Planisware

Version February 12th 2026

APPENDIX II – PLANISWARE SECURITY MEASURES

This Exhibit presents the architecture, infrastructure and security policies and standards of the Planisware solutions, which are all applicable to SaaS Services. The security measures applicable also to On Premise Products are strictly identified in a dedicated part at the end of the present Exhibit. For the avoidance of doubt, provisions not identified as applicable also to On Premise Products are only applicable to SaaS Products.

PROVISIONS ONLY APPLICABLE TO SAAS PRODUCTS

SOLUTION ARCHITECTURE

DATACENTER MANAGEMENT

Planisware owns and manages the physical components related to its Planisware SaaS service in datacenters. Planisware's datacenters are defined as "Planisware Ping Power Pipe" or "4P" datacenters which provide remote access to servers, power, and internet connections.

Planisware leverages private space from host colocation centers that provide a physical environment and basic services such as:

- Physical security management (perimeter security, physical access control)
- Supply of energy
- A/C
- Management of network links between Planisware computer arrays
- The provision of WAN connections (Internet access, specialized links)

Planisware's 4P enables general server management and all SaaS services to be provided directly by Planisware.

Customers may choose where their data is stored among locations offered by Planisware. By default, the data is stored as follows:

Localisation of the Customer	Data storage
Europe	European Union
Switzerland	Switzerland
Africa	European Union
Middle East	Switzerland
United States	United States
Asia	Singapor
Other	In a location chosen by Planisware, and in compliance with all applicable laws governing the protection of Personal Data

Data Centers are SSAE16 and/or ISO27001 certified. Solutions are supported by full-time onsite engineers and secured 24/7/365 by audited security personnel, badge/photo ID access screening,

biometric access screening, motion sensors and security breach alarms. Remote access to servers is available exclusively via Planisware internal IPSec VPNs. In addition to VPN, Planisware authorized staff members have network and credential access to production servers.

END-USER DEVICES AND DATA EXCHANGE

Web traffic between Planisware servers and external systems is encrypted using TLS (HTTPS), depending on the end user's browser's cipher suite support. Planisware supports Site-to-Site IPsec VPN for integration with external systems on shared network devices, providing AES-256 encryption of data in-transit between sites.

SECURITY MEASURES

HUMAN RESOURCES SECURITY

A cursory background check is included in the Planisware employee recruitment process. Subject to local applicable laws, Planisware may conduct further background checks. All resources are trained on security measures and procedures on a regular basis.

IP-BASED ACCESS RESTRICTION

If specified in the Financial Terms or a dedicated purchase order, Customer's access to the application may be managed at the Firewall level to limit the set of end users that can access the application to a specific IP subnet.

ENCRYPTION

Planisware uses cryptographic algorithms that are in line with the sensitivity of the data to be protected, with the current encryption regulations imposed per country, and with the recommendations of governmental security bodies.

Data in Transit

Web traffic between end users and servers is encrypted using TLS (HTTPS) depending on the end user's browser's cipher suite support.

File exchanges with external systems can also be encrypted using PGP or according to other customer requested standards. For non-secure protocols, Planisware SaaS product supports Site-to-Site IPsec VPN for integration with external systems.

Data at Rest

Planisware provides two level of data encryption. Database partition encryption is the default of our SaaS platform:

- Database file is mounted on an encrypted partition.
- Encryption-decryption of the partition is done by Planisware , when starting the application.
- The encryption key is present only in the memory of the Planisware Server, never stored on the application server disk, so that it's impossible to decrypt the partition when the Planisware's Server is stopped.
- The key is encrypted and exchanged with the application server from a key server located in a different data center.
- Database partition encryption is done via symmetric encryption AES-XTS with a key size of 512 bits.

Data encryption in the database:

Depending on attributes usage in the database, encryption is done either with symmetric encryption AES-ECB with a key size of 256 bits or with symmetric encryption AES-CBC with a key size of 128 bits.

ACCESS LOGGING

Planisware maintains a time stamped log file of the following activities:

- When an end user is connected
- Pages of the application visited by end users

Updates made to customer's data by end user is also tracked and can be available for forensic analysis. Customers can also create their own audit trail by configuring traces in the application. This way they can track and access real-time reports on, for example, who changes a specific attribute and when.

For additional control, customers can configure enforceable workflows in the application, ensuring that key data updates are controlled by a RACI-defined approval processes.

DATA SEGREGATION

Our Planisware SaaS solutions leverage a combination of component options that include PostgreSQL database, Apache web server, and Linux OS. Planisware SaaS is a single tenant solution. Client data is isolated and segregated from one client to another through:

- Dedicated VM(s) containing all components
- A dedicated database with dedicated access credentials
- A dedicated VLAN

SEGREGATION OF DUTY

Planisware follows segregation of duty principles and enforces a strict end user profile by a responsibility assignment matrix. The customer production environment is only accessible to:

- the Incident Response Team (without access to Customer Data),
- Support Team, to act on an issue (without access to Customer Data, unless otherwise authorized by Customer),
- the Planisware Delivery Manager, to deploy a change to production as requested by customer
- the Technical Delivery Manager (without access to Customer Data), for server configuration
- the Planisware System Administrators, as required to address unexpected major incident.

These roles are audited regularly, and all assignment extensions, revocations or creations are tracked in a ticketing system.

VIRUS AND MALWARE PROTECTION

A layered security approach has been implemented according to the logic of Defense in depth:

- Customer environments are on Linux OS servers with an antivirus.
- An antivirus is installed on Planisware workstations accessing Planisware SaaS.
- As part of the alert and incident management process, malware risks are regularly monitored.
- Planisware partitions infrastructure and applications. Firewalls filter communications between components in different zones. All components are updated regularly and monitored to ensure they are on the latest update version.

SOFTWARE AND SYSTEM PATCHES

Customer environments receive automatic Linux updates for OS security patches. As part of the alert and incident management process, the Chief Information Security Officer (CISO), asset managers, and the infrastructure manager for Planisware SaaS review security risks on a regular basis, leveraging the following security alerts:

- From the CERT-FR (ANSSI), CERT-US;

- From publishers, builders and subcontractors;
- Detected by the administrators (via events located in traces and alerts raised by the Planisware SaaS infrastructure team);
- From cybersecurity agencies, clubs and media;
- Released by Planisware SaaS Hosting datacenter providers;
- Identified while running the Safety Control Plan.
- Identified while running external audit

After identifying and assessing the risks resulting from the monitoring and alert system, safety patches are applied as soon as possible (after validation of the action plan) or deployed depending on the severity of the risk.

NETWORK SECURITY

Planisware configures all network infrastructure according to the principle of "least access" by including filters that allow only the minimum required traffic. All communications between the web server and the clients over the Internet are encrypted using TLS depending on the end user's browser's cipher suite support.

Planisware SaaS leverages:

- Secure protocols only (HTTPS, SFTP, IPSec)
- Web application firewall monitoring HTTP requests
- Firewall log monitoring for inbound and outbound network flows
- Intrusion Detection System (IDS) to monitor and block malicious traffic and attacks on network traffic.

DATA BACKUP

Our standard Planisware SaaS offering includes backups for the customer's production environment only. Data backup services are described in the table below.

Data to backup/perimeter	Frequency	Retention rules	Backup type	Means of protection	Localization	Responsible	Offsite storage
Customer database backup	Daily	By default: Last 10 days Last 6 weeks (1st day of each week) Last 6 months (1st day of each month) Option(s): according to customer requirements	Full	Encrypted dump Encrypted transfer	Database backup platform of customer environments	Planisware	Yes
Full backup of virtual machine	Incremental each day	At least 15 days (minimum retention period)	Increm ental	Encryption	NAS	Planisware	Yes

As a base option, a customer data backup is generated on-site and off-site, daily per the backup process described above. In the event of a disaster at the main site location, the main site infrastructure is restored first, then the environment is restored. On top of the daily backup for production environments, customers may opt, at cost, to add a warm-backup option where a copy of the environment and database is replicated off-site in a passive environment, on standby. In the event of a disaster at the main site location, the passive site can be activated with limited interruption to service.

BUSINES CONTINUITY PLAN AND DISASTER RECOVERY PLAN

Planisware's Business Continuity Plan (BCP) addresses:

- Impacts on business processes,
- Thresholds of activation,
- The organizational roles and functions of the respondents (members of the crisis unit),
- Internal and external communication plans,
- Operating principles in emergency mode,
- Return to normalcy.

Planisware's BCP includes the IT-backup plan procedures as well as the Disaster Recovery Plan (DRP).

VULNERABILITY TESTING

VULNERABILITY SCAN

Vulnerability scans are performed on a regular basis. Web pages are served using the HTTPS protocol only.

PENETRATION TESTING

An independent security auditing company is contracted by Planisware to conduct penetration testing once a year. Annual penetration test certificates are available upon request.

APPLICATION SECURITY TESTING – ALSO APPLICABLE TO ON PREMISE PRODUCTS

OWASP application security risks are reviewed, assessed and included as part of Planisware's testing suites.

PROVISIONS APPLICABLE TO ON PREMISE PRODUCTS AND SAAS PRODUCTS

END-USER IDENTIFICATION AND AUTHENTICATION

End-User accounts are managed directly by the client within our solution. Within the application, customer's administrator can assign each end user a specific profile and authorization level that defines access to modules, functionality, and data rights. Authentication must be managed by the client via Single Sign On (SSO), leveraging the SAML 2 or Open ID Connect (OIDC) web-based authentication standard.
For system accounts, for example to interface with external systems, passwords are stored using an encryption algorithm. **Using SSO**, end-users passwords are not stored nor managed in the solution.

PROFILE-BASED ACCESS CONTROL

Once an end user is authenticated, access to the application is further restricted via multi-level authorization access layers. Access is defined according to the following dimensions:

- Per module, based on end user profile
- Per screen within a module, based on end user profile
- Per feature within the module, based on end user profile
- By data element based on end user profile AND/OR specific user rules

User profiles provide application-level segregation of duties. They can be created, updated, and managed in the application by a Customer business administrator. Changes to a given end user profile automatically propagate to all end users with that given profile.

Planisware

Version February 12th 2026

AUDITS

Planisware's data centers and other premises are ISO27001 certified or SOC 2 Type II certified. SOC1/SOC2 reports and the ISO27001 compliance certificate are usually available at the beginning of each calendar year. Planisware may share such certificate upon Customer's reasonable request.

INTERNAL POLICIES

Planisware has implemented an Information Security Management system (ISMS) in accordance with ISO- 27001:2013. This approach focuses on:

- Defining and sharing clear security objectives,
- Raising security awareness amongst Planisware employees,
- Creating a framework for security management,
- Using a risk management framework,
- Monitoring security measure effectiveness through internal and external audits,
- Creating a framework to manage security alerts and reduce security incidents.

PRIVACY COMPLIANCE

Where it is established Customer has End Users within the European Economic Area, Planisware requires the signature of its Data Processing Agreement governing the processing of such end users' personal data, including the signature of EU Commission Standard Model Clauses. Additional Data Processing Agreements are executed for processing of data subjects located in other jurisdictions as required (e.g., California, Brazil). Upon request, it is possible to set up privacy zone rules for categories of end users. Personal data are encrypted on the fly for all end users not sharing the same privacy zone.

Planisware's Data Protection Officer (DPO) can be contacted at dpo@planisware.com.