Service Description - HCL Workload Automation on Now

This Service Description ("Service Description") describes the HCL Workload Automation on HCL Now Service ("HCL Workload Automation Now" or "Service"). Additional terms governing the HCL Workload Automation 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 Workload Automation on HCL Now

HCL Workload Automation on HCL Now is the automation platform to orchestrate, initiate, run and manage digital business processes from legacy to cloud & Kubernetes systems.
HCL Workload Automation optimizes business with the most advanced modeling, scheduling and monitoring capabilities to seamlessly orchestrate simple to complex workflows across multiple platforms and applications.

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

- HCL Workload Automation on HCL Now Infrastructure Service
- HCL Workload Automation on HCL Now Managed Service

1.1 HCL Workload Automation Software

A separate license entitlement for HCL Workload Automation software is necessary for use of the HCL Now Service.

1.2 HCL Workload Automation on HCL Now Infrastructure Service

HCL Workload Automation on HCL Now Hosting Service is the hosting environment and infrastructure on which the Workload Automation application runs. The exact provisioning and configuration of the hosting environment will be determined by the HCL Workload Automation on HCL Now team in its sole discretion.

HCL Workload Automation is based on a cloud-native Kubernetes infrastructure with high availability and external database servers in HADR (High Availability Disaster Recovery) running on Virtual Machines.
The configuration and pricing for the infrastructure and hosting environment is based on two metrics:

- Peak of jobs per hour on the HCL Workload Automation Engine
- Number of concurrent users on the Dynamic Workload Console (UI)

According to the values defined by the metrics, **5 standard configurations** in high availability have been defined:

- Extra small:
  - Engine（regardless if production/test/dev): <1K jobs/hour
  - UI: Max 60 concurrent users
- Small:
  - Engine（regardless if production/test/dev): <2K jobs/hour
  - UI: Max 200 concurrent users
- Medium:
  - Engine（regardless if production/test/dev): <15k jobs/hour
  - UI: Max 300 concurrent users

- Large:

    - Engines（regardless if production/test/dev):
        - <15k jobs/hour
        - <5k jobs/hour
    - UI: Max 300 concurrent users
- Extra large:
    - Engines（regardless if production/test/dev):
        - <15k jobs/hour
        - <10k jobs/hour
        - <5k jobs/hour
    - UI: Max 300 concurrent users

Per each tier, the following infrastructure components are sized and priced:

- **K8s Regional Cluster**: it is the set of nodes running containerized applications. As per standard configuration, all tiers have 2 regional clusters.
- **K8s Regional Cluster – Nodes**: it reports the number of worker machines ("nodes") per each regional cluster. It includes the characteristics of the nodes (CPUs, memory)
- **Database servers + OS**: it is the number of servers running on Red Hat Enterprise Linux OS used for the DB2 database. It includes the characteristics of the machines (CPUs, memory)
- **Bastions**: key components of security, the bastions are servers providing access to a private network from an external one
- **K8s Regional SSD Storage (GB)**: it indicates the amount of storage (solid state disc type) – expressed in Gigabyte – needed for the Kubernetes regional cluster.
- **DB2 Storage - Zoned SSD PD (GB)**: it indicates the amount of storage (solid state disc type) – expressed in Gigabyte – needed for the DB2 servers.
- **Backup storage [cold line / multi-region / 1% retrieve]**: it indicates the backup storage amount. It has the following characteristics:
    - Cold line: highly durable storage service used for storing infrequently accessed data
    - Multi-region: to ensure geo-redundancy of data
    - 1% retrieve: it relates to the amount of data that can be retrieved each month without additional costs
- **Load Balancer**: it distributes the workloads across multiple computing resources
- **Networking (GB)**: it is a VM to VM internet egress type
- **VPN (Virtual Private Network):** by default, 2 networks are available per each tier (1 on the main region and the second one for Disaster Recovery)

1.3 HCL Workload Automation on HCL Now Managed Service

HCL Workload Automation on 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
- Business Continuity Planning and Execution for the HCL Now platform in the event of Disaster Recovery events

1.4 HCL Workload Automation on HCL Now Capacity

HCL Workload Automation on HCL Now can scale based 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 the following. If these metrics are exceeded the performance of the Service may degrade.

- Peak of jobs per hour on the HCL Workload Automation Engine
- Number of concurrent users on the Dynamic Workload Console (UI)

Hosting environments contain items which are charged based on usage. The maximum amount of these resources you can have, use or consume on a monthly or annual basis will be listed in the Order Schedule. If those thresholds are exceeded, HCL will charge for the excess consumption. For infrastructure usage the HCL Now Workload Automation implementation allows autoscaling up to twenty percent (20%) for a cumulative total of two weeks during the contract term. Infrastructure usage beyond such limit shall be calculated and presented to you in the form of an amendment to the Order Schedule. The pricing for such additional usage will be based on the rates published by the chosen cloud service provider and will be charged under HCL Now Infrastructure Usage part.

1.5 Variations to Entitlement

Variations in configuration from the entitlement may be established prior to commencement of the service or during the life of the contract. For variations made to the entitlement prior to contract start, the scope and cost of these will be quoted in the Order Schedule. For changes made during the life of the contract, scope and cost will be estimated and agreed via amendments to the Order Schedule. These include:

- # of K8s Regional Cluster Nodes
- Database Servers Type(s)
- K8s Regional SSD Storage (GB)
- Database Storage - Zoned SSD PD (GB)
- # of VPN
- Networking (GB)
- Increase in software entitlement

Variations to entitlements may impact the Managed Service costs, which may also be estimated and agreed by amendments to the Order Schedule

2 Service Features – HCL Workload Automation on HCL Now Hosting

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 Workload Automation on HCL Now Hosting 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.

Customers can decide if they want to use the engines servers for production/test/dev, based on the needed capacity as defined in paragraph 1.2.

Additional engine servers 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 up to 14 days and are stored securely and in a highly available manner. Storage snapshot backups provide the ability to restore retained data to any day

within the previous 14 days. Additional backup and restore capacity and services are available upon request and for an additional charge.

2.3 Service Integration

The following capability is 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.

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.

- Virtual Private Network

2.5 Security Features and Responsibilities

Security monitoring and incident response is provided by 24/7 365 Security Operations Center. HCL Workload Automation 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 HCL network 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 Workload Automation 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 ID's 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 prevention 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 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. Disaster recovery includes a full copy of the Customer data to HCL managed storage infrastructure at the geographically disperse DR location. 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.

3 Service Features – HCL Workload Automation on HCL Now Management

3.1 Service Level Agreement ("SLA")

HCL provides the following availability service level agreement ("SLA") for the Service: 99.9% infrastructure availability. 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 Workload Automation on HCL Now Management Team. Incidents are categorized using Priority levels as described below:

3.2.1 Priority Definition, Response Time, Coverage

Priority	**Priority 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 condition requires an immediate solution.	Within 15 minutes	24/7
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

Managed Services Support applies to the hosted environment and associated managed services. Managed Services 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. Managed Services Support tickets raised with the Managed Services Support team that require product technical support will be transferred to the product technical support team and such tickets 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 Workload Automation on 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 Workload Automation on 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.

3.3 Monitoring

3.3.1 HCL Software Product and Environment Monitoring

HCL Workload Automation on HCL Now Managed Service guarantees continuous monitoring at product and infrastructure level, to ensure business continuity.

3.4 Customer Extensions

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, management, maintenance and support of all Extensions. 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 any such third-party contractor complies with these terms.

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

(1) Customer agrees to comply with the Offering Standards in connection with the development and delivery of Extensions.

(2) 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.

(3) 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 and shall co-operate with HCL in resolving issues identified by HCL. Customer is responsible for troubleshooting any performance issues related to Customer Extensions.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

(10) 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.

Additional considerations:

- Customer is responsible for testing and validation of Extensions in all Environments.
- Prior to Customer Operational Acceptance (COA), Customer deploys Extensions to Integration, Test, Pre-Production, and Production Environments as applicable.
- After Customer Operational Acceptance (COA), HCL will deploy Extensions to Pre-Production and Production Environments as applicable through an HCL support ticketing tool request. Extensions are required to be deployed and validated in a Pre-Production environment prior to deployment to Production.
- 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.

- 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.

3.5 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, tested, including Extensions and data loads, 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 person(s) authorized for access, opening trouble tickets, 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.

3.6 Environment Updates

3.6.1 Software Versions

The Service is based on a version/release level of the generally-available HCL Workload Automation ("HCL Workload Automation") 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 Workload Automation 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 Workload Automation.

3.6.2 Maintenance Windows

Maintenance activities may occur on a weekly basis. These maintenance windows are the Customer's opportunity to request the application releases be applied to their 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 and the Service planned downtime from the maintenance will not exceed eight hours in a calendar month.

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.

3.6.3 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 Workload Automation software are made available, they will be pushed to your 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.

3.6.4 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 achieve certification/attestation for ISO27K, SOC 2 Type 2, PCI 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, Availability, Confidentiality, and Privacy. As any applicable certifications are achieved, they will be referenced at **https://www.hcltechsw.com/legal/compliance.**

5.4 6.3.3 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 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 Workload Automation on HCL Now, collect PII from Customer (Customer's employees and contractors) related to the use of HCL Workload Automation on HCL Now, through tracking and other technologies. HCL does so to gather usage statistics and information about effectiveness of HCL Workload Automation 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.

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 Workload Automation on 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 Workload Automation on HCL Now Management 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.
Extensions – 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 Workload Automation ecosystem components – components the Customer would like the HCL Workload Automation on HCL Now team to manage which fall outside the scope of HCL Workload Automation on as defined in this Service Description. Examples include 3rd party content management systems, custom developed services, agents installed on customer's environment or other 3rd party software that form part of the Customer's ecosystem.