Convention de Niveaux de Service (SLA & Support)

Version	Contributeur	Date de publication	Date de validité	Commentaires
1.0	LM	01/08/2026	01/08/2026	Création. Remplace l'ancienne documentation (PAQS, Garantie, Contrat de maintenance)

Sommaire

ARTICLE 1. ARTICULATION CONTRACTUELLE ET RENVOIS

La présente Convention de Niveaux de Service (SLA & Support) a pour objet de définir exclusivement les métriques techniques de disponibilité, les garanties de continuité (PCRA), ainsi que les prérequis techniques applicables à la Solution MenKorn.
Structure de la Convention et Indivisibilité : La présente Convention de Niveaux de Service constitue un bloc contractuel indissociable comprenant le présent document socle ainsi que ses deux annexes :

- **Annexe B — Cahier des Charges Opérationnel :** Définit les prestations de maintenance corrective et évolutive, la qualification des anomalies, les engagements de résolution (GTI/GTR) et la matrice d'escalade N0 à N3.
- **Annexe C — Plan d'Assurance Qualité et Sécurité (PAQS) :** Définit les mesures techniques et organisationnelles (MTO) de cybersécurité, de chiffrement et de protection des infrastructures.

Afin de garantir l'indivisibilité de la Liasse Contractuelle et d'éviter toute contradiction juridique :

- **Garantie, Modalités d'Acquisition et Facturation :** L'ensemble des dispositions relatives à l'inclusion de la garantie initiale de douze (12) mois et à la formalisation de la maintenance récurrente via le Bon de Commande sont exclusivement régies par les **Conditions Générales de Vente (CGV)** de CrisiSoft.
- **Accès au Support, Filtrage et Horaires (JHO/HHO) :** Les règles encadrant l'habilitation des Référents pour contacter le support technique, les jours et horaires ouvrés, ainsi que les modalités de facturation des interventions d'astreinte hors contrat, sont exclusivement régies par le **Contrat de Licence Utilisateur Final (CLUF / CGU)**.

ARTICLE 2. CLASSIFICATION DES INCIDENTS ET ENGAGEMENTS

Les engagements de CrisiSoft prennent effet à compter de la qualification formelle de l'anomalie par le support technique, sous réserve que l'alerte ait été émise conformément aux procédures définies dans le **Contrat de Licence Utilisateur Final (CLUF / CGU).**
La classification de sévérité (A à E), les délais d'intervention (GTI), de contournement (GTC) et de résolution (GTR) sont centralisés et définis dans **l'Annexe B — Cahier des Charges Opérationnel**.

ARTICLE 3. DISPONIBILITÉ ET HÉBERGEMENT HDS

(Source unique d'information pour la disponibilité applicative)

3.1. Taux de Disponibilité Mensuel et Hébergement HDS

L'infrastructure de la Solution est hébergée sur des datacenters souverains situés en France métropolitaine, bénéficiant des certifications Hébergeur de Données de Santé (HDS) et ISO/IEC 27001.
CrisiSoft s'engage à mettre en œuvre tous les moyens raisonnables pour assurer un taux de disponibilité annuel de la Solution de 99,8 %.

3.2. Exclusions du calcul de disponibilité

Ne sont pas comptabilisées comme indisponibilités applicatives :
Les fenêtres de maintenance planifiée (notifiées au minimum 48 heures à l'avance et réalisées préférentiellement en heures creuses) ;
Les suspensions d'accès résultant d'un manquement de l'Organisme ou de l'Utilisateur au **Contrat de Licence Utilisateur Final (CLUF / CGU)** (ex: utilisation de scripts/robots interdits, refus de coopération) ;
Les cas de force majeure, cyberattaques d'ampleur nationale ou défaillances des opérateurs télécoms et Fournisseurs d'Accès Internet (FAI).

ARTICLE 4. PLAN DE CONTINUITÉ ET DE REPRISE D'ACTIVITÉ (PCRA)

(Source unique d'information pour les métriques de sauvegarde et de reprise)
Pour des raisons impérieuses de cybersécurité, le document détaillé du Plan de Continuité et de Reprise d'Activité (PCRA) de CrisiSoft est strictement confidentiel et non diffusé. Toutefois, CrisiSoft garantit contractuellement les métriques et principes de résilience suivants :

- **Redondance d'infrastructure** : Architecture **haute disponibilité déployée en mode actif-actif** sur deux datacenters distants.
- **Politique de Sauvegarde (RPO)** : Sauvegardes quotidiennes managées et répliquées sur un 3ème datacenter dédié et géographiquement distant (isolation "Air-Gapped"), avec une rétention sur 30 jours glissants **incluant une rétention anti-ransomware de 14 jour**s (sauvegardes immuables).
- Temps de Reprise Maximal (RTO) : L'objectif de temps de reprise maximal du service est fixé à 4 heures en cas de sinistre majeur sur le datacenter principal

ARTICLE 5. PRÉREQUIS TECHNIQUES DE L'ORGANISME

L'Organisme fait son affaire de l'ensemble du matériel technique et des réseaux nécessaires à l'utilisation de MenKorn. La responsabilité de CrisiSoft ne saurait être engagée en cas de dégradation des performances liée au non-respect des prérequis suivants. Évolutivité : CrisiSoft se réserve le droit de modifier à sa discrétion les présents prérequis techniques, notamment pour permettre aux progiciels de s'adapter aux évolutions technologiques et sécuritaires.

5.1. Prérequis Généraux (Postes de travail)

- **Matériels et Systèmes :**
  - Postes de travail (PC/Mac) récents avec au minimum 8 Go de RAM.
  - Les horloges systèmes doivent être synchronisées à l'heure juste.
  - Microsoft Teams pour mise en place et suivi projet.
  - Format HTML des emails
- **Affichage :**
  - Écran : 14 pouces minimum, 17 pouces recommandés.
  - Résolution pour les écrans de salle de crise : 1600x900 pixels minimum, résolution recommandée de 1920x1080 pixels (Full HD).
- **Navigateurs :** Utilisation exclusive des deux dernières versions majeures de Google Chrome, Mozilla Firefox ou Microsoft Edge (Internet Explorer formellement interdit).
- **Réseau et Flux :**
  - Connexion internet haut-débit continue (10 Mbps dédié min.).
  - Pare-feux (firewalls) : doivent impérativement autoriser les flux HTTPS (Port 443) et les WebSockets vers les serveurs CrisiSoft, **sans déchiffrement SSL (SSL Inspection)**.
  - Autorisation de domaines : liste fournie au déploiement.
  - Autorisations d'IP : liste fournie au déploiement.

5.2. Prérequis Mobiles (Smartphones et Tablettes)

- Systèmes d'exploitation : Le fonctionnement optimal de la Solution sur terminaux mobiles nécessite de supporter, au minimum, un système d'exploitation Android ou iOS à jour de ses versions majeures et correctifs de sécurité.
- Affichage : La configuration de l'affichage du site internet et des applications sur terminaux mobiles repose exclusivement sur les paramètres d'affichage et de résolution par défaut des systèmes d'exploitation Android et iOS.
- Sécurité et Terminaux Professionnels : En raison de la nature sensible des données de santé (HDS) et des données opérationnelles traitées, CrisiSoft recommande formellement l'utilisation exclusive de terminaux mobiles professionnels, maintenus régulièrement et dédiés à l'utilisation de la Solution. L'usage de terminaux personnels (BYOD) est fortement déconseillé par CrisiSoft et relève de la seule responsabilité de l'Organisme.
- Chiffrement des Terminaux : CrisiSoft n'assure pas le chiffrement natif des données stockées localement sur les terminaux mobiles. Le Client fera son affaire de la configuration de ses terminaux mobiles (via outil MDM ou OS) afin qu'ils soient intégralement chiffrés.

5.3. Prérequis Spécifiques (Module Déporté « PMA »)

- **Matériels Recommandés :** PC serveur durci respectant les prérequis généraux. Terminaux Mobiles PDA/Durcis (normes IP65/IP67, résistance aux chutes, températures extrêmes) et respectant les prérequis mobiles.
- **Réseau Local de Secours :** Routeurs/Points d'accès Wi-Fi autonomes et durcis (Dual Band 802.11n, PoE, IP67) pour garantir le maillage local en cas de rupture internet. L'Organisme est seul responsable du chiffrement matériel (disque dur) de ses flottes mobiles.

Annexe B - Cahier des Charges Opérationnel

Article 1. Articulation Contractuelle et Objet

Le présent Cahier des Charges Opérationnel (ci-après l'« **Annexe B** ») **fait partie intégrante de la Convention de Niveaux de Service (SLA & Support)** liant CrisiSoft à l'Organisme utilisateur et au Client.
Il a pour objet unique de définir la classification des anomalies, la matrice de sévérité (A à E), le processus de traitement du support et les engagements de résolution (GTI/GTR) applicables à la Solution MenKorn.
Principe d'indivisibilité et d'étanchéité : Afin d'éviter toute contradiction juridique, les stipulations commerciales (durée, facturation, pénalités financières, résiliation) sont exclusivement régies par les **Conditions Générales de Vente (CGV)**. Les règles d'usage, de sécurité et d'accès au support incombant aux agents sont régies par le **Contrat de Licence Utilisateur Final (CLUF / CGU)**. Le présent document ne contient aucune disposition financière.

Article 2. Périmètre de la Maintenance et Services Associés

2.1. Maintenance Corrective (Inclus)

CrisiSoft assure la maintenance corrective de la Solution, consistant à corriger ou contourner les anomalies de fonctionnement (bugs) reproductibles imputables au logiciel, signalées par l'Organisme.

2.2. Maintenance Évolutive et Mises à jour (Inclus)

CrisiSoft assure la maintenance évolutive, comprenant la mise à disposition des mises à jour correctives (patchs de sécurité) et des évolutions fonctionnelles mineures ou majeures de la Solution (upgrades). L'Organisme s'engage à accepter le déploiement de ces mises à jour pour continuer à bénéficier du support technique. La fréquence et le contenu des mises à jour relèvent de la seule discrétion de la roadmap R&D de CrisiSoft.

2.3. Services Associés (Activables par Bon de Commande)

Les prestations complémentaires et dotations suivantes ne sont pas incluses par défaut dans la maintenance applicative standard. Leur périmètre, leur volume et leur facturation (ainsi que les dépassements éventuels) sont exclusivement définis et activés via le Bon de Commande :

- Packs et forfaits de consommables (SMS, Appels Vocaux automatisés).
- Journées d'accompagnement sur site ou prestations de conseil/formation.
- Accès au « Club Utilisateurs » de CrisiSoft.
- Prestations d'accompagnement à la configuration et paramétrage avancé.
- Option d'assistance Hotline étendue (24h/24 et 7j/7).
- Déploiements spécifiques (VPN, infrastructure dédiée…).
- Evolutions spécifiques optionnelles du logiciel à la discrétion de CrisiSoft

Article 3. Processus de Sollicitation et de Traitement du Support

Conformément aux règles d'usage et de filtrage édictées à l'Article 4.3 du Contrat de Licence Utilisateur Final (CLUF / CGU), l'accès au support technique s'effectue via les canaux dédiés suivants :

1. **Le Portail Web de Support (Ticketing)** : Accessible 24/7 pour toute demande d'assistance, question d'usage, demande d'évolution, et pour le signalement d'anomalies de sévérité C, D et E.
2. **La Ligne Téléphonique d'Urgence (Hotline) : Strictement réservée aux signalements d'incidents de Sévérité A et B se produisant en « Situation Réelle » de gestion de crise**. Tout appel non justifié par une crise réelle sera réorienté vers le portail web

Article 4. Matrice de Sévérité et Engagements (GTI / GTR)

Les engagements de temps de CrisiSoft sont calculés en Jours et Heures Ouvrés (JHO), sauf souscription à l'Option Hotline 24/7. Les délais courent à compter de la qualification de l'incident par CrisiSoft suite à l'ouverture d'un ticket conforme.
Afin de protéger la continuité des opérations, CrisiSoft distingue le contexte de **Situation Réelle** (crise sanitaire, attentat, plan blanc) du contexte d'**Exercice** (simulation, entraînement).

Niveau de Sévérité	Définition & Impact	Contexte	GTI (Temps d'Intervention)	GTR / GTC (Temps de Résolution ou Contournement)
Sévérité A *(Bloquant)*	Indisponibilité totale de la solution. Pas de contournement possible.	**Situation Réelle**	30 Minutes	**4 Heures** (GTC)
Sévérité A *(Bloquant)*	*Idem.*	*Exercice / Simulation*	2 Heures	**12 Heures**
Sévérité B *(Majeur)*	Dégradation forte d'une fonctionnalité essentielle, mais la main courante reste accessible.	**Situation Réelle**	2 Heures	**8 Heures**
Sévérité B *(Majeur)*	*Idem.*	*Exercice / Simulation*	4 Heures	**24 Heures**
Sévérité C *(Significatif)*	Dysfonctionnement non critique ou disposant d'une solution de contournement (GTC) simple.	*Indifférent*	8 Heures	**Semaine +1** (Patch)
Sévérité D *(Mineur)*	Anomalie d'affichage, gêne cosmétique ne bloquant pas l'usage.	*Indifférent*	24 Heures	**Prochaine Version**
Sévérité E *(Évolution)*	Demande d'évolution ou d'assistance au paramétrage.	*Indifférent*	48 Heures	**Planifié selon Roadmap**

(GTI = Délai de prise en charge et début du diagnostic / GTC = Mise en place d'une solution de contournement fonctionnelle).

Article 5. Matrice d'Escalade (N0 à N3)

Le traitement des incidents respecte le processus de qualification ITIL suivant :

- **Niveau 0 (N0) - Qualification par l'Organisme :** Conformément à l'Article 4.3 du **Contrat de Licence Utilisateur Final (CLUF / CGU)**, le Référent de l'Organisme qualifie le besoin, consulte la base de connaissances et les tutoriels fournis, vérifie que le poste de travail respecte les prérequis techniques (réseau, navigateur), et rassemble les éléments de reproduction avant de solliciter CrisiSoft.
- **Niveau 1 (N1) - Qualification CrisiSoft :** Réception de l'alerte par le Centre de Support. Vérification de la conformité du ticket, qualification de la sévérité et assistance fonctionnelle.
- **Niveau 2 (N2) - Support Avancé :** Intervention des techniciens experts (investigation des logs, requêtes en base de données, mise en place d'une solution de contournement - GTC).
- **Niveau 3 (N3) - R&D et Éditeur :** Escalade aux équipes de développement et/ou infra pour correction du code source (fix) et déploiement d'un patch correctif.

Article 6. Exclusions de Garantie et Suspension des Délais

CrisiSoft est dégagée de ses engagements de niveaux de service (GTI/GTR), et pourra facturer les temps d'investigation en régie, dans les cas suivants :

1. **Non-respect du Contrat de Licence Utilisateur Final (CLUF / CGU) :** Utilisation de comptes génériques partagés, refus de coopérer, ou agissement contraire aux règles de sécurité.
2. **Défaut de Prérequis Techniques :** Panne ou dégradation résultant du non-respect des prérequis techniques (ex: intervention d'un pare-feu local avec *SSL Inspection*, navigateur obsolète).
3. **Absence de coopération :** Le délai GTR est automatiquement suspendu tant que l'Organisme ne fournit pas les éléments demandés par le support pour reproduire l'anomalie (logs locaux, captures d'écran, accès à distance).
4. **Intervention tierce :** Anomalie causée par une modification de l'environnement informatique de l'Organisme non notifiée à CrisiSoft, ou par l'intégration d'un logiciel tiers non certifié.

Article 7. Renvois pour l'Hébergement HDS, la Disponibilité et la Sécurité

Afin de garantir une source d'information unique et d'éviter les doublons :

- Taux de disponibilité (99,8 %) et PCRA (Sauvegardes / RTO) : Sont exclusivement régis par les Articles 3 et 4 du socle de la Convention de Niveaux de Service (SLA & Support).
- Cybersécurité et Chiffrement : Sont exclusivement régis par l'Annexe C — Plan d'Assurance Qualité et Sécurité (PAQS).
- Sous-traitants HDS et RGPD : Sont exclusivement consignés dans l'Annexe A (DPA) rattachée au **Contrat de Licence Utilisateur Final (CLUF / CGU)**.

Article 8. Réversibilité et Fin de cycle

À l'issue de la relation contractuelle, et conformément aux dispositions **de l'Annexe A (DPA) du Contrat de Licence Utilisateur Final (CLUF/CGU),** CrisiSoft garantit la réversibilité des données de l'Organisme. La restitution des bases de données et des mains courantes s'effectue dans un format standard du marché.

Annexe C — Plan d'Assurance Qualité et Sécurité (PAQS)

(Source unique d'information pour la cybersécurité technique et la démarche qualité)

Article 1. Objet, Gouvernance et Évolution

La présente Annexe C (ci-après le « **PAQS** ») fait partie intégrante de la **Convention de Niveaux de Service (SLA & Support).**

Elle documente l'ensemble des Mesures Techniques et Organisationnelles (MTO) de cybersécurité appliquées par CrisiSoft et ses sous-traitants d'infogérance pour garantir la sécurité, l'intégrité, la traçabilité et la confidentialité de la Solution MenKorn.

Évolution : CrisiSoft étant tenue de s'adapter en permanence à l'état de l'art et aux nouvelles menaces, CrisiSoft se réserve le droit de faire évoluer le présent PAQS et ses dispositifs techniques pour maintenir ou élever le niveau de sécurité global de la Solution.

La gouvernance de la sécurité et de la qualité s'articule autour d'un Comité Technique et d'un Comité de Pilotage, chargés de valider les choix architecturaux et d'appliquer les recommandations de l'ANSSI, de la CNIL et les exigences du référentiel ISO/IEC 27001.

Qualification des équipes : Le personnel de CrisiSoft (ingénieurs, support, chefs de projet) est régulièrement formé et sensibilisé aux exigences de sécurité des systèmes d'information (MOC de l'ANSSI) et à la réglementation sur la protection des données de santé (CNIL). Les accès aux environnements clients sont strictement limités aux personnels habilités et soumis au secret professionnel.

Article 2. Sécurité des Infrastructures et Hébergement (HDS)

2.1. Environnement Souverain et Sécurité Physique

L'infrastructure web de la Solution est déployée sur des datacenters souverains localisés en France métropolitaine. CrisiSoft s'appuie sur un hébergeur infogéreur disposant de la certification **Hébergeur de Données de Santé (HDS)** et de la certification **ISO/IEC 27001**.

La sécurité physique des sites est garantie : aucun accès physique aux serveurs n'est possible en dehors du personnel biométriquement habilité de l'hébergeur.

Architecture Redondée : Pour garantir la continuité de service, l'architecture applicative est redondée. Elle repose sur la séparation et la duplication des machines d'interfaces web (Front-end), des machines de traitement (Back-end) et des clusters de Bases de Données, déployés sur des zones de disponibilité distinctes.

2.2. Chiffrement et Protection des Flux

- **Données en transit :** L'ensemble des communications avec les serveurs d'authentification et les accès aux services (Applications, APIs) sont obligatoirement chiffrés par le protocole HTTPS/TLS (Transport Layer Security) avec une clé de 2048 bits et une signature SHA-256.
- **Données au repos :** Les machines virtuelles (VM), les bases de données et les sauvegardes sont systématiquement chiffrées (KMS géré par l'infogéreur HDS).
- **Protection périmétrique :** L'infrastructure est protégée en continu par des pare-feux (Firewalls), un WAF (Web Application Firewall), un système anti-DDoS, et supervisée 24/7 par une solution EDR (Endpoint Detection and Response) comportementale, dotée de capacités d'isolation autonome et de remédiation (rollback) en cas d'attaque.
- **Accès des équipes DevOps :** L'accès aux serveurs par les équipes d'ingénierie et de développement de CrisiSoft est hautement sécurisé. Il s'effectue obligatoirement au travers d'un tunnel VPN chiffré, d'une authentification par clés SSH, et transite par un serveur Bastion certifié par l'ANSSI (CSPN). Ce Bastion exige une authentification multifacteur (MFA) et procède à l'enregistrement vidéo systématique de l'ensemble des sessions d'administration, garantissant une zone de confiance absolue.

Article 3. Sécurité Applicative et Cycle de Développement (Secure SDLC)

3.1. Philosophie du Moindre Privilège et Authentification

La Solution MenKorn est conçue selon le principe du moindre privilège (Need-to-Know). L'attribution des profils métiers et des droits d'accès au sein de la Solution reste sous le contrôle exclusif de l'Administrateur de l'Organisme (RBAC - Role-Based Access Control).

- **Mots de passe :** Aucun mot de passe n'est stocké en clair dans le code ou l'application. Les mots de passe utilisateurs sont stockés en base de données après un hachage réputé robuste (SHA-256).
- **Complexité :** Le système impose des règles de complexité (longueur minimale de 8 caractères, incluant majuscules, minuscules et chiffres).
- **Désactivation :** Pour garantir la traçabilité légale, les comptes utilisateurs ne sont pas supprimés mais désactivés.

3.2. Méthodologie, Environnements et Tests

- **Méthode Scrum et Pipeline de qualité :** Les développements (nouvelles fonctionnalités et correctifs) sont menés selon la méthodologie Agile (Scrum). Chaque version (release) suit un processus strict de validation avant sa mise en production.
- **Niveaux de Tests :** Le code est soumis à un pipeline d'intégration continue comprenant des tests automatiques unitaires, des tests d'intégration, et des tests de bout-en-bout (End-to-End). Ces phases sont obligatoirement suivies de tests manuels de non-régression menés sur une plateforme de recette dédiée.
- **Séparation des environnements :** L'environnement de préproduction (tests et recettes) est maintenu de manière strictement indépendante et étanche par rapport à l'environnement de production nominale.
- **Tests d'Intrusion (Pentests) :** CrisiSoft fait réaliser régulièrement des tests d'intrusion (architecture, flux, interface) par des tiers qualifiés indépendants. Les correctifs identifiés sont priorisés et intégrés aux sprints de la roadmap technique.
- **Gestion des correctifs (Patch Management) :** Les mises à jour de sécurité sur l'infrastructure (OS, bases de données) sont qualifiées et appliquées de manière hebdomadaire pour limiter tout impact sur la production.

Article 4. Traçabilité, Logs et Audits

Afin de garantir l'imputabilité des actions et la détection d'incidents (enjeux médico-légaux), la Solution intègre une politique stricte de journalisation à deux niveaux :

1. **Traçabilité Technique (Infrastructure) :** Journalisation en continu de la santé des serveurs (CPU, temps de réponse) et de l'ensemble des connexions administrateurs aux systèmes et aux bases de données. L'enregistrement vidéo inaltérable des sessions d'administration via le Bastion certifié complète ce dispositif pour une imputabilité totale.
2. **Traçabilité Fonctionnelle et d'Audit (Mains Courantes) :** Journalisation complète des connexions utilisateurs, des actions de déclenchement et de gestion d'événements, et de la modification ou suppression des fiches personnels.

Téléchargement et Transparence : L'Organisme a la possibilité de télécharger de manière autonome ses propres logs fonctionnels et historiques via l'interface de la Solution, durant et à l'issue de chaque événement de crise. En cas de situation réelle, CrisiSoft s'assure auprès du client que ces logs ont bien été sécurisés.

Identitovigilance et Enquêtes : Des demandes d'accès aux traces applicatives pourront être formulées par l'Organisme auprès de CrisiSoft dans le cadre d'audits internes, d'activités de la cellule d'identitovigilance ou de recours légaux. CrisiSoft mettra en œuvre les moyens nécessaires pour faciliter la fourniture de ces journaux de connexion et traces d'accès aux données pour ces opérations intégrées à l'offre de support de base.

Droit d'Audit : L'Organisme peut demander l'accès aux rapports d'audits de sécurité réalisés par les tiers mandatés par CrisiSoft. Conformément à la convention de service, CrisiSoft coopérera également aux audits de sécurité sur pièces ou sur place initiés par l'Organisme, sous réserve d'un préavis raisonnable de trente (30) jours et de la signature d'un accord de confidentialité (NDA).