

Cegid PRIVATE

PREVENTCARE

ARTICLE 1 – DEFINITIONS

Les termes définis ci-après ont la signification suivante au singulier comme au pluriel:

Demande : désigne un incident reproductible de fonctionnement rencontré par le Client lors de l'utilisation du Logiciel que le Client porte à la connaissance de Cegid. Les Demandes ne concernent pas les incidents de fonctionnement (reproductibles ou pas) des Progiciels Cegid et Progiciels Auteur. Les Demandes traitées par Cegid dans le cadre du Service seront uniquement celles mentionnées dans l'article traitant du périmètre des Demandes.

Jour ouvré : Désigne un jour compris entre le lundi et le vendredi et qui n'est pas un jour férié en France métropolitaine.

Logiciels : Désigne le ou les programmes informatiques, à l'exclusion du Progiciel Cegid et du Progiciel Auteur, comprenant indifféremment les logiciels du système d'exploitation, de sauvegarde, de gestion de base de données ainsi que, d'une manière générale, les antivirus et les progiciels bureautiques ou d'environnement technique. L'auteur et éditeur des Logiciels est un tiers.

Mises à Jour : Désigne les améliorations apportées aux Logiciels, décidées unilatéralement par l'auteur des Logiciels.

Portail : Désigne l'espace d'informations et d'échanges appartenant à Cegid et que Cegid met à la disposition de ses clients utilisateurs des Progiciels Cegid 7j/7 et 24h/24 sauf interruption pour des raisons de maintenance et de sécurité.

Progiciel Cegid : Désigne le ou les progiciel(s) conçu(s) et développé(s) par Cegid, dont elle est propriétaire.

Progiciel Auteur : Désigne le ou les progiciel(s) conçu(s) et développé(s) par d'autres éditeurs que Cegid et pour lesquels Cegid dispose d'un droit de distribution.

Pré-requis Techniques : Désigne les caractéristiques de l'environnement informatique nécessaires au bon fonctionnement des Logiciels et des Progiciels Cegid. Les Pré-requis désignent notamment la configuration nécessaire à l'utilisation des Logiciels et des Progiciels Cegid conformément à leur destination.

Service : Désigne les prestations de support des Logiciels fournies par Cegid en exécution du Livret Service.

ARTICLE 2 – OBJET

Le présent document a pour objet de définir les conditions dans lesquelles Cegid fournit au Client le Service ainsi que les engagements que le Client s'engage à respecter.

En l'absence de dispositions particulières dans l'article 3 Description du Service, la fourniture de Mises à Jour par Cegid est exclue du Service.

ARTICLE 3 – DESCRIPTION DU SERVICE

3.1 – PRE REQUIS

La mise en place du Service ne pourra être assurée par Cegid que dans la mesure où :

- le Client dispose d'un équipement de sécurité avec relai SMTP ;
- l'accès internet est assuré par un abonnement professionnel (de type Orange Business) avec IP fixe ;
- les Logiciels sont utilisés sur des matériels fournis ou conformes aux Pré requis Techniques de Cegid;
- les Logiciels ont été paramétrés par Cegid. A défaut, le paramétrage effectué devra faire l'objet d'une homologation par Cegid, c'est-à-dire d'une vérification et d'une mise en conformité par rapport aux Pré requis Techniques lors de la mise en place du Service ;
- le Client utilise une version du Logiciel maintenue par l'éditeur concerné et accepte l'installation de la dernière version du service pack du Logiciel validée par Cegid ;
- le Client dispose d'un accès opérationnel à la téléassistance, via l'internet, au serveur et poste de travail du Client avec les outils validés par Cegid ;
- le Client dispose d'un accès téléphonique dans le local qui abrite le serveur ;
- le Client donne accès à Cegid à l'ensemble de sa configuration avec des droits de type administrateur ;
- pour le traitement de ses Demandes le Client dispose obligatoirement des Services Cegid Windows serveur, Cegid Base de données, Cegid Sauvegarde ;
- pour le traitement de ses Demandes le Client dispose des Services Cegid Protection Suite (si la solution antivirus a été acquise auprès de Cegid), et Cegid Sécurité Basic ou Premium (si le boîtier de sécurité a été acquis auprès de Cegid).

3.2 – PERIMETRE DU SERVICE

Le Service de Cegid, permet, dans le cadre d'une démarche préventive, au Client d'être assisté dans l'exploitation des Logiciels Systèmes de son outil informatique sous réserve du respect, par le Client, des conditions préalables requises au 3.1.

Le Service comprend :

- une télésurveillance par l'intermédiaire d'outils d'alerte à distance, permettant à Cegid de surveiller l'état de fonctionnement des serveurs (physiques ou virtuels) et Logiciels systèmes du Client inclus dans le périmètre Prevent Care défini au moment de la souscription du Service par le Client ;
- des visites sur site d'un ingénieur système référent.

1. Mise en œuvre des capteurs de surveillance

Cette mise en œuvre donne lieu à une intervention sur site afin de :

- positionner les capteurs destinés à générer des alertes sur les différents éléments qui composent l'infrastructure du client. Ces capteurs réagissent sur un résultat ou sur un seuil d'alerte préalablement défini.
- mettre en conformité les systèmes d'exploitation des serveurs concernés si besoin mettre en place une stratégie de sauvegarde des données en collaboration avec le Client rédiger un document technique listant la configuration des serveurs sous surveillance pour transmission à la

Ce document contient des informations administratives (noms des interlocuteurs Clients et Cegid), un descriptif des serveurs sous surveillance (implémentation physique, nommage, nom de domaine, rôle des serveurs), un descriptif réseau (plan d’adressage ip, type de postes client référencés, éléments matériels de routage, accès internet), un détail du système d’information (partages et scripts, sécurité, sauvegarde, antivirus, messagerie, politique de gestion des mises à jour windows, outils de téléassistance), une liste des autres périphériques (système d’impression, onduleurs), configuration prevent care, schéma réseaux si multiserveurs et multisites.

Ce document pourra être transmis au Client sur simple demande de celui-ci.

La durée de la prestation est adaptée à la complexité du site du Client:

- 1 jour pour les sites ayant 1 à 9 utilisateurs avec maximum 2 serveurs ;
- 2 jours pour les sites ayant 10 à 49 utilisateurs. 3 serveurs et plus ;
- En fonction du montant spécifié au Contrat à partir de 50 utilisateurs.

Les outils installés lors de la journée de mise en œuvre sont:

Éléments sous surveillance	Logiciels installés et paramétrés
Matériel	HP Event Notifier
Sauvegarde	Gestionnaire d’alerte CA, gestionnaire WSB, Gestionnaire Linux
Antivirus	Console de supervision Cegid Protection Suite V3
Telecom	Cegid Preventcare Monitor
Système	Cegid Preventcare Monitor

2. Processus de surveillance détaillé.

La surveillance porte sur les différents éléments ci-dessous

- Matériel.

Les alertes sont remontées par les logiciels du constructeur HP, Dell ou IBM, dans le cas d’HP c’est le logiciel HP event notifier qui collecte les alertes, celles-ci portent sur les éléments ci-dessous :

- Batterie
- Dysfonctionnement du Raid
- Surveillance du lecteur de Bande
- Ventilateur
- Alimentation
- NIC (network infrastructure Card)
- Statut du disque physique

Lorsque le gestionnaire HP détecte un dysfonctionnement sur un des composants, HP event notifier adresse une alerte mail à la cellule de surveillance Prevent Care.

- Mécanismes de sauvegarde:

Les sauvegardes de données doivent être programmées périodiquement, idéalement tous les jours.

Les Logiciels validés par Cegid pour la sauvegarde sont :

- Solution Arcserve backup 11.x, 12.x

- Windows Server Backup pour les serveurs Windows 2008
- Nt backup pour les serveur Windows 2003
- Sauvegarde CPIO+TAR sur les serveurs Linux

Il appartient au Client de mettre en place le support de sauvegarde dans le lecteur en accord avec la politique de sauvegarde définie entre le Client et l'ingénieur système de Cegid au moment de la mise en place des capteurs de surveillance.

Les alertes sur le résultat sont envoyées tous les jours, l'équipe de surveillance procède à une analyse quotidienne des sauvegardes échouées, incomplètes, annulées ou non reçues.

○ Surveillance Système :

La surveillance du système consiste à monitorer l'ensemble des indicateurs propres au système d'exploitation Windows.

Ces indicateurs peuvent être des compteurs « WMI », des messages repris du « journal d'évènement », des services Windows ou des seuils d'espace disque.

Voici en détail les seuils en valeur et en temps à partir desquels une alerte est adressée à preventcare@cegid.fr:

Compteur de Performance Windows (Temps disque, Fichier d'échange, Mémoire, temps Processeur) collecte et envoi d'alerte au bout d'1 minute

- % du temps disque > à 95 % pendant plus de 20 minutes
- Long moyenne de la file d'attente > à 95% pendant plus de 20 minutes
- Pourcentage d'utilisation du fichier d'échange > 85% pendant 15 minutes
- % d'octet dédiés à la mémoire > 90% pendant 10 minutes
- Temps processeur supérieur à 95% pendant 20 minutes.

Espace disque faible - collecte et envoi d'une alerte 1 fois par jour (à 3h)

- Surveillance des disques système (C:\) et de donnée (D:\) avec déclenchement d'une alerte au seuil de 10% restant.

Event Log Errors – collecte et envoi des alertes toutes les 10 minutes

- Surveillance des événements systèmes identifié comme pertinent (erreurs Active directory, reboot ...).

Event notifier – collecte et envoi des alertes toutes les heures

- Surveillance des services identifiés comme nécessaire au fonctionnement du système ou générateurs d'instabilité système.

○ Surveillance des liens télécom :

Toutes les heures une alerte est envoyée depuis le Logiciel « *Cegid preventcare monitor* » pour valider le fonctionnement du logiciel ainsi que le fonctionnement du relai de messagerie.

Si l'alerte n'est pas envoyée cela sera considéré comme une alerte majeure car potentiellement il y a une rupture du lien internet ou défaillance du serveur hébergeant le Logiciel Cegid preventcare monitor

Pour les Clients « multi-site » une sonde mesure les latences > 600 ms ainsi que les ruptures de lien VPN. (Virtual private network).

Une alerte est envoyée régulièrement à la cellule de surveillance Prevent Care jusqu'à remise en état du lien.

○ Antivirus

Le Client doit disposer de la solution Cegid Protection Suite.

Lors de la mise en service l'ingénieur référant paramètre un accès sécurisé vers « le cloud » de trend micro (wfrm-emea.trendmicro.com), ainsi la cellule de surveillance dispose d'un accès sur une console, hébergée (par l'éditeur Trend Micro) qui permet de suivre en temps réel les menaces détectées pour chacun des Clients.

3. Traitement des alertes

Les alertes sont matérialisées par des mails envoyés à l'adresse preventcare@cegid.fr, mails qui sont compilés dans une console de supervision et analysés par une équipe de techniciens support.

Une équipe de techniciens support Cegid est dédiée à la surveillance de l'ensemble des clients pendant les heures ouvrées de Cegid

La communication vers le client se fera essentiellement par mail.

Toutes les alertes sont traitées de la façon suivante :

- A réception l'équipe de surveillance fixe un niveau de criticité (ou niveau de risque) déterminé par l'impact sur l'activité de l'entreprise
 - **Sans impact** : Prise en considération de l'alerte, pas de communication Client, éventuels ajustements depuis la console de supervision.
 - **Mineur, modéré** : Mail ou contact téléphonique pour indiquer les consignes de résolution ou de contournement à réaliser par le client.
 - **Significatif** : Enregistrement d'une demande au support, mail au client pour signifier l'enregistrement et la prise en charge par les équipes de support Cegid.
 - **Majeur, étendu** : Enregistrement d'une demande au support, appel téléphonique de l'équipe de surveillance pour mettre en place un diagnostic de niveau 1 d'une durée inférieure à 1 heure. Au-delà de ce délai, il transfère la demande vers l'équipe de niveau 2 pour poursuite du dépannage.

Le traitement des Demandes s'effectuera dans les conditions prévues dans le Livret Service Contact ou Open applicable (cf 3.1).

4. Visites sur site

Le service comprend également deux visites préventives par an sur site d'un consultant système Cegid, et d'une visite par serveur (physique ou virtuel) au-delà du premier serveur.

Ces visites s'appliquent sur le périmètre du système d'information Client couvert par le Service et décrit dans le document technique rédigé lors de la mise en place du service

Ces interventions seront planifiées à l'avance entre le Client et Cegid.

L'objectif est de contrôler le système d'information et transmettre les informations pertinentes au Client et à l'équipe Prevent Care.

Elles permettent d'effectuer les prestations suivantes :

- Installer, contrôler, mettre à jour les outils de remontée d'alertes Prevent Care ;
- Compléter sur site le contrôle du bon fonctionnement des systèmes de sécurité existants :
 - Contrôle des accès informatiques (domaine, annuaire...)
 - Systèmes redondant des serveurs
 - Sauvegarde des serveurs
 - Antivirus serveurs
 - Boitiers de sécurité accès Internet
 - Onduleurs
- Compléter sur site le contrôle des performances et la disponibilité des serveurs et du réseau ;
- Effectuer les mises à jour de sécurité système et/ou transférer le savoir-faire correspondant aux intervenants du Client ;
- Faire un reporting détaillé aux intervenants du Client des anomalies détectées pendant la période de télésurveillance entre les 2 visites sur le site du Client;
- Conseiller les intervenants Client sur les évolutions d'équipement et de procédure nécessaires à la prévention des anomalies détectées ou prévisibles ;
- Répondre aux questions des intervenants Client sur les problèmes rencontrés en exploitation depuis la précédente visite et leur promulguer les conseils nécessaires ;
- Mettre à jour le dossier technique du Client.

La durée de la visite ne dépassera pas une journée.

L'ensemble des actions menées seront tracées dans un document fiche de visite transmis à l'équipe Prevent Care et pouvant être remis au Client sur simple demande.

ARTICLE 4 – PROPRIETE INTELLECTUELLE

Le Client devra, pour permettre la fourniture du Service :

- bénéficier des licences d'utilisation des Logiciels ;
- respecter les conditions normales d'utilisation des Logiciels et les Pré-requis Techniques.

ARTICLE 5 – RESPONSABILITE

5.1 RESPONSABILITÉ DE CEGID

Pour l'exécution de l'ensemble de ses obligations, Cegid est soumise à une obligation de moyens. Cegid ne fournit aucune garantie en ce qui concerne l'absence totale d'anomalies ou d'erreurs dans les Logiciels.

Cegid est responsable uniquement des dommages directs et prévisibles résultant d'un manquement à ses obligations contractuelles.

Cegid ne pourra pas être tenue responsable pour tout préjudice subi par le Client qui serait qualifié de dommage indirect, qu'il soit matériel ou immatériel, prévisible ou imprévisible, tels que la perte d'une chance, la perte de chiffres d'affaires, d'économies prévues, de clientèle et/ou de commandes.

Dans l'hypothèse où la responsabilité de Cegid serait retenue, l'indemnisation globale et cumulée, toutes causes confondues, à laquelle le Client pourrait prétendre sera limitée au montant versé par le Client à Cegid au cours des douze (12) derniers mois précédent l'événement à l'origine de la responsabilité de Cegid.

Les Parties reconnaissent que le prix du Service reflète la répartition des risques découlant du Contrat, ainsi que l'équilibre économique voulu par les Parties, et que le Service n'aurait pas été conclu sans les limitations de responsabilité définies aux présentes.

Cegid s'engage à maintenir en vigueur une assurance responsabilité civile professionnelle couvrant les dommages qui pourraient survenir à l'occasion de l'exécution du Service.

5.2 RESPONSABILITÉ DU CLIENT

Le Client est responsable du bon respect des Pré-requis Techniques. A cet égard, le Client est avisé que le non respect des Pré-requis Techniques déchargera Cegid de tout ou partie de ses obligations contractuelles.

Le Client est exclusivement responsable des moyens (outils, méthodes, configuration...) qu'il utilise et qui ne sont ni fournis ni mis à sa disposition par Cegid dans le cadre du présent Service.

Il appartient au Client de prendre toutes les précautions nécessaires pour garantir la sécurité, la confidentialité et l'intégrité de toutes les données qu'il pourra traiter directement ou indirectement dans le cadre de l'utilisation des Logiciels et, notamment, s'assurer que toutes les mesures nécessaires pour la sauvegarde et la reconstitution de ses données ont été prises en temps utile.

De la même manière, le Client doit prendre toutes les mesures nécessaires pour la protection de son système d'information, notamment en ce qui concerne la protection contre les virus, vers et autres procédés hostiles d'intrusion.

ARTICLE 6 – RESILIATION DU SERVICE

En cas de manquements graves par l'une ou l'autre des Parties aux obligations qui lui incombent en application du Contrat pour le Service, la Partie défaillante se verra adresser par l'autre Partie une mise en demeure par courrier recommandé avec accusé de réception détaillant les griefs.

La résiliation de plein droit du Service prendra effet vingt (20) jours calendaires après la réception de la mise en demeure précitée par la Partie défaillante, sauf à ce que cette dernière justifie des remèdes appropriés apportés pour supprimer le manquement constaté. La résiliation interviendra sans préjudice de tous les dommages et intérêts auxquels la Partie non défaillante pourrait prétendre.

Cegid aura le droit de résilier le Contrat immédiatement de plein droit et par lettre recommandée avec accusé de réception, en cas d'utilisation par le Client d'une version du Logiciel ne bénéficiant plus de la maintenance et du support de l'éditeur concerné.

ARTICLE 7 – DONNEES PERSONNELLES

Il est rappelé qu'au sens de la loi n° 78-17 du 6 janvier 1978 dite Informatique et libertés, Cegid agit en qualité de sous-traitant, sur instructions du Client, lequel est qualifié de responsable des traitements de données mis en œuvre grâce aux Logiciels.