Service Levels and Support Policy for eComply & Verify SaaS

Incident Support Service levels

Accenture shall provide the support and maintenance for the SaaS Services as set forth in this Schedule. Accenture will use commercially reasonable efforts to perform the SaaS Services to meet or exceed the applicable Service Levels set forth below for incident response and resolution and for SaaS Services availability.

1. Support:

1.1 In scope and out of scope Support. Support types.

Level	Description	In Scope
Level 1 Support	Application Support / End User Support	No
Service Management	Available 24/7 every day of the year to receive tickets from L1 Support.	Yes
Monitoring and Alerting	Available 24/7. Sensor system that provides automated and dedicated monitoring of Key Performance Indicators. If any of the KPIs go out of range, the system alerts the Support Incident Triage Team.	Yes
Support Incident Triage	Handled by the Accenture eComply & Verify RunOps team (Incident Triage Team) and handles tickets and alerts from the Monitoring and Alerting sensors	Yes
Level 4 Support.	Core Product Support. Handled by the Accenture Product team.	Yes

1.2 Support Desk Hours:

Accenture will provide support via Accenture's eComply & verify ticketing system. The table A-1 below details the timeframes and availability of for each type of support:

UTC	CET*)	IST	MYT	EST*)	Week Day				Weekend			
00:00	01:00	05:30	08:00	19:00								
01:00	02:00	06:30	09:00	20:00								
02:00	03:00	07:30	10:00	21:00								
03:00	04:00	08:30	11:00	22:00								
04:00	05:00	09:30	12:00	23:00								
05:00	06:00	10:30	13:00	00:00								
06:00	07:00	11:30	14:00	01:00				6:00 UTC				
07:00	08:00	12:30	15:00	02:00			7:00 UTC					7.00 UTC
08:00	09:00	13:30	16:00	03:00								
09:00	10:00	14:30	17:00	04:00								On-call support during the weekend can be provided based on requests
10:00	11:00	15:30	18:00	05:00								
11:00	12:00	16:30	19:00	06:00								
12:00	13:00	17:30	20:00	07:00								
13:00	14:00	18:30	21:00	08:00								
14:00	15:00	19:30	22:00	09:00				15:00 UTC				
15:00	16:00	20:30	23:00	10:00								
16:00	17:00	21:30	00:00	11:00								
17:00	18:00	22:30	01:00	12:00								
18:00	19:00	23:30	02:00	13:00			19:00 UTC					19:00 UTC
19:00	20:00	00:30	03:00	14:00								
20:00	21:00	01:30	04:00	15:00								
21:00	22:00	02:30	05:00	16:00								
22:00	23:00	03:30	06:00	17:00								
23:00	00:00	04:30	07:00	18:00								

Table A-1

1.3. Support Service Level assumptions:

- Service Levels apply only to the Production environment of the SaaS Services and not to the non-production environment (except when support is required to effectively resolve an ongoing production incident).
- Errors, interruption, or outages in the SaaS Services caused by or resulting from Client's use of third-party software or services not approved or contracted by Accenture are excluded from the scope of the SLAs.
- Activities necessary to repair the SaaS Services which require issue analysis and fixing by the Level 4 Core Product Support is excluded from the scope of the SLAs and Service Level Targets shall not apply.
- Accenture Response Targets, as applicable, are based upon the Incident Priority Levels detailed in Table A-2 below.

1.4. Incident Classification and Response:

Accenture will make commercially reasonable efforts to maintain the quality of the service provided. However, the use of the service may result in unexpected behaviour or an observed anomaly that deviates materially from the SaaS Service specifications ("Incident"). Related Incidents are categorized into the following classification levels:

Classification	Description
P1 – Critical	The entire service is unavailable (see Service Availability) or unusable for all service use cases in client production. Example: e-invoices cannot be processed (applies to all e-invoices for a jurisdiction), all e-Invoices are not submitted to the Tax Authority as it should be, or all e-invoices are impacted by false positive validation.
P2 – High	The service is available (see Service Availability). However, the service is repeatedly unusable for majority of the use cases. Example: Majority of the e-invoices cannot be processed, e-invoices are not submitted to the Tax Authority as it should be, or e-invoices are impacted by false positive validation.
P3 – Medium	The service is available (see Service Availability). However, the service is repeatedly unusable for subset of the use cases. Example: A minor number of e-invoices cannot be processed or are not submitted to the Tax Authority as it should be, or false positive validated.
P4 – Low	The service is available (see Service Availability). However, the service is occasionally unusable for rare and not substantial use cases. Example: Specific individual e-invoices cannot be processed or are not submitted to the Tax Authority as it should be, or false positive validated

Accenture will apply workarounds, partial or full remediation on own considerations to resolve the Incidents.

For non-production services the same classification applies except the P1 - Critical as it applies to use cases only in Production environments as defined above.

Incidents are classified by Client according to their initial assessment. Accenture may reclassify based on Accenture assessment of the classification which becomes final. Accenture can also reclassify in cases where workarounds or partial fixes are leading to new classification.

1.5 Incident Support Response Times.

Prior to raising an Incident, the Client shall make reasonable efforts to analyse and resolve the observed issue when it relates to its own Client Content or its own systems e.g. data, network connectivity, etc.

The “Response Time” is dependent on the service level classification and is counted from the point in time the Incident is reported via the Accenture Ticket System. The duration of the “Response Time” means the time until the processing of the Incident is initiated which is triggering the Incident triage process.

Clients L1 Support via its Designated Client Contacts communicate with the eComply & Verify Support Centre by submitting a ticket. After submitting a ticket, the client user will receive an email confirmation that the ticket has been received by the Accenture SaaS Support team within the target time mentioned in the Table A-2. Accenture shall make commercially reasonable efforts meeting the Response Times as stated for each service level classification in table A-2.

Table A-2

Classification	Response Time	Workaround	Partial or Full Remediation
P1 – Critical	1 working hour of support*	Urgency to establish a workaround to reduce implications as soon as possible. Target workaround time P1 or reduced to P2 within 12 working hours of support	Highest priority to establish partial or full remediation as soon as possible with an urgency update. Accenture informs on the remediation progress with sufficient frequency.
P2 – High	4 working hours of support*	High priority to establish a workaround to reduce implications as soon as possible. Target workaround time P2 or reduced to P3 within 36 working hours of support	High priority to establish partial or full remediation as soon as possible either with an additional update or with the next maintenance update. Accenture informs on the remediation progress with sufficient frequency.
P3 – Medium	5 working days of support*	Typical the focus is on partial or full remediation; potential workarounds might get applied	Medium priority to establish partial or full remediation aimed to be delivered with next maintenance update.
P4 – Low	20 working days of support*	Typical the focus is on partial or full remediation	Low priority to establish partial or full remediation with a future release or update
**In accordance with the SaaS Support Triage Team timeframe as detailed in Table A-1*			

Targeted response and resolution/workaround times are indicative and may be influenced by volume, severity and root cause of Incidents raised.

The response and resolution/workaround time apply for both production and none-production environments. Workaround and Remediation of production Incidents are prioritized over non-production Incidents as needed. The response and resolution/workaround time does not apply for any preview, beta, or pilot version of the SaaS service.

If Accenture deems an Incident as feature request, there is no obligation to respond or resolve such feature request under this response and resolution/workaround time or to include such feature request in the next release. However, Accenture may note such feature requests for potential future consideration.

1.6 Language

Accenture operates and provides the eComply & Verify SaaS Support Service and related collateral in English; however, Accenture is enabled to communicate also in local language to clients in countries where Accenture locally operates as an additional offering subject to additional fees.

1.7 Escalation

If there is no response by Accenture within the timeframes specified in tables A-1 and A-2, the client may escalate. If the first or any previous escalation level is not available or requires further escalation, the Client may escalate to the next level within the eC&V SaaS Support Service:

- Escalation Level 1: Help Desk
- Escalation Level 2: Sr. Manager – Technical Operations
- Escalation Level 3: Director – Technical Operations

2. EC&V Support Team Internal Monitoring of the SaaS Service

This section describes the way the eC&V SaaS Support team monitors eComply & Verify Service in production environments.

2.1 Accenture eC&V SaaS Support Team

Accenture will have a dedicated eC&V SAAS Support team to internally maintain and monitor the eComply & Verify service up and running as expected. For clarity, the monitoring systems are internal to Accenture and therefore only the eC&V SaaS Support team shall have direct access to said system.

a) Status Tracking and Notification

eComply & Verify will monitor transaction statuses at individual level to track performance and detect possible exceptions.

Status tracking will be standardized across multiple jurisdictions. This enables updates on:

- The progress of invoices as they flow through their lifecycle.
- Accurate and standardized error handling.
- Supporting data jurisdictional residency and data processing requirements.

b) Monitoring of the SaaS Services

The processing engine will provide monitoring of the status, performance and availability of e Comply & Verify 24/7. Monitoring will occur programmatically and will raise automatic internal warning and alert messages to the eC&V SAAS Support team.

Monitoring will allow to provide metrics about:

- The processing progress of invoices (inbound, processing, outbound).
- Errors and Warnings detected / Debug data being loaded.
- Global availability per region and jurisdiction.
- Technical components such as databases, queues and batch processing, response.
- Version and configuration tracking
- Performance KPIs.

3. Service Availability:

The following sections describe how the Service Availability of the eComply & Verify Service is defined from the client production usage with business go-live and start of the CTC Mandate for the jurisdiction in scope until the termination of the eComply & Verify Service.

3.1 Definition of Service Availability:

The Service Availability (REST API Endpoint availability) is considered as available when:

1. the REST API Endpoints can be reached; and

2. is responding as per its definition published at the eComply & Verify document portal.

3.2 Measuring of the Service Availability:

Service Availability % = (Agreed Service Time – Unplanned Downtime) / Agreed Service Time

Agreed Service Time: 24/7 within a month. Calculates as: 24 x number of days within a month minus Managed Downtime for that month.

Unplanned Downtime: Elapsed unplanned downtime within a month. Unplanned downtime starts with the event which is reported earliest, a detection by service monitoring or reported downtime by consumers of the service. Unplanned downtime ends with the event which is reported earliest, detection by service monitoring or reported resolution by consumers of the service.

Managed Downtime: Accenture will apply required changes and security patches on a regular basis. This is managed within service maintenance windows and considered as managed service downtime. Client acknowledges that depending on the nature of the deployed changes the service availability might be affected within the thresholds described in the table below which shall not be considered as Unplanned Downtime.

Downtime Duration	Maximum Frequency
Below 10 minutes	1 event per hour 5 events per day 10 events per week
between 10 minutes and 20 minutes	1 event within month 3 events within a year
more than 20 minutes	1 event per year

3.3 Commitment on Service Availability

Accenture will make reasonable efforts to achieve the Service Level availability of >= 99.99% within a year and >= 99.95% within a month, however, does not guarantee the service availability.

The eComply & Verify service is supported by an internal monitoring service which is consuming the API endpoint with a test request from outside, from different locations and routing. This availability check is executed every 5 seconds with three retry attempts with retry wait time of 20 seconds. Downtime is recorded as soon the check fails with error code 504/503 and ends once the check is recorded successful. Downtimes in between 2 checks (< 10 seconds) will not be detected by the monitoring service.

In cases where the monitoring service itself is not available, for example for maintenance reasons, the downtime is measured based on the consumer reported status.

3.4 Reporting of the Service Availability

Reports on the service availability can be requested via a service ticket. The report is made available based on the service ticket for the requested timeframe.

3.5 Service Maintenance Windows

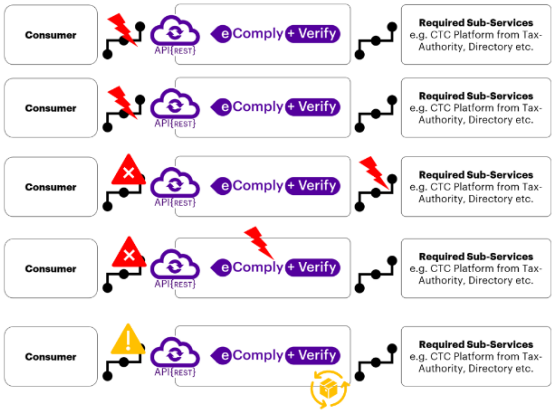
To keep the service up to date in accordance with Accenture's product internal development cadence, changes and security patches are required and planned on a regular basis:

Standard Maintenance Windows:

- Weekly: Saturday 07am UTC, up to 2 hours
- Monthly: 2nd Saturday of each month 07am UTC, up to 4 hours

Ad-Hoc / Hot fixes, for example, for critical issue resolution or urgent security fixes will require a forced maintenance window with potential managed service downtime on short notice outside of the standard schedule.

3.6 Example Scenarios of the Service Availability



Consumer is observing potential scenario	API Endpoint Available	Description
End-Point can not be reached by a consumer	YES	End point can be reached by others but not from a single consumer
End-Point can not be reached by consumer / no feedback send	NO – unplanned downtime	End point can not be reached at all / no feedback is send
eComply & Verify end-point connection error response	YES	e.g. CTC Platform End-Point can not be reached after retries. eComply & Verify restricts receiving new messages
eComply & Verify end-point processing error response	YES	eComply & Verify fails on processing a request.
eComply & Verify end-point maintenance response	Managed down-time	eComply & Verify is in service maintenance window which requires to restrict receiving new messages

To meet and exceed the SAAS Services availability SLA expectations, and in addition to the Standard Maintenance Windows described above, periodic ongoing maintenance in the SaaS Service is a required procedure. Such maintenance will sometimes render the SaaS Service unavailable amounting to Scheduled Downtime. Accenture will take commercially reasonable efforts to minimize "**Scheduled Downtime**" which must (A) not exceed 12 hours in any month, (B) only occur after Accenture has provided Client with at least one weeks' notice (e-mail permitted) and any maintenance that does not comply with such requirements will not be considered Scheduled Downtime. Scheduled Downtime and unscheduled downtime may be communicated through Accenture's Service Point of Contact through to Client's Point of Contact or following the procedure mutually agreed during the SaaS Service enablement. For avoidance of doubt, Scheduled Downtime shall not include application release maintenance (e.g. downtime required to upgrade the core SaaS service to a new release). In any case, application release maintenance will only occur after Accenture has provided Client with at least two weeks' notice (e-mail permitted) and Accenture will provide client with the option to test the new release prior to production deployment into a separate user acceptance test environment.

4. Support terms:

4.1. Updates. Accenture may, in its sole discretion, issue Updates to the SaaS Services from time to time according to its development schedule, for which it maintains exclusive control, provided always that Accenture shall not be entitled to apply such Updates in a manner that would make the SaaS Services materially non-conforming with the applicable service descriptions, or otherwise materially diminish the scope or the quality of the service provided, unless such changes are necessary for Accenture (at Accenture's discretion) to comply with any applicable laws. All such updates and changes shall be provided to Client without additional charge. Accenture is under no obligation under this Agreement to provide any Updates to the SaaS Services. If Accenture does generally release an Update to the SaaS Services, it will apply the Update to the SaaS Services according to its implementation schedule but will not unreasonably delay implementing any Update for Client. Notwithstanding the foregoing, Accenture may provide Client with prior notice of any such Update in accordance with this Service Order, other than for updates and changes developed and released in response to urgent security or operational incidents with the SaaS Services. Accenture will make commercially reasonable attempts to make Updates to the SaaS Services

during periods of Standard Maintenance Windows and Scheduled Downtime. Accenture will inform Client if it knows that any Updates may require material changes to Client configuration or use of the SaaS Services to implement. In such event Accenture will facilitate client a test environment to complete analysis, testing, problem definition and ticketing as part of the Update or upgrade process. Accenture is accountable for SaaS Services testing and Client is accountable for user acceptance testing of the Updated or customized solution. Client is responsible for all aspects of updates or upgrades associated with Client systems external to the SaaS Services

4.2. Technical Support. Technical support consists of (i) access to Accenture's support help desk for Incident reporting via e-mail or Telephone (only for Priority 1 Incidents, such as SaaS Services not being available or accessible); (ii) attempted diagnosis of reported Incidents in the SaaS Services and (iii) reasonable commercial efforts to resolve reported Incidents.

4.3. Contact Information: Help Desk Contact Information:

Telephone +1 646 254 3537 / +1 855 594 9151

4.4. Incident Reporting:

Designated Client Contact(s) (to be agreed with Accenture) shall promptly notify Accenture of any suspected Incidents. Such notification must include, at a minimum, the following information which may be updated by Accenture upon written notice:

- Name and contact information of the Designated Client Contact sending report (email and phone)
- Client name and, if applicable, location
- Initial analysis by Client's internal help desk
- A description of the issue, error messages received, etc.
- Steps taken by Client to reproduce the issue, if applicable, include screenshots
- Activity being performed at the time of the issue.
- Client impact (a description of the business impact caused by the product issue)
- Client's identification of the Priority Level

If a Designated Client Contact neglects to provide any such forgoing information, Accenture shall prompt such individual for all such needed information. Accenture may use such information solely to provide correction services in accordance with this Agreement.

Accenture will track all reported Incidents with an incident identification number ("Incident ID"). Accenture will track all information and correspondence related to the Incident with the Incident ID, which Accenture will share with Client for tracking purposes.

4.5. Notification:

Accenture will provide appropriate downtime notifications to a limited number of Designated Client Contacts. Client is responsible for providing customer service (if any) to Authorized Users, including internal communications on planned or unplanned downtime to these Authorized Users. Accenture does not provide any support or services directly to Authorized Users.

4.6. Root Cause Analysis:

For any failure of Accenture to meet any Service Level herein (each, a "Service Level Default"), Accenture shall perform an analysis of the underlying problem to formally identify, and share with Client on the SaaS Service, the "root cause" of such Service Level Default ("Root Cause Analysis").

4.7. Exclusive remedies:

As its exclusive remedy relating to SLAs, Client's may terminate this Agreement if (a) SaaS Services availability is less than 90% in three consecutive months or (b) SaaS Services availability is less than 75% in any month