Planisware

Version February 12th 2026

APPENDIX I –SAAS SUPPORT POLICY

This Planisware SaaS Support Policy ("**Support Policy**") describes Planisware's technical support offering for SaaS Services. This Support Policy is an exhibit to Planisware General Terms and Conditions ("**GTCs**") and forms part of the Agreement as defined therein. This Support Policy shall be updated with each major Service release Update with terms no less protecting for the Customer.
Capitalized terms are defined in this Support Policy or in the GTCs.

1. SYSTEM ACCESS

Planisware maintains and provides all required infrastructure and network components for the delivery of the SaaS Service to Customer, including disk storage space to allow full and proper installation and operation of the SaaS Service.

End-Users must connect to the Service with an approved browser as listed in the Planisware version compatibility browser matrix, which can be found in the Documentation at https://myportal.planisware.com and which may be updated from time to time. The SaaS Service is accessed using the Hypertext Transfer Protocol Secure (HTTPS). The SaaS Service supports the following protocols for each type of data exchange:

For file exchange: SFTP / HTTPS

For web services (over HTTPS): ODATA / SOAP / REST

Planisware will, in consultation with Customer, provide to the Customer a dedicated Internet domain name and URL managed by Planisware for the Service (such as https://customer_choice.planisware.live). Planisware shall not be liable for any failure to obtain a particular URL if this is due to circumstances outside Planisware's reasonable control (for example, because that URL has already been allocated for another resource or project).

Planisware will provide sufficient bandwidth access to ensure that End-Users can obtain access to the SaaS Service at all times without unreasonable delays or interruptions in downloading, viewing or uploading data from or to the SaaS Service. Planisware is not responsible for any access or performance issues caused by Customer's or End-Users' devices, internet connection service, hardware, software or security measures that may restrict access to the SaaS Service.

2. CUSTOMER DATA HOSTING AND BACKUPS

The SaaS Service provides limited storage space for Customer's Data as specified in the Order Form. Customer can request additional storage for files and documents subject to a separate SOW. Planisware will use reasonable efforts to notify Customers when their storage usage reaches approximately 90% of the applicable limit.

Planisware makes daily backups of Customer Data. In addition to any backup restoration for disaster recovery purposes, Planisware will restore backups to Customer's database as set forth in this Support Policy.

3. UPGRADES

From time to time, Planisware will implement Upgrades. "**Upgrade**" means a new version of the SaaS Service in either a major or minor release. An Upgrade is conventionally indicated as an increased version number (including post decimal increases for minor releases).

Planisware will deliver at least one Upgrade per calendar year, at no additional cost to Customer, provided that (i) configurations will be migrated to the new version as-is and (ii) new modules or features included in an Upgrade will be standard and not configured, unless any such configuration is mutually agreed under a SOW subject to additional costs. Such annual Upgrade is mandatory, and Customer may not request to continue to use an outdated version of the SaaS Service, subject to the exceptions below.

Upgrades may result in changes to the appearance and/or functionality of the SaaS Service. However, Upgrade will not materially diminish or impair the functions of the SaaS Service.

Planisware will give Customer at least 20 business days advanced written notice before the implementation of any Upgrade. Planisware may provide Customer with access to an Upgraded environment (when available) in which to test the Upgrade before it is pushed to production for a maximum period of 20 business days. Customer will notify Planisware during this testing period of any material diminishment or impairment of the functions of the SaaS Service, and Planisware shall resolve such notified issues. Customer may decline an Upgrade only if the Upgrade is found to cause a Priority 1 or Priority 2 incident without a workaround, as defined in the Incident Management Rules (Article 5) below, and Customer shall accept the Upgrade once the Priority 1 or Priority 2 incidents have been resolved in accordance with the Incident Management Rules. In the event where an Upgrade is found to cause a Priority 3 or Priority 4 incident, as defined in the Incident Management Rules, Planisware will respond in accordance with such Incident Management Rules, unless Customer and Planisware agree to address such incidents under a separate SOW.

The release lifecycle milestones are defined in the product roadmap communicated to the Customer (general availability, end of life and end of support with corresponding incident management obligations).

4. TERMINATION OR EXPIRY OF THE AGREEMENT

Upon termination or expiry of the Agreement, Planisware shall make available to Customer, upon written request, a database back up of Customer Data (for any other format, the Parties shall sign a SOW). Planisware retains Customer Data for a maximum of 30 days after the termination or expiry date and the written request must be made within such 30 days. Planisware has no obligation to retain Customer Data and may delete Customer Data after such 30-day period. Upon termination of the Agreement, Planisware's sole responsibility with respect to Customer Data shall be limited to providing such export of Customer Data back-up.

5. SERVICE LEVEL AGREEMENT ("SLA") AND INCIDENT MANAGEMENT

5.1 Technical support

Planisware will provide technical support on the SaaS Service per Article 5.2 (SLA) and Article 5.4 (Incident Management Rules). **Support is limited as follows**:

1. Technical support is only accessible to certain End-Users identified by Customer (typically users with administration profile)and not to all End-Users.
2. Support does not include consulting or training with respect to functional use or configuration of the SaaS Service.
3. The SLA only applies to the use of the SaaS Service in Customer's production environment only and only after the Go Live date. The SLA does not apply to use of the SaaS Service in non-production environments when available (e.g., testing or training environment).
4. The incidence response plan of the SLA applies to the Customer's production environment only. Incidents within other non-production environments (e.g., testing or training environment) will not be covered by the incident management requirements defined below.
5. Support will be provided during business hours, depending on Planisware signing entity, as stated in the Order Form:
   - Planisware S.A (also applicable to Planisware UK and Planisware Belgium): 9 a.m. to 6 p.m. (CET) during business days excluding local national holidays ;
   - Planisware Deutschland GmbH: 9 a.m. to 6 p.m. (CET) during business days excluding German national holidays and bank holidays in Bavaria ;
   - Planisware USA Inc: 9 a.m. (EST) to 6 p.m. (PST) during business days excluding US bank holidays ;
   - Planisware Singapore PTE. LTD.: 9 a.m. to 6 p.m. (SGT) during business days excluding Singapore national holidays ;
   - Planisware Japan KK : 9 a.m. to 6 p.m. (JST) during business days excluding Japan national holidays.
6. The SLA and Incident Management rules shall not apply to performance/availability issues caused by the following:
   - Overall internet congestion, slowdown, or unavailability.
   - Unavailability of generic internet SaaS Services (e.g. DNS servers) due to virus or hacker attacks.
   - Force majeure event as described in the GTCs.
   - Actions or inactions of Customer or third parties beyond the control of Planisware.
   - A result of Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Planisware.
   - Configuration(s) created or modified by Customer or by a third-party on Customer's behalf. Planisware will address those Incidents only if requested by Customer and subject to an amended or separate agreement.

5.2 SLA

Measure / Name	Definition	Requirement
Availability	Total Availability: total number of minutes in any calendar month minus Permitted Downtime for such calendar month. Actual Availability: The percentage of Total Availability in a calendar month that the SaaS Service is available for use by End-Users in Customer's production environment accessible via internet protocols.	Actual Availability of 99.5% in each calendar month (excluding permitted downtime)
Permitted Downtime	Measure of the aggregate amount of time in a calendar month during which the SaaS Service is not available due to: ➢ Regular maintenance (e.g., regularly scheduled outage without a required notification) ➢ Scheduled maintenance (e.g., upgrade or other ad-hoc downtime planned with sufficient notification to Customer) ➢ Emergency maintenance, including response to immediate security threats, and preventative or corrective measures required to adhere to contractual security and business continuity obligations and applicable law. ➢ Circumstances beyond Planisware's reasonable control, including, but not limited to: - Computer, telecommunications, internet service provider or hosting facility failures - Acts of government, flood, fire, earthquakes, acts of terror, strikes or other labor problems (other than those involving Planisware employees) - Delays involving hardware, software or power systems not within Planisware's possession or reasonable control, and denial of service attacks - Other activities Customer directs, - Changes resulting from government, political, or other regulatory actions or court orders, and/or - Customer's failure to respond where an incident requires Customer's participation for resolution - End-User connectivity issues	➢ Regular maintenance: on Sundays mornings (up to four hours every week-end unless otherwise agreed by the Parties). ➢ Scheduled maintenance: Customer will be notified at least 5 business days in advance, and Planisware will use its best commercial efforts to schedule the outage to minimize impact to the Customer. ➢ Emergency maintenance: may be applied without notice in the event of a credible security threat; Customer will be notified upon the emergency maintenance or as soon as possible thereafter, depending on the severity of the threat. This includes time necessary for the restart of the application after emergency issue is addressed.
Disaster maximal data loss guarantee (RPO)	Maximum amount of data loss from the point of a disaster	No more than 24 hours of data loss
Return to Operations (RTO)	Timeframe to restore service after an unscheduled interruption excluding Disaster.	No more than 12 hours (standard)
Customer requested backup restoration	Measures the time from recovery request to recovery	Restore backed up of complete set of Customer Data within 4 business hours of request by Customer to restore backup. Time of restoration of partial Customer Data set will depend on complexity of request and may require additional Permitted Downtime of up to 4 hours and may be subject to a separate Service Order.
Non-production environment Customer Data refresh	Customer Data database restoration onto a non-production environment (e.g., test, training.).	3 business days after written request and limited to 6 requests per year per non-production environment.

SLA Time Measurement Rules

The SLA clock for an incident begins at the time the incident is first recorded in the service management system by either the customer or the service provider.. It may be paused during customer dependencies, third-party delays, or scheduled maintenance.

Clock Pause / Suspension:

The SLA timer may be paused in the following cases:

1. Awaiting Customer Action – e.g., when additional information, approval (release to test, to prod..) confirmation (on test or prod), or system access is required from the customer and the provider is unable to proceed.
2. Third-Party Dependency – e.g., when resolution depends on another vendor or external system outside the provider's control.

3.Scheduled Maintenance or Agreed Downtime – time during approved maintenance windows is excluded from SLA calculation.

5.3 CONFIGURATIONS MADE BY CUSTOMER OR A THIRD-PARTY APPOINTED BY CUSTOMER

SLA is not applicable to incidents, unavailability, performance issues or post-upgrade regressions that, upon investigation carried out by the Customer or a third party appointed by the Customer have not as determined root cause, Planisware's direct performance, liabilities or omission. Nevertheless, Planisware can be requested, subject to a dedicated SOW, to investigate and attempt to fix such configurations. In conformity with clause 9.1, Planisware's liability cannot be triggered regarding damages caused to Customer and arising from Customer or a third party 's act or omission (including but not limited to damages arising from Customer supplier's or subcontractors creation or modification of configurations).

5.4 INCIDENT MANAGEMENT RULES

Planisware's support team shall be available and shall respond to incidents as set forth in the chart below.

Support Level	Priority 1 (P1)	Priority 2 (P2)	Priority 3 (P3)	Priority 4 (P4)
Support Availability	24h/7days per week	Business Hours	Business Hours	Business Hours
First Response	Within 1 hour of incident being reported	Within 2 hours of case being reported during Business Hours	8 hours of case being reported during Business Hours (acknowledgement only)	8 hours of case being reported during Business Hours (acknowledgement only)
Follow Up Responses	Every 2 hours from report of incident until incident is resolved	Every Business Day	N/A	N/A
Resolution of Incident (including via a temporary workaround solution)	Within 8 hours of report of incident	Average 2 and maximum 5 Business Days	In a future release	In a future release

*Business Hours/Days as defined in Article 5.1

Incident Priorities are defined as follows:

Scope of Incident	SaaS Service Unavailable	SaaS Service available and usable but: (1) performance is degraded causing an inability to complete a desired process in a reasonable time frame. (2) Major Functionality* not available or not functioning and no work-around is available	SaaS Service available and usable but: (1) performance is slightly degraded. (2) Major Functionality* not available or not functioning but work-around is available (3) Non-Major Functionality* not available or not functioning and no work-around is available	Non-Major Functionality* not available or not functioning Cosmetic issue or issue that has no impact on usability of the SaaS Service or ability to complete a process
System-wide	P1	P2	P3	P4
Impact on more than 25% of End-Users	P2	P2	P3	P4

Multiple End-Users with no established pattern	P3	P3	P3	P4
Single End-User	P3	P4	P4	P4

***"Major Functionalities"** means the critical functions of the SaaS Service as determined between the Parties prior to the Service go live date in the SOW. Upon execution of a SOW for Professional Services providing for the development and implementation of any configuration of the SaaS Service, the Parties may agree on the addition of corresponding new Major Functionalities.