Planisware

Version : 12 février 2026

ANNEXE II : MESURES DE SÉCURITÉ PLANISWARE

La présente Annexe décrit l'architecture, l'infrastructure ainsi que les politiques et normes de sécurité des solutions Planisware, toutes applicables aux Services SaaS. Les mesures de sécurité également applicables aux Produits On-Premise sont strictement identifiées dans une partie dédiée à la fin de la présente Annexe. Pour lever toute ambiguïté, les dispositions non identifiées comme étant également applicables aux Produits On-Premise sont uniquement applicables aux Produits SaaS.

DISPOSITIONS UNIQUEMENT APPLICABLES AUX PRODUITS SAAS

ARCHITECTURE DE LA SOLUTION

GESTION DES DATACENTERS

Planisware possède et gère les composants physiques liés à son Service SaaS Planisware dans des datacenters. Les datacenters de Planisware sont définis comme des datacenters « Planisware Ping Power Pipe » ou « 4P », qui fournissent un accès à distance aux serveurs, à l'alimentation électrique et aux connexions Internet.

Planisware utilise des espaces privatifs de datacenters d'hébergement mutualisés qui fournissent un environnement physique et des services de base tels que :

- La gestion de la sécurité physique (sécurité périmétrique, contrôle d'accès physique)
- L'alimentation en énergie
- La climatisation
- La gestion des liaisons réseau entre les baies informatiques de Planisware
- La fourniture de connexions WAN (accès Internet, liaisons spécialisées)

Le modèle 4P de Planisware lui permet d'assurer directement la gestion générale des serveurs et la fourniture de l'ensemble des Services SaaS.

Les Clients peuvent choisir le lieu de stockage de leurs données parmi les emplacements proposés par Planisware. Par défaut, les données sont stockées comme suit :

Localisation du Client	**Stockage des données**
Europe	Union européenne
Suisse	Suisse
Afrique	Union européenne
Moyen-Orient	Suisse
États-Unis	États-Unis

Asie	Singapour
Autre	Dans un lieu choisi par Planisware, conformément à l'ensemble des lois applicables en matière de protection des Données Personnelles

Les datacenters sont certifiés SSAE16 et/ou ISO27001. Les solutions sont prises en charge par des ingénieurs sur site à temps plein et sécurisées 24h/24, 7j/7, 365 jours par an par du personnel de sécurité audité, un contrôle d'accès par badge/photo d'identité, un contrôle d'accès biométrique, des détecteurs de mouvement et des alarmes de violation de sécurité. L'accès distant aux serveurs est disponible exclusivement via les VPN IPsec internes de Planisware. En complément du VPN, les membres du personnel autorisés de Planisware disposent d'un accès réseau et d'identifiants d'accès aux serveurs de production.

APPAREILS DES UTILISATEURS ET ÉCHANGES DE DONNÉES

Le trafic web entre les serveurs Planisware et les systèmes externes est chiffré à l'aide du protocole TLS (HTTPS), en fonction de la compatibilité de la suite de chiffrement du navigateur de l'Utilisateur. Planisware prend en charge le VPN IPsec Site-à-Site pour l'intégration avec des systèmes externes sur des équipements réseau partagés, assurant un chiffrement AES-256 des données en transit entre les sites.

MESURES DE SÉCURITÉ

SÉCURITÉ DES RESSOURCES HUMAINES

Une vérification rapide des antécédents est incluse dans le processus de recrutement des employés de Planisware. Sous réserve des lois locales applicables, Planisware peut effectuer des vérifications complémentaires des antécédents. L'ensemble des ressources est formé aux mesures et procédures de sécurité de manière régulière.

RESTRICTION D'ACCÈS PAR ADRESSE IP

Si cela est spécifié dans l'Offre, l'accès du Client à l'application peut être géré au niveau du pare-feu afin de limiter l'ensemble des Utilisateurs pouvant accéder à l'application à un sous-réseau IP spécifique.

CHIFFREMENT

Planisware utilise des algorithmes cryptographiques conformes à la sensibilité des données à protéger, aux réglementations en vigueur en matière de chiffrement imposées par pays, et aux recommandations des organismes gouvernementaux de sécurité.

Données en Transit

Le trafic web entre les Utilisateurs et les serveurs est chiffré à l'aide du protocole TLS (HTTPS) en fonction de la compatibilité de la suite de chiffrement du navigateur de l'Utilisateur.

Les échanges de fichiers avec des systèmes externes peuvent également être chiffrés à l'aide du protocole PGP ou selon d'autres normes demandées par le Client. Pour les protocoles non sécurisés, le Produit SaaS Planisware prend en charge le VPN IPsec Site-à-Site pour l'intégration avec des systèmes externes.

Données au Repos

Planisware fournit deux niveaux de chiffrement des données. Le chiffrement de la partition de la base de données est le niveau par défaut de notre plateforme SaaS :

- Le fichier de base de données est monté sur une partition chiffrée.
- Le chiffrement-déchiffrement de la partition est effectué par Planisware lors du démarrage de l'application.
- La clé de chiffrement est présente uniquement dans la mémoire du Serveur Planisware, jamais stockée sur le disque du serveur d'application, de sorte qu'il est impossible de déchiffrer la partition lorsque le Serveur Planisware est arrêté.
- La clé est chiffrée et échangée avec le serveur d'application depuis un serveur de clés situé dans un centre de données distinct.
- Le chiffrement de la partition de la base de données est réalisé via un chiffrement symétrique AES-XTS avec une taille de clé de 512 bits.

Chiffrement dans la base de données :

Selon l'utilisation des attributs dans la base de données, le chiffrement est effectué soit par chiffrement symétrique AES-ECB avec une taille de clé de 256 bits, soit par chiffrement symétrique AES-CBC avec une taille de clé de 128 bits.

JOURNALISATION DES ACCÈS

Planisware tient un fichier journal horodaté des activités suivantes :

- Connexion d'un Utilisateur
- Pages de l'application visitées par les Utilisateurs

Les Mises à Niveau effectuées sur les Données Client par les Utilisateurs sont également suivies et peuvent être mises à disposition pour une investigation interne. Les Clients peuvent également créer leur propre piste d'audit en configurant des traces dans l'application. Ils peuvent ainsi suivre et accéder à des rapports en temps réel, par exemple sur les modifications apportées à un attribut spécifique et leur date.

Pour un contrôle supplémentaire, les Clients peuvent configurer des workflows contraignants dans l'application, garantissant que les mises à jour de données clés sont contrôlées par des processus d'approbation définis selon une matrice RACI.

SÉGRÉGATION DES DONNÉES

Nos solutions SaaS Planisware s'appuient sur une combinaison d'options de composants incluant la base de données PostgreSQL, le serveur web Apache et le système d'exploitation Linux. La solution SaaS Planisware est une solution à locataire unique. Les Données Clients sont isolées et séparées d'un Client à l'autre grâce à :

- Des machine(s) virtuelle(s) dédiée(s) contenant tous les composants
- Une base de données dédiée avec des identifiants d'accès spécifiques
- Un VLAN dédié

SÉPARATION DES TÂCHES

Planisware applique les principes de séparation des tâches et impose un profil Utilisateur strict via une matrice d'attribution des responsabilités. L'environnement de production du Client n'est accessible qu'à :

- L'Équipe de Réponse aux Incidents (sans accès aux Données Client),
- L'Équipe Support, pour intervenir sur un incident (sans accès aux Données Client, sauf autorisation contraire du Client),
- Le Delivery Manager Planisware, pour déployer une modification en production à la demande du Client,
- Le Technical Delivery Manager (sans accès aux Données Client), pour la configuration des serveurs,
- Les Administrateurs Système Planisware, si nécessaire, pour faire face à un incident majeur imprévu.

Ces rôles sont audités régulièrement, et toutes les extensions, révocations ou créations d'attribution sont suivies dans un système de gestion de tickets.

PROTECTION CONTRE LES VIRUS ET LES LOGICIELS MALVEILLANTS

Une approche de sécurité à plusieurs couches a été mise en œuvre selon le principe de défense en profondeur :

- Les environnements des Clients se trouvent sur des serveurs Linux OS avec un antivirus.
- Un antivirus est installé sur les postes de travail Planisware accédant au SaaS Planisware.
- Dans le cadre du processus de gestion des alertes et des incidents, les risques liés aux logiciels malveillants sont surveillés régulièrement.
- Planisware cloisonne l'infrastructure et les applications. Les pare-feu filtrent les communications entre les composants situés dans différentes zones. Tous les composants sont régulièrement surveillés et mis à jour afin de s'assurer qu'ils sont à la dernière version.

CORRECTIFS LOGICIELS ET SYSTÈMES

Les environnements des Clients reçoivent des mises à jour Linux automatiques pour les correctifs de sécurité du système d'exploitation. Dans le cadre du processus de gestion des alertes et des incidents, le Responsable de la Sécurité des Systèmes d'Information (RSSI), les gestionnaires d'actifs et le responsable de l'infrastructure SaaS Planisware examinent régulièrement les risques de sécurité, en s'appuyant sur les alertes de sécurité suivantes :

- Du CERT-FR (ANSSI), du CERT-US ;
- Des éditeurs, constructeurs et sous-traitants ;
- Détectées par les administrateurs (via les événements localisés dans les traces et les alertes remontées par l'équipe d'infrastructure SaaS Planisware) ;
- Des agences, clubs et médias spécialisés en cybersécurité ;
- Diffusées par les fournisseurs de datacenters d'hébergement SaaS Planisware ;

- Identifiées lors de l'exécution du Plan de Contrôle de Sécurité ;
- Identifiées lors de la réalisation d'audits externes.

Après identification et évaluation des risques résultant du système de surveillance et d'alerte, les correctifs de sécurité sont appliqués dans les meilleurs délais (après validation du plan d'action) ou déployés en fonction de la gravité du risque.

SÉCURITÉ RÉSEAU

Planisware configure l'ensemble de l'infrastructure réseau selon le principe du « moindre privilège » en incluant des filtres qui n'autorisent que le trafic minimum requis. Toutes les communications entre le serveur web et les clients via Internet sont chiffrées à l'aide du protocole TLS en fonction de la compatibilité de la suite de chiffrement du navigateur de l'Utilisateur.

La plateforme SaaS Planisware s'appuie sur :

- Des protocoles sécurisés exclusivement (HTTPS, SFTP, IPsec)
- Un pare-feu applicatif web (WAF) surveillant les requêtes HTTP
- Une surveillance des journaux de pare-feu pour les flux réseau entrants et sortants
- Un système de détection d'intrusion (IDS) pour surveiller et bloquer le trafic malveillant et les attaques sur le réseau

SAUVEGARDE DES DONNÉES

Notre offre standard SaaS Planisware inclut des sauvegardes pour l'environnement de production du Client uniquement. Les services de sauvegarde des données sont décrits dans le tableau ci-dessous.

Données à sauvegarder/périmètre	Fréquence	Règles de conservation	Type de sauvegarde	Moyens de protection	Localisation	Responsable	Stockage hors site
Sauvegarde de la base de Données Client	Quotidienne	Par défaut : Les 10 derniers jours Dernières 6 semaines (premier jour de chaque semaine) Derniers 6 mois (1er jour de chaque mois) Option(s) : selon les besoins du Client	Complète	Vidage chiffré Transfert chiffré	Plateforme de sauvegarde de bases de données des environnements client	Planisware	Oui
Sauvegarde complète de la machine virtuelle	Progressive chaque jour	Au moins 15 jours (période minimale de rétention)	Incrémentielle	Chiffrement	NAS	Planisware	Oui

En option de base, une sauvegarde des Données Client est générée sur site et hors site, quotidiennement selon le processus de sauvegarde décrit ci-dessus. En cas de sinistre sur le site principal, l'infrastructure du site principal est restaurée en premier, puis l'environnement. En complément de la sauvegarde quotidienne pour les environnements de production, les Clients peuvent opter, moyennant un coût supplémentaire, pour une option de sauvegarde à chaud (warm-backup) dans laquelle une copie de l'environnement et de la base de données est répliquée hors site dans un environnement passif, en attente. En cas de sinistre sur le site principal, le site passif peut être activé avec une interruption de service limitée.

PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE D'ACTIVITÉ

Le Plan de Continuité d'Activité (PCA) de Planisware couvre :

- Les impacts sur les processus métier,
- Les seuils d'activation,
- Les rôles et fonctions organisationnels des intervenants (membres de la cellule de crise),
- Les plans de communication interne et externe,
- Les principes de fonctionnement en mode urgence,
- Le retour à la normale.

Le PCA de Planisware inclut les procédures du plan de sauvegarde informatique ainsi que le Plan de Reprise d'Activité (PRA).

TESTS DE VULNÉRABILITÉ

SCAN DE VULNÉRABILITÉS

Des scans de vulnérabilité sont effectués de manière régulière. Les pages web sont accessibles uniquement via le protocole HTTPS.

TESTS D'INTRUSION

Une société d'audit de sécurité indépendante est mandatée par Planisware pour réaliser des tests d'intrusion une fois par an. Les certificats de tests d'intrusion annuels sont disponibles sur demande.

TESTS DE SÉCURITÉ APPLICATIVE – ÉGALEMENT APPLICABLES AUX PRODUITS ON-PREMISE

Les risques de sécurité des applications OWASP sont examinés, évalués et intégrés aux suites de tests de Planisware.

DISPOSITIONS APPLICABLES AUX PRODUITS ON-PREMISE ET AUX PRODUITS SAAS

IDENTIFICATION ET AUTHENTIFICATION DE L'UTILISATEUR

Les comptes Utilisateurs sont gérés directement par le Client au sein de notre solution. Dans l'application, l'administrateur du Client peut attribuer à chaque Utilisateur un profil spécifique et un niveau d'autorisation définissant l'accès aux modules, aux fonctionnalités et aux droits sur les données. L'authentification doit être gérée par le Client via le Single Sign On (SSO), en utilisant le standard d'authentification web SAML 2 ou Open ID Connect (OIDC).

Pour les comptes système, pour l'interfaçage avec des systèmes externes par exemple, les mots de passe sont stockés à l'aide d'un algorithme de chiffrement. Avec le SSO, les mots de passe des Utilisateurs ne sont ni stockés ni gérés dans la solution.

CONTRÔLE D'ACCÈS PAR PROFIL

Une fois l'Utilisateur authentifié, l'accès à l'application est davantage restreint via des couches d'autorisation d'accès multi-niveaux. L'accès est défini selon les paramètres suivants :

- Par module, en fonction du profil Utilisateur,
- Par écran au sein d'un module, en fonction du profil Utilisateur,
- Par fonctionnalité au sein du module, en fonction du profil Utilisateur,
- Par élément de données, en fonction du profil de l'Utilisateur et/ou de règles spécifiques à l'Utilisateur.

Les profils Utilisateurs assurent une séparation des tâches au niveau applicatif. Ils peuvent être créés, mis à jour et gérés dans l'application par un administrateur métier du Client. Les modifications apportées à un profil Utilisateur donné se propagent automatiquement à tous les Utilisateurs disposant de ce profil.

AUDITS

Les datacenters et autres locaux de Planisware sont certifiés ISO 27001 ou SOC 2 Type II. Les rapports SOC1/SOC2 et le certificat de conformité ISO 27001 sont généralement disponibles en début de chaque année civile. Planisware peut partager ces certificats sur demande raisonnable du Client.

POLITIQUES INTERNES

Planisware a mis en place un Système de Management de la Sécurité de l'Information (SMSI) conformément à la norme ISO 27001:2013. Cette démarche se concentre sur :

- La définition et le partage d'objectifs de sécurité clairs,
- La sensibilisation des employés de Planisware à la sécurité,
- La création d'un cadre de gestion de la sécurité,
- L'utilisation d'un cadre de gestion des risques,
- Le suivi de l'efficacité des mesures de sécurité par des audits internes et externes,
- La création d'un cadre de gestion des alertes de sécurité et de réduction des incidents de sécurité.

CONFORMITÉ EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Lorsqu'il est établi que le Client a des Utilisateurs au sein de l'Espace Économique Européen, Planisware exige la signature de son Accord de Traitement des Données régissant le traitement des Données Personnelles de ces Utilisateurs, y compris la signature des Clauses Contractuelles Types de la Commission Européenne. Des Accords de Traitement des Données complémentaires sont conclus pour le traitement des données de Personnes Concernées situées dans d'autres juridictions, selon les exigences applicables (par exemple, Californie, Brésil). Sur demande, il est possible de mettre en place des règles de zones de confidentialité pour des catégories d'Utilisateurs. Les Données Personnelles sont chiffrées à la volée pour tous les Utilisateurs ne partageant pas la même zone de confidentialité.

Le Délégué à la Protection des Données (DPO) de Planisware peut être contacté à l'adresse dpo@planisware.com.

Code de champ modifié