

SERVICE LEVEL AGREEMENT - SLA

GENERALLY APPLICABLE TO VELRA SOFTWARE SERVICES

1. Document Information and Applicability

Document title:	Service Level Agreement for Velra Software Support and Maintenance	Document code:	SLA-VELRA-01
Issued by:	Velra Joint Stock Company	Version:	1.2
Issue date:	30/04/2026	Effective date:	30/04/2026
Conditions of validity:	Applicable only where a valid Contract/Order is in effect	Review cycle:	Every 06 months or upon a service change

1.1. Parties and Order of Precedence

- **“Velra”** means the legal entity providing software and services under a Contract or Order;
- **“Customer”** means an organization or individual that has entered into a valid Contract or Order for services with Velra;
- This SLA takes effect only when the Customer has a valid Contract/Order that references this SLA. If a Contract/Order or appendix signed by authorized representatives of both Parties contains provisions that clearly differ from this SLA, such separately agreed provisions shall prevail; all remaining matters shall be governed by this SLA.

1.2. Effectiveness, Version Updates, and Termination

1. This SLA remains effective throughout the term of the corresponding Contract/Order and does not apply where a Contract has not been entered into or has expired;
2. A Contract that remains in effect shall continue to apply the version of the SLA referenced therein, unless the Parties agree otherwise in writing or an update mechanism specified in the Contract applies;
3. A newly published version of the SLA shall apply to new Contracts/Orders or renewal periods from the effective date of the new version.

2. Objectives, Scope, and Principles

2.1. Objectives

This SLA establishes a consistent operational and technical support framework for Velra software services in order to:

- Standardize the processes for incident intake, classification, response, updates, and restoration;
- Clearly define the respective responsibilities of Velra, the Customer, and third parties;

- Apply reasonable technical measures and processes to maintain the stability, safety, security, and integrity of systems within Velra's management scope;
- Provide a transparent basis for monitoring, measuring, and reconciling service quality.

2.2. Scope of Application

1. This SLA applies only to Customers that have entered into a valid Contract or Order for services with Velra under an On-premise or Cloud model;
2. The specific support scope for each Customer is determined by the deployment model, product, location, device scale, and service package stated in the executed Contract/Order;
3. The public standards in this document do not automatically create rights or obligations beyond the scope of a valid Contract/Order.

2.3. System Administration, Ownership, and Monitoring Principles

1. **Software ownership and service model:** The Customer pays fees to receive the right to use the software system and services under the Contract; the software copyright, source code, and technical documentation are Velra's intellectual property;
2. **Scope directly administered by Velra:** To ensure consistency, security, and operational integrity, Velra directly administers the following three components: (i) the Operating System, (ii) the Operating System Administrator Account, and (iii) the installed Velra Software System;
3. **Customer monitoring rights:** Velra's possession of the privileged operating system administrator account is intended to control changes and protect the system and does not limit the Customer's right to inspect its assets. Velra provides the Customer's administration team with a monitoring account (for On-premise) or status tools/reports (for Cloud) to monitor resources, hardware status, and authorized logs;
4. **Control of technical intervention:** The monitoring account does not have permission to modify the operating system or access source code. Change requests are submitted through the support channel and are logged. The operating system administrator account is managed by Velra, and full administrative privileges are not granted to the Customer or any third party; ownership of the server does not automatically transfer operating system administration rights or source code copyright.

2.4. Uptime/Availability Commitment Principles

1. For On-premise services: Physical servers, storage, power supply, and internal network infrastructure managed by the Customer are not covered by Velra's uptime commitment. Velra applies response indicators and restoration targets to incidents involving software/operating systems administered by Velra under Section 5, subject to the cooperation conditions and exclusions set out in Section 5.3.
2. For Cloud services: Availability levels, measurement periods, calculation methods, excluded maintenance periods, and remedies for failure to meet targets (if any) apply only when expressly stated in the Contract/Order or Cloud package appendix. This general SLA does not automatically establish an uptime commitment for every Cloud package.

3. Definitions

Term	Definition
Velra Software	The software system provided and installed by Velra under the Contract/Order
CMS	The system for managing content, interfaces, and service configuration
PMS	The hotel management system connected to Velra Software within the scope of the Contract/Order
HA	A redundancy mechanism intended to maintain or restore service operation during an incident, if deployed under the Contract/Order
On-premise	A model in which Velra Software is installed on servers and physical infrastructure owned or controlled by the Customer
Cloud	A model in which Velra provides services on Cloud infrastructure provided, leased, and administered by Velra
System Administered by Velra	The operating system, operating system administrator account, and Velra Software System installed within the scope of the Contract
Monitoring Account	A read-only account provided to the Customer to inspect resources, hardware status, and authorized logs; it has no operating system administration rights or source code access
Incident	An unplanned event that interrupts or degrades software functionality compared with the accepted specifications
Workaround	A measure that restores part or all of the business operation without eliminating the root cause
Change Request (CR)	A request for additional functionality, interface changes, integrations, or business workflows beyond the accepted scope
Business Hours / Business Day	From 08:30 to 17:30 Vietnam time, Monday through Friday each week, excluding public holidays and days off prescribed by Vietnamese law

4. System Scope and Responsibility Matrix

4.1. Systems Within Velra's Administration and Support Scope

No.	Component	Support Scope
1	Operating System	Administration, monitoring, maintenance, and updates within the scope required to support the Velra system
2	Operating System Administrator Account	Management of privileged rights, account security, and change control
3	Installed Velra Software System	Operation, monitoring, maintenance, updates, and fault handling under the Contract/Order

4.2. On-premise Responsibility Matrix

Simplified responsibility matrix notation: R (Responsible) = Party directly performing the task; S (Support) = Coordination support; C (Consulted) = Advisory role; — = Not directly responsible. Final approval responsibility shall be exercised in accordance with the Contract and the agreed change process.

Item	Velra	Customer
Operating System	R	S
Operating System Administrator Account	R	—
Installed Velra Software System	R	S
Monitoring of operating system and software status	R	S
Physical infrastructure, disks, power supply, server room, and internal network	C	R
Hardware warranty, repair, and replacement	—	R
Endpoint devices (TVs), PMS, and third-party services managed by the Customer	C	R
Customer data and business operations	S	R
Internet connectivity for the server hosting Velra Software	S	R

4.3. Cloud Responsibility Matrix

Item	Velra	Customer
Cloud infrastructure and availability within the service package scope	R	—
Operating System	R	—
Operating System Administrator Account	R	—
Installed Velra Software System	R	S
Monitoring, maintenance, and restoration under the service package	R	S
Internet connectivity and internal network at the Customer's premises	—	R
Endpoint devices (TVs), PMS, and third-party services managed by the Customer	C	R
Customer-side data, business content, and user management	S	R

4.4. Customer Monitoring Rights and Cooperation Conditions

- **Monitoring rights:** For On-premise, Velra provides the Customer with a dedicated monitoring account to inspect resources, hardware health, and authorized logs. For Cloud, Velra provides service status information and reports in accordance with the Contract;

- **Infrastructure cooperation and change conditions:** The Customer shall maintain power supply and network/Internet connectivity for the server and provide a VPN connection for Velra's remote access (for On-premise), appoint a technical contact for coordination, refrain from unauthorized intervention in the operating system/software within Velra's administration scope, and provide at least 03 Business Days' prior notice of changes to power supply, servers, networks, or PMS connectivity that may affect the system.

5. Incident Classification and Service Level Commitments (SLA)

5.1. Incident Classification and Committed Timeframes

The commitments below apply to Customers with a valid Contract or Order for services. If the Contract/Order specifies different service levels, the executed document shall apply.

Priority	Criteria and Typical Incident Examples	Response Time	Restoration Target	Restoration Measurement Schedule	Update Frequency
P1 – Critical	The entire service is unavailable, or the CMS is unavailable and disrupts the service on TVs or core functions; the HA mechanism (if any) cannot restore the service; or there is a risk of serious data loss/corruption	No more than 30 minutes, 24/7	Target ≤ 04 hours*	Continuous 24/7	At least once every 60 minutes
P2 – High	Significant service disruption: multiple devices cannot connect to Velra Software/CMS, or PMS connectivity is disrupted on a widespread basis	No more than 01 hour, 24/7	No more than 08 hours	Continuous 24/7	At least once every 02 hours
P3 – Medium	Localized fault: some devices experience an application error or a feature is unavailable; the main service remains operational	Target ≤ 04 Business Hours*	No more than 02 Business Days	During Business Hours	Each Business Day while work is in progress
P4 – Low/Request	Interface fault, configuration request, content adjustment, or user guidance.	No more than 01 Business Day	As mutually scheduled	During Business Hours	As mutually scheduled

(*) Service target, subject to the measurement principles in Section 5.2 and the suspension conditions and exclusions in Section 5.3.

5.2. Measurement Principles and Incident Severity Determination

- Response Time is measured from the time Velra receives a valid notice through a Ticket or the P1/P2 Hotline until technical personnel acknowledge receipt and begin isolating the issue; it does not mean that service has been restored.
- Restoration Time is measured from valid receipt until the affected business function is restored to a usable state through a fix or an acknowledged workaround; root-cause remediation may continue thereafter.
- P1/P2 timeframes are service targets for incidents within Velra's control and do not constitute a guarantee that every cause will be fully remedied in every circumstance. P3 timeframes are calculated in Business Hours/Business Days as defined in Section 3.
- Priority is based on actual impact: a CMS fault is not automatically classified as P1 if the TVs and core functions remain operational; PMS incidents, television stream incidents, and incidents in which multiple TVs cannot connect are assessed according to their scope of impact and cause.

5.3. Cooperation Conditions, Clock Suspension, and Exclusions

- Time spent waiting for the Customer to provide a VPN, account, logs, access permissions, a coordinating contact, change approval, ready server/power/network infrastructure, or a valid backup shall be recorded in the ticket and the applicable restoration target clock shall be suspended; the clock resumes when the required condition is satisfied.
- Disruptions caused by television channel sources, multicast, ISP, switch/VLAN/DHCP, power supply, hardware, TV devices, PMS, or third-party services outside Velra's control are not included in Velra's restoration obligations; Velra shall assist in identifying the cause and coordinating within the scope of the Contract.
- Excluded periods include notified and approved maintenance, changes made by the Customer/third party contrary to the prescribed process, force majeure events under the Contract, and other circumstances confirmed by both Parties. A Velra software fault is not excluded merely because the incident concurrently involves another system.
- **Third-party risks for Cloud:** Periods of disruption caused by the following shall not count toward the restoration target or Cloud availability metric (if applicable under the Contract/Order): (i) a widespread outage affecting a Cloud infrastructure provider, data center, public Internet backbone, or third-party platform service; (ii) a large-scale cyberattack exceeding standard protection thresholds or a newly discovered security vulnerability for which the vendor has not yet issued a fix; or (iii) a mandatory requirement imposed by a competent government authority.
- **Velra's coordination responsibility:** When a third-party incident occurs, Velra shall remain the point of contact for receipt, tracking, and status updates to the Customer and shall coordinate with the relevant provider to restore service as soon as possible.
- All suspension and resumption times, priority changes, workarounds, and confirmation results shall be updated in the ticket to enable transparent reconciliation.

5.4. Actions When Targets Are Not Met

- Velra shall provide status updates, the preliminary cause, and the remediation plan at the update frequency specified in Section 5.1. Compensation, service credits, limitations of

liability, or remedies shall apply only in accordance with the terms agreed in the Contract/Order; this SLA does not by itself create any penalty or exemption from legal liability.

6. Contact Channels and Incident Handling Process

6.1. Official Support Channels and After-Hours P1/P2 Activation

Support Channel	Contact Details	Purpose
Priority Ticket System	As specified in the Contract/Order or via email at ticket@velra.vn	The sole official channel for recording, tracking, and reconciling all requests
Hotline P1/P2	+84 794 168 368	Receipt of P1 and P2 incidents outside Business Hours

After-hours P1/P2 activation: When a P1 or P2 incident occurs outside Business Hours, the Customer shall call the P1/P2 Hotline and provide the Customer name, observed symptoms, impact level, and coordinating contact. Velra shall begin handling the incident and create or update a ticket in the system. If the ticket system is unavailable, the hotline call shall be recorded as the valid receipt time.

6.2. Handling Process, Ticket Closure/Reopening, and Root Cause Analysis (RCA)

- 1. Handling steps:** (i) Receive the request through the Ticket system (or Hotline for after-hours P1/P2 incidents) and classify it by impact level -> (ii) Isolate the scope attributable to Velra, the Customer, or a third party -> (iii) Restore operations through a workaround or fix -> (iv) Test and confirm the result -> (v) Close the ticket and record recommendations;
- 2. Ticket closure and reopening:** A ticket shall be closed when the Customer confirms completion or does not respond within 03 Business Days after Velra issues a completion notice. The ticket shall be reopened within 05 Business Days if the same symptoms recur due to the same cause;
- 3. Root Cause Analysis (RCA):** Velra shall provide an RCA report for a P1 incident within 05 Business Days after restoration (and for a recurring P2 incident upon reasonable request), including the timeline, impact, identified cause, remediation measures, and preventive actions. If the incident relates to Customer or third-party infrastructure, Velra shall still provide the timeline and technical data reasonably observed by Velra.

7. Periodic Maintenance, Change Management, and Version Lifecycle

7.1. System Maintenance and Maintenance Window

- **Maintenance scope:** Administration and security updates for the operating system; control of the operating system administrator account; and maintenance, updates, and bug fixes for the installed Velra Software System;
- **Proposed maintenance window:** 01:00–05:00 (Vietnam time);

- **Advance notice period:** At least 03 Business Days for periodic maintenance; at least 05 Business Days for changes with significant impact; and as much advance notice as practicable for emergency security patches;
- **Control of disruption duration:** The above window is the expected maintenance period and does not automatically constitute service downtime. Any disruption exceeding the notified duration shall be recorded when reconciling the applicable indicators, unless it falls within an exclusion under Section 5.3 or the Customer approves an extension.

7.2. Change Requests (CR) and Version Lifecycle

1. **Change Request (CR):** Any request for additional functionality, interface changes, or integrations beyond the accepted specifications shall be handled through a separate assessment, quotation, approval, and implementation process; the incident timeframes in Section 5 do not apply;
2. **End of support lifecycle:** Velra shall provide at least 60 days' prior notice when a software version is approaching the end of support in order to coordinate an upgrade. If the Customer continues to use an unsupported version or declines a mandatory patch, related faults shall fall outside the SLA commitments.

8. Data Backup and Restoration

8.1. Allocation of Backup Responsibilities

- **Velra's general responsibilities:** Configure the backup mechanism within the software scope, check backup status at the frequency specified by the service package, issue alerts when a backup failure is detected, and assist in restoring software/data from a valid backup;
- **For On-premise (the Customer is responsible for storage infrastructure):** The Customer is responsible for storage equipment and disk capacity and shall maintain at least 01 independent backup outside the primary server.
- **For Cloud:** Velra provides backup storage, monitoring, and restoration support according to the frequency, retention period, and RPO/RTO (if any) specified in the Contract/Cloud package. Where no RPO/RTO is specified, restoration shall be based on the most recent valid backup and does not constitute a commitment to a fixed data-loss threshold or restoration time.

8.2. On-premise Restoration Following Hardware Failure

Velra's reinstallation and restoration support time begins only after the Customer has: (i) made the physical server, power supply, and network connection available and ready; (ii) provided an accessible, valid backup; and (iii) approved the reinstallation plan. Once these conditions are satisfied, restoration of the software system shall be handled according to the priority levels in Section 5; data-copying time depends on the data volume, backup quality, and speed of the Customer's equipment and shall therefore be separately confirmed in the ticket.

9. Security, Access Rights, and Ownership

9.1. Least-Privilege Principle and Security Incident Notification

- Each individual shall use a separate named account; passwords/access keys shall not be shared through tickets or unsecured channels;
- Access rights shall be reviewed at least once every 06 months and revoked immediately following personnel changes; all material administrative actions must be logged;
- In an emergency involving human safety, property, or a requirement of a competent authority, Velra shall coordinate immediate action or grant time-limited temporary access (excluding full operating system administrative privileges), with the action recorded and the access revoked immediately upon completion;
- A Party that detects signs of unauthorized access, data leakage, or malware shall notify the other Party immediately and no later than 04 hours after confirming credible indications, in order to coordinate evidence preservation and contain the impact.

9.2. Data Management

- The Customer's operational data is owned and managed by the Customer;
- Velra shall access and process data only to the extent necessary to provide the services; exporting or copying data outside the deployment environment requires the Customer's approval.

9.3. Asset Ownership and Software Copyright

- 1. On-premise assets:** Servers and physical infrastructure funded by the Customer are owned by the Customer;
- 2. Cloud infrastructure:** Cloud resources provided or leased by Velra to operate the services are under Velra's administration;
- 3. Velra Software:** The software, source code, technical documentation, and updates developed by Velra are Velra's intellectual property. Service/license fees grant the Customer the right to use the software within the scope, term, location, and number of devices specified in the principal Contract; they do not automatically transfer the source code or any right to modify or distribute the software;
- 4. Administration does not constitute ownership:** Velra's administration of the operating system and software does not alter the Customer's ownership of On-premise hardware; conversely, the Customer's ownership of the server or use of Velra services does not create any ownership interest in Velra Software.