with the schedule mutually agreed upon; and
- If applicable, be prepared to redirect Domain Name System (DNS) entries from the existing sites/services (if applicable) to the Service IP addresses at Go-Live. When necessary, HCL will validate the DNS redirection.

3.7 Environment Updates

3.7.1 Software Versions

The Service is based on a version/release level of the generally-available HCL Commerce Enterprise ("HCL Commerce") software current as of the date of Customer's initial agreement for the Service. Support for the Service is available only while that version or release of HCL Commerce is under support in accordance with the HCL software support lifecycle policy, and support for the Service will no longer be available as of the announced end-of-support date for that version or release of HCL Commerce.

3.7.2 Maintenance Windows

HCL's standard weekly maintenance windows are currently scheduled for the Service. These maintenance windows are the Customer's opportunity to request the application releases be applied to their Production Environment. Restrictions may apply and coordination with HCL is required. These maintenance windows do not necessarily mean the Services will be down or unavailable and Service disruptions will be minimized for HCL activities. If the Customer has maintenance activities for their extensions that maintenance activity must be performed during the maintenance windows. HCL will notify the Customer if the Services will not be available during the maintenance windows.

Other scheduled and non-scheduled (emergency) down times may occur and Customer will be notified of the Services being unavailable at least five (5) business days in advance unless the vulnerability, risk of loss or Service integrity is deemed by HCL to be too high.

3.7.3 Deployment of HCL-Initiated Updates

HCL performs the required maintenance and updates of the Service which includes implementing infrastructure patches, Security Patches, and new versions of Containers (collectively, "HCL-Initiated Updates").

HCL-Initiated Updates are performed on a routine basis or during scheduled maintenance windows. Scheduled maintenance is announced at least five business days in advance or maintenance determined by HCL to be an emergency upon notice provided to a customer ("Scheduled Maintenance"). Scheduled maintenance windows are excluded from SLA calculations and remedies.

If an HCL-Initiated Update requires Customer testing of Extensions, or there is a negative effect of an HCL-Initiated Update on Extensions, prior to promotion to the Production Environment, HCL and Customer will develop a mutually agreeable schedule for deployment. Configuration changes or code changes required to ensure the system operates with the HCL-Initiated Update is the responsibility of the Customer. As new versions of HCL Commerce software are made available, they will be pushed to Customer's container registry as HCL-Initiated Updates. Customers must not run a container in the Production Environment more than 2 point releases older the current version.

If HCL determines that as a result of an HCL-Initiated Update not being promoted to the Production Environment a high severity security vulnerability exists or potentially exists, HCL may immediately suspend the Service until the HCL-Initiated Update has been promoted.

Should the HCL-Initiated Update remain unimplemented in the Production Environment because of an Extension issue, or lack of Customer permission to promote the change, Customer agrees to indemnify, defend and hold HCL harmless against any third-party claims arising in connection with the use of the Service to the extent such claim could have been avoided by implementing the HCL-Initiated Update. Further, SLA and security provisions will not apply and additional fees will result if this condition is not met.

3.7.4 Deployment of Customer-Initiated Updates

Customer may request that HCL apply Customer-supplied updates to Extensions, data, or Application configuration (excluding Upgrades) to the Service (collectively "Customer-Initiated Updates"). HCL will work with the Customer to develop a mutually agreed upon schedule for deploying Customer-Initiated Updates to the Pre-Production and Production Environments. Customer will provide the necessary deployment package and instructions including verification and back-out steps.

HCL may publish black-out or restricted change windows to accommodate holidays, peak activity periods, or other such similar events.

4 Term and Renewal Options

The term of the Service begins on the date HCL notifies Customer of their access to the Service, as documented in the Entitlement. The Entitlement will specify whether the Service renews automatically, or terminates at the end of the term.

For automatic renewal, unless Customer provides written notice not to renew at least 90 days prior to the term expiration date, the Service will automatically renew for the term specified in the Entitlement.

5 Additional Terms

5.1 Security, Compliance Standards and Data Protection

HCL will provide certification/attestation for ISO27K, SOC 2 Type 2, PCI, and HIPAA against the HCL Now platform. As any applicable certifications are achieved, they will be referenced at**:** https://www.hcltechsw.com/legal/compliance.

5.2 ISO27K

HCL will provide certification/attestation against the following ISO27K standards. As any applicable certifications are achieved, they will be referenced at**:** https://www.hcltechsw.com/legal/compliance:

- ISO 27001 - ensures that HCL manages the security of all information assets and adheres to its ISMS (Information Security Management System) for maintaining the confidentiality, integrity, and availability of data.
- ISO 27017 - ensures that HCL manages the information security aspects of cloud computing.
- ISO 27018 - ensures that HCL offers suitable information security controls to protect the privacy of Personally Identifiable Information (PII) in the Cloud.
- ISO 27701 – ensures that HCL offers suitable information security for implementing a continually improving Privacy Information System (PIMS).

5.3 SOC 2 Type 2

HCL will demonstrate adherence to the AICPA's Trust Services Principles and Criteria for Security and Availability, Confidentiality, and Privacy. As any applicable certifications are achieved, they will be referenced at**:** https://www.hcltechsw.com/legal/compliance.

5.4 Payment Card Industry (PCI) Account Data

HCL will demonstrate its adherence to the technical and operational standards that secure and protect credit card data transmitted through card processing transactions. The Service is not intended for storage of PCI Account Data, and storage of account data is not supported by HCL. HCL will comply, for the duration of the Service, with the Payment Card Industry Data Security Standard (PCI DSS) for those controls that are managed by the Service. Proof of compliance will be provided through an Attestation of Compliance (AOC). As any applicable certifications are achieved, they will be referenced at**:** https://www.hcltechsw.com/legal/compliance.

5.5 HIPAA

HCL will attest that administrative, physical, and technical safeguards are in place to protect the confidentiality, integrity, and availability of protected health information (PHI).

5.6 Data Protection

Personally Identifiable Information (PII) processed by HCL as a data controller will be processed in accordance with the HCL Privacy Statement found here: https://www.hcltech.com/privacy-statement and the Cookie Disclosure found here: https://www.hcltech.com/cookie-disclosure.

Customer is aware and agrees that HCL may, as part of the normal operation and support of HCL Commerce on HCL Now, collect PII from Customer (Customer's employees and contractors) related to the use of HCL Commerce on HCL Now, through tracking and other technologies. HCL does so to gather usage statistics and information about effectiveness of HCL Commerce on HCL Now for the purpose of improving Customer's user experience and/or tailoring interactions with Customer. Customer confirms that it will obtain or has obtained consent to allow HCL to process the collected PII for the above purpose within HCL, other HCL affiliates and their subcontractors, wherever HCL and such

subcontractors do business, in compliance with applicable law. Customer data that does not contain PII may also be used by HCL to improve its products and services. HCL will work with Customer to respond to valid requests from Customer's employees and contractors to access, update, correct or delete their PII. PII processed by HCL as a data processor will be processed in accordance with the terms and conditions of the MLA including, if applicable, the HCL Data Processing Agreement located here or found on the HCL Software Master Agreements page here: https://www.hcltechsw.com/resources/master-agreements.

6 Definitions

Application – refers to the HCL software products that provide the base functionality for the Service, including the original and all whole or partial copies: 1) machine-readable instructions and data, 2) components, 3) audio-visual content (such as images, text, recordings, or pictures), 4) related licensed materials, and 5) license use documents or keys, and documentation, which are provided by HCL and which Customer may access through the Service.
Container – a Docker container that contains HCL Commerce application functionality.
Disaster – is a natural or human-induced event which disrupts the operations of vital technology infrastructure and systems creating a complex or irreversible disruption to the Service.
Disaster Recovery (DR) – actions taken by the HCL Now Managed Service team to recover from a Disaster back to operational state.
Environment – refers to a deployable instance of the Application, including the infrastructure necessary to support that Application for its intended use, and refers to the Integration Environment, Development/Test Environment, Pre-Production Environment, Non-Production or Production Environment, as the context requires.
Extensions (also known as Customizations) – are the software artifacts and configuration provided by the Customer, or their authorized third party, to extend the Service by implementing the Customer's business process flow, manage specific data needs, and provide Customer specific branding, in support of the Customer's business requirements. This can be, but not limited to, software code, software assets, plug-ins, customizations, database extensions, scripts or files created to customize Customer's utilization of the Service, including Integrations to Third Party Services or data sources. Extensions are the responsibility of the Customer.
Gigabyte (GB) – a unit of measure for network traffic or storage.
Go-Live – is the activation of the Production Environment Site for use by the Customer for normal business activities and/or use by the Customer in servicing, in anyway, their customers and/or use by the Customer in support of revenue generation.
Payment Card Industry (PCI) Account Data – is the cardholder account information contained on a payment card, or associated with a payment card transaction, including major debit, credit, prepaid, e-purse, ATM, POS cards, including Cardholder Data (CHD) and Sensitive Account Data (SAD) subject to security and handling guidelines set by the Payment Card Industry Data Security Standard (PCI DSS).
Personally Identifiable Information (PII) – is any information which relates to an identified or identifiable individual.
Recovery Point Objective – is the maximum tolerable period in which data might be lost from an IT service due to a Disaster.
Recovery Time Objective – is the targeted duration of time, and a service level, within which a business process must be restored after a Disaster is declared in order to avoid unacceptable consequences associated with a break in business continuity.
Security Patch – is a fix for a security-related vulnerability that affects the Application.
Terabyte (TB) – a unit of measure for network traffic or storage.
Third-Party Services – are third party data services, databases, web services, software, or other third-party content accessed via the Service.
Upgrade – is a new version or release of the base Application that replaces an earlier version or release, and typically includes new features and functions.

Extended Commerce ecosystem components – components the Customer would like the HCL Now Managed Service team to manage which fall outside the scope of HCL Commerce as defined in this Service Description. Examples include 3rd party content management systems, custom developed services, or other 3rd party software that form part of the Customer's ecosystem.

7 Revision History

Date	Change	Rationale
6/18/2021	2.8 Transactional Emails added	The service does not at this time have a transactional SMTP gateway capability. Customers should procure a SMTP relay that caters for greater capacity and functionality for managing transactional and campaign emails coming from the Commerce Now service.
6/22/2021	2.2 Backup time period and capacity moved to the order schedule.	Backup requirements may differ between customers, so the time duration and capacity will be noted on the Order Schedule. This provides customer with cost flexibility as storage is an expensive component.