DESCRIPTION SAAS HOPEX

LES SERVICES DECRITS AUX PRESENTES NE SONT APPLICABLES QU'A LA VERSION STANDARD D'HOPEX. SI LE CLIENT SOUHAITE QU'ILS SOIENT APPLICABLES AUX DEVELOPPEMENTS SPECIFIQUES ET PARAMETRAGES, IL DOIT ALORS SOUSCRIRE A L'OPTION PREMIUM MAINTENANCE.

L'ATTENTION DU CLIENT EST EGALEMENT ATTIREE SUR LE FAIT QUE SON REFUS MIGRER VERS UNE VERSION SUPPORTEE, EN PLUS DE NE PLUS BENEFICIER DES SERVICES DE MAINTENANCE, EN CE COMPRIS LA DELIVRANCE DE CORRECTIONS, L'EXPOSE A DES PROBLEMES DE SECURITE. MEGA NE SAURAIT ETRE TENUE POUR RESPONSABLE DE TOUTE CONSEQUENCE QUI AURAIT PU ETRE EVITEE SI LE CLIENT AVAIT MIGRE VERS UNE VERSION SUPPORTEE OU AVAIT ACCEPTE L'INSTALLATION D'UN CORRECTIVE PACK OU HOTFIX DONT L'IMPLEMENTATION EST RECOMMANDEE PAR MEGA.

DEFINITIONS

TERME	DEFINITION
1. Développement Spécifique / Paramétrages	Développement spécifique ou paramétrage du progiciel HOPEX consistant à modifier son fonctionnement selon des besoins fonctionnels spécifiques du Client. Les modifications peuvent porter sur : la structure de données, les écrans, les workflows, les règles d'accès aux données, les interfaces nécessitant des développements, les exports spécifiques tels qu'un intranet ou des rapports complexes nécessitant de la programmation. La gestion des utilisateurs et les configurations faites par les utilisateurs finaux (préférences d'affichage, requêtes, rapports) ne sont pas considérées comme des customisations, mais des actes de configuration simples du progiciel standard
Erreur	Fonctionnement non-conforme du Service par rapport à la Documentation du Service. Toute erreur doit être reproductible, présenter des symptômes clairement identifiables et entraîner des conséquences fonctionnelles sur le Service standard.
Solution de Contournement	Désigne un mode de fonctionnement alternatif permettant de résoudre une Erreur.
Incident	Comportement ne faisant pas partie du fonctionnement normal du Service, qui cause ou peut causer une interruption de la production chez le Client ou une baisse de la qualité du Service.
Case	Instance utilisée par le Support technique de MEGA pour suivre un Incident signalé par le Client.
Période d'applicabilité du SLA	Désigne la période définie au Bon de Commande.
Période d'indisponibilité du Service ou Interruption	Désigne la période inclue dans la période d'applicabilité du SLA durant laquelle le Service n'est pas disponible aux utilisateurs.
Release ou Nouvelle Version	Désigne une nouvelle version du Progiciel, introduisant notamment de nouvelles fonctionnalités ou modules.
Correction	Les Corrections sont regroupées dans un Service Pack ou parfois fournies par le biais de Mises à jours cumulées.
Service Pack	Désigne les mises à jour afin de rendre le progiciel HOPEX plus fiable. Un SP fournit un ensemble cohérent de corrections, ainsi que des améliorations de la sécurité et des performances applicable à une release.
2. Mises à jour cumulées	Désigne un groupe de Corrections créé et fourni par MEGA en dehors du contexte d'une Release ou d'un Service Pack. Les Mises à jour cumulées répondent généralement à des Erreurs critiques et ne peuvent être installés que sur le dernier SP d'une Release.

ACCES AU SERVICE

L'accès au Service est limité aux seules adresses IP prédéfinies et fournies par le Client. Ces adresses IP doivent être publiques (routables), statiques et répertoriées.

3. Les utilisateurs itinérants se connectent en premier lieu à un site relais du Client qui leur fournira une adresse IP dont l'accès est autorisé par MEGA, pour ensuite pouvoir se connecter au Service.

Le Client s'engage à signaler sans délai à MEGA tout incident concernant l'accès au Service. Le Client accepte également de ne pas volontairement perturber le Service, y compris les serveurs de MEGA ou les serveurs des fournisseurs d'hébergement par quelque moyen que ce soit et de se conformer aux recommandations, procédures et règles qui lui seront communiquées par MEGA pendant la durée du contrat.

INFORMATIONS D'IDENTIFICATION DE L'UTILISATEUR

MEGA fournit au Client les informations nécessaires afin de permettre à l'administrateur du Client de créer les identifiants pour ses autres utilisateurs.

Le Client doit mettre en œuvre toutes les mesures nécessaires afin de garantir la confidentialité des identifiants des utilisateurs. MEGA ne pourra être tenue responsable de tous dommages découlant de l'utilisation du Service par un tiers non-autorisé. En cas de perte ou divulgation par un utilisateur de ses informations de connexion à un tiers non-autorisé, le Client notifie MEGA par écrit et sans délai. Pour des raisons de sécurité, MEGA peut à tout moment imposer au Client le changement d'un mot de passe ou la suppression d'un identifiant sans son accord préalable.

DISPONIBILITE DU SERVICE

MEGA fait ses meilleurs efforts afin que la plateforme soit accessible dans les conditions stipulées aux présentes, sauf :

- Pendant les périodes de maintenance. La maintenance planifiée fait l'objet d'un préavis raisonnable, alors qu'une maintenance non planifiée fera l'objet d'un préavis de 1 jour ouvré (hors Incidents liés à la sécurité).
- A la suite de toutes circonstances extérieures à MEGA, telles que la perturbation d'Internet et tout autre événement figurant à l'article « Force Majeure »,
- En cas d'un quelconque problème de sécurité, tel que l'utilisation anormale, frauduleuse ou abusive du Service par le Client, toute intrusion, accès frauduleux au Service par un tiers, ou extraction illégale de tout ou partie des données, etc.

MEGA mettra en œuvre tous les moyens possibles pour en minimiser les conséquences et rétablir le Service après la cessation des causes susvisées.

DISPONIBILITE DU SERVICE	DEVELOPPEMENT	PRODUCTION
Durée d'interruption non planifiée maximale par occurrence	1 jour ouvré	3 heures ouvrées
Interruption non planifiée maximale par mois	1 jour ouvré	4 heures ouvrées

Toutes les périodes d'indisponibilité sont prises en compte dans le calcul de la durée d'interruption présentée ci-dessus, à l'exception :

- Des périodes d'indisponibilité planifiées, par exemple les périodes autorisées au préalable par le Client dans le cadre d'opérations de gestion du changement
- Des périodes d'indisponibilité non planifiées résultant des conditions d'exclusion de responsabilité stipulés dans la présente clause.

L'interruption est calculée à partir du moment où le Client contacte MEGA : déclaration d'un *No Access* depuis le portail d'enregistrement des incidents de notre Community (https://community.mega.com).

En cas de non-respect des engagements de disponibilité, le Client peut demander l'octroi d'un avoir de service. Un avoir de Service représente le nombre de jours de Service supplémentaires (venant s'ajouter à la période d'abonnement souscrite par le Client) accordé au Client au titre de l'indisponibilité de Service. Tout avoir de Service doit faire l'objet d'une demande écrite du Client. Cette demande doit être faite dans un délai de 3 mois, à compter de la fin de l'évènement générateur. L'avoir de Service représente le seul et unique recours du Client en cas d'indisponibilité du Service.

La Période de disponibilité du Service est de 9h à 18h, du lundi au vendredi, hors jours fériés du territoire concerné. La time zone applicable est celle de la localisation de la filiale de MEGA avec laquelle le Client a conclu le contrat.

5. LIMITATION DE LA RESPONSABILITE DE MEGA

La responsabilité de MEGA est limitée ou exclue dans les cas suivants :

- Non-respect par le Client des instructions d'utilisation du Service contenues dans la Documentation et le guide utilisateur.
- Dégradation des performances dues à la configuration et aux équipements de sécurité du Client.
- Disfonctionnement du Service dû à un logiciel installé dans le système informatique du Client.
- Indisponibilité du contact Client durant la période d'interruption du Service.
- Refus du Client de fournir rapidement des informations (ou l'autorisation pour y accéder) susceptibles d'aider le Service de Support MEGA à traiter l'Incident.

6. SEVERITE DES INCIDENTS ET TEMPS DE REPONSE

SEVERITE	SITUATION	TEMPS DE REPONSE & ATTENTES
Aucun accès	Problèmes de sécurité Plateforme hors-service/aucun accès pour tous les utilisateurs	1 heure ouvrée
Critique	Dégradation significative d'une ou plusieurs fonctionnalités Impact business critique	Client contacté dans un délai de 4 heures ouvrées. Effort continu quotidien pendant les heures ouvrées. Escalade rapide au sein du service du Support Technique et aux Product Managers. Affectation rapide des ressources appropriées. Présentation d'un plan d'action. Selon la complexité de l'Erreur, une première solution ou une Solution de Contournement pourra être fournie afin de diminuer au maximum les perturbations opérationnelles.
Modéré	Dégradation d'une fonctionnalité. Le travail peut se poursuivre de manière satisfaisante, mais altérée. Impact business modéré	Client contacté dans un délai de 1 jour ouvré. Affectation des ressources afin de maintenir un effort constant pendant les heures ouvrées. Un plan d'action peut être fourni.
Mineur	Dégradation mineure d'une ou plusieurs fonctionnalités. Aucun impact sur le business.	Client contacté dans un délai de 2 jours ouvrés. Meilleurs efforts fournis pendant les heures ouvrées.

Le temps de réponse est calculé à partir du lendemain du moment où le Client informe MEGA de la survenance de l'Erreur via le portail d'enregistrement des incidents accessible depuis notre Communauté en ligne (https://community.mega.com).
Le support technique de MEGA est susceptible d'abaisser le niveau de sévérité si le Client n'est pas en mesure de fournir les ressources ou les réponses nécessaires pour permettre à MEGA de poursuivre ses efforts pour résoudre l'Incident.
Les Services de Support standard ne comprennent pas l'assistance sur site. Dans des cas spécifiques, et après approbation par le Client des conditions techniques et financières de l'intervention de MEGA, MEGA pourra intervenir sur le site du Client à sa discrétion. Le Client devra permettre à MEGA d'accéder sans frais aux ressources informatiques du Client et mettra à la disposition de MEGA du personnel suffisamment qualifié pour lui communiquer toutes les informations dont elle aurait besoin. Le Client met à la disposition de MEGA les données nécessaires au support et s'assure de disposer de l'ensemble des droits de propriété intellectuelle sur les éléments tiers mis à la disposition de MEGA.

CYCLE DE VIE DU PRODUIT

DEFINITION	DESCRIPTION
Release	Nouvelle version de HOPEX maintenue pendant les périodes suivantes : en Full Support pour une durée de 27 mois, puis en Limited Support pour une durée de 9 mois, et régulièrement enrichie par des Services Packs. Les durées de support applicables pour chaque version sont indiquées dans la Support Policy de la communauté MEGA.
Full Support	Désigne la période au cours de laquelle le Client bénéficie des Services de Maintenance et de Support incluant l'amélioration des fonctionnalités existantes, nouvelles fonctionnalités et produits, et la fourniture de Corrections.
Limited Support	Désigne la période consécutive à celle du Full Support, au cours de laquelle le Client bénéficie uniquement des Corrections des Incidents Critiques, sous forme de Corrections uniquement.

7.

SAUVEGARDE ET PLAN DE REPRISE D'ACTIVITE (Option PRA avancé)

8.1. Sauvegarde.

8. Au titre des services (non-optionnels) d'hébergement, MEGA s'engage à réaliser le nombre de sauvegardes des données indiqué dans le présent article.
En cas de sinistre affectant ses serveurs d'hébergement, MEGA s'engage à rétablir les Services dans les délais définis dans la présente annexe.
Par défaut, la restauration s'effectue à partir de la dernière sauvegarde réalisée. Toutes les autres sauvegardes conservées selon les modalités figurant dans la présente annexe sont considérées comme des archives et peuvent donner lieu à une restauration.

SAUVEGARDES	QUOTIDIENNE	HEBDOMADAIRE	MENSUELLE
Durée de conservation des sauvegardes à compter d'une sauvegarde périodique	7 jours	4 semaines	6 mois
Temps de restauration	Dernière sauvegarde : 4 heures ouvrées Archive : 6 heures ouvrées		

8.2. Plan de Recouvrement d'Activités (Option PRA avancé).

Le Client peut bénéficier d'un Plan de Recouvrement d'Activités avancé en cas d'Erreur ayant altéré une base de données ou d'un sinistre affectant les serveurs informatiques hébergeant la Plateforme, les Solutions et/ou les données du Client.

MEGA s'engage :
- A réaliser des sauvegardes des données du Client selon une fréquence prédéfinie. Cette fréquence désigne la dernière sauvegarde réalisée à partir de laquelle MEGA effectuera son plan de reprise (RPO),
- A restaurer les données du Client à partir de la dernière sauvegarde réalisée dans le délai défini ci-après. Ce délai désigne le temps de reprise (RTO) qui est nécessaire à MEGA pour le rétablissement des Services.

Le Client peut souscrire, s'il le souhaite, à une option « Advanced DRP » pour bénéficier de sauvegardes à une fréquence plus élevée et/ou d'un délai de rétablissement des Services plus court.

9.

	Objectif de temps de reprise (RTO)	Objectif de Plan de reprise (RPO)
Offre Standard	1 semaine	25 heures
Avec l'option "Advanced DRP"	24 heures	25 heures

TESTS DE PÉNÉTRATION

MEGA effectuera chaque année des tests de pénétration. Ces tests seront effectués sur les versions existantes en Full Support (dernier Service Pack) au jour des tests de pénétration. Toute autre demande du Client pourra faire l'objet d'un devis complémentaire. MEGA fournira au Client, sur demande, une « opinion letter » et un rapport de synthèse relatif aux dits tests.

SERVICE REQUEST

10.1. Service Request

Une Service Request est une demande formalisée d'intervention sur la ou les plateformes SaaS du Client.
Les seules personnes habilitées à faire des Services Request sont celles désignées par le Client comme « Contacts de MEGA ».

Le champ d'application initial ainsi que les Services Requests disponibles sont en fonction du **SaaS Platform Package** auquel le Client à souscrit :

- Starter
- Standard
- Advanced.

Au début du Service, chaque Client reçoit une base de référence et peut demander des services supplémentaires dans les limites suivantes :

SaaS Platform Package		Starter	Standard	Advanced
Production		Oui	Oui	Oui
Pre-Production		Oui * Uniquement pour la gestion des versions	Oui	Oui
Développement		Non disponible	Oui	Oui
Portail HOPEX 360		(Option)	1	1
Base de référence				
Instance HOPEX		1 instance and 1 répertoire par défaut (avec 2 répertoires maximum)		
Accès au Service		IP Whitelist ou Web Application Firewall (WAF, selon le SaaS Package, ou disponible en option)		
Authentification		SSO (SAML 2.0, OpenID Connect) & HOPEX Authentication		
Stockage de données		20 Go		
Service Request inclus		**Fréquence/Quantité MAX**		
Catégories de Service	**Type de Service Request**	**Starter**	**Standard**	**Advanced**
Gestion des Customisations	Up-alignment (Passage en Production)	1 par an	4 par an	12 par an
	Down-alignment	1 par an	4 par an	12 par an
Gestion des Utilisateurs	Export des logs de connexion	1 par mois	1 par mois	1 par mois
	Réassigner les utilisateurs/profil à un jeton de licences (nommée)Reassign a user/profile to a token license (named)	5 réassignations par an	10 réassignations par an	20 réassignations par an
Gestion des Accès	Modification du nom de domaine du service	Configuration initiale + 1 modification par an	Configuration initiale + 1 modification par an	Configuration initiale + 1 modification par an
Gestion de l'intégration	Planification des tâches	2 demandes par an	4 demandes par an	6 demandes par an
	Nombre de connexions via une API/WebService disponibles	Jusqu'à 1	Jusqu'à 3	Jusqu'à 6
HOPEX Store	Déploiement d'un module	10 demandes par an	10 demandes par an	10 demandes par an

Tout changement dans la fréquence et/ou la quantité maximale des services requests fait l'objet d'un accord commercial et de frais supplémentaires.
Toute Service Request additionnelle en plus du celles décrites au-dessus (indiquées au catalogue ci-dessous) fera l'objet d'une facturation complémentaire.
Toute demande de Service Request non-listée feront l'objet d'une approbation par MEGA et pourront être rejetées pour des raisons de sécurité. Elles feront l'objet d'un devis.

Aucun logiciel tiers ne sera déployé en dans les environnements de Production/Pré-production.
Tous logiciels tiers nécessaires pour les Développements (y inclus mais sans s'y limiter Word, Excel, etc.) feront l'objet de redevances supplémentaires.
Veuillez noter qu'aucun environnement de développement intégré (IDE) ne sera autorisé (ni en Développement).

10.2. Niveau de Service Request

Catégorie de Service	Nom du Service	Description du Service	Fréquence/ Quantité max	Garantie temps intervention
Gestion des versions	Mise à jour applicative	Déployer une mise à jour HOPEX sur l'une des plateformes SaaS (DEV ; PRE-PROD ; PROD) ; HotFix, Correctif Patch, Version.	4 par an	HotFix, Corrective Patch 2 jours ouvrés (PPROD en premier) Version Doit être planifié à l'avance
Gestion des utilisateurs	Log de connexion des utilisateurs	Fournir un fichier log (format TXT) indiquant toutes les connexions des utilisateurs, notamment les licences d'utilisateur, les noms d'utilisateur, les profils ainsi que la disponibilité de la plateforme.	1 par mois	1 jour ouvré
	Réaffecter un utilisateur/profil à une licence jeton	Dans le cadre des licences nommées, il est possible de réaffecter un utilisateur à un modèle de licence basé sur jeton. Un utilisateur peut être : utilisateur principal, contributeur ou lecteur. Ce service ne s'applique pas aux licences flottantes.	10 réaffectations (tous utilisateurs confondus) par an	
Gestion des accès	Modifier le nom de domaine du service	Modifier l'URL d'accès à HOPEX Cloud d'un nom de domaine « aaa.hopexcloud.com » à un autre « bbb.hopexcloud.com ».	2 modifications par an	2 jours ouvrés
	Déclarer des plages d'adresses IP supplémentaires sur la liste d'accès autorisés	Ajouter jusqu'à 5 plages d'adresses IP supplémentaires sur la liste des adresses IP dont l'accès au Progiciel HOPEX est autorisé.	3 demandes par an	1 jour ouvré
Gestion de l'intégration	Planification de tâches	Planification de tâches récurrentes avec transfert amont ou aval (si applicable) vers et depuis l'environnement du Client en utilisant un « Secure File Transfer Protocol » (« SFTP » en anglais). Les tâches planifiées concernent principalement des imports/exports et la génération de site web statique. La conception, la réalisation et la validation des éléments à planifier reste sous la responsabilité du Client.	6 demandes par an	2 jours ouvrés (PPROD en premier)
	Déploiement de Web Services	Déployer un web Services en production. La conception, la réalisation et la validation d'un Web Services reste sous la responsabilité du Client.		3 jours ouvrés (PROD en premier)
HOPEX Store	Déploiement d'un module	Liste des modules evolutives : https://store.mega.com/modules	10 demandes par an	2 jours ouvrés (PPROD en premier)

Les services requests sont soumis au présent Accord de Niveaux de Service.

De plus, l'engagement de MEGA au titre des services requests n'est garanti que si :
- Le service request est ouvert depuis le site Portail des Incidents de la MEGA Community (aucune demande de service request adressée par mail ne sera traitée) ;
- Le « Contact de MEGA » reconnait avoir fourni à MEGA toutes les informations nécessaires à la mise en œuvre d'un service request. Le temps nécessaire à la collecte de ces informations sera décompté.

[11] Pour les demandes ne figurant pas dans le catalogue de Service Request :
- Estimation du temps de réponse dans les 2 jours ouvrés
- Etude et traitement en fonction de la demande

CONTACTS ET GOUVERNANCE

Le Client doit avoir au maximum trois (3) personnes qui doivent être formées aux solutions HOPEX, pour seuls contacts de MEGA pour recevoir les Services de Support. Ces contacts se doivent d'être en mesure de réaliser a minima les fonctions suivantes :
- Gérer les utilisateurs et leurs assignations aux différents profils des solution(s) Hopex ;
- En cas d'Incident :
  - Déclarer un « Case » sur le portail MEGA en fournissant toutes les informations concernant les conditions dans lesquelles l'Incident s'est produit
  - Si un problème de sécurité apparaît, contacter immédiatement MEGA par le moyen le plus approprié qu'il soit.
- Pour une plus grande efficacité opérationnelle, participer aux réunions de direction et d'arbitrage organisés par MEGA

REVERSIBILITE

A compter de la date de résiliation ou d'expiration de la souscription, les données du Client sont conservées pour une période de 3 mois. Pendant cette période, le Client n'a plus accès aux Services. Ce délai a pour objet de laisse au Client le soin de mettre en place une éventuelle réversibilité. A l'issue de cette période de 3 mois, les données sont supprimées définitivement.

Le Client peut solliciter :

- Soit une conservation des données pour une période allant au-delà de ladite période de 3 mois.
- Soit la mise en place d'une prestation de réversibilité, telle que définie ci-après.

Toute demande de prorogation de la durée de conservation ou de mise en place de prestations de réversibilité doit parvenir à MEGA au plus tard dans les 2 mois avant la date d'effectivité de la résiliation ou de l'expiration des Services.
La prolongation de la conservation et/ou les prestations de réversibilité est facturée au tarif en vigueur au jour de ladite demande.

La réversibilité est une prestation ayant pour objet la récupération par le Client de ses données contenues dans le référentiel HOPEX.

MEGA propose deux types de prestations de réversibilité : la réversibilité simple et la réversibilité complexe.

- Réversibilité Simple : Cette réversibilité a pour objet la fourniture des sauvegardes des données de production pour restauration dans la même version de SGBD MS-SQL-Server pour utilisation avec la même solution applicative dans la même version.
  Le fichier est (i) soit mis à disposition du Client sur un Serveur FTP de MEGA pour téléchargement, (ii) soit envoyé au Client sur un serveur qu'il désigne à cet effet.
  Le Client doit disposer des licences nécessaires pour pouvoir accéder aux informations du référentiel. MEGA lui conseille de suivre les formations d'administration de la solution.

- Réversibilité Complexe : Cette réversibilité est mise en œuvre dans les cas où la réversibilité simple n'est pas applicable. Ce peut être la récupération des données pour rechargement dans une solution logicielle alternative.
  Cette réversibilité a pour objet la fourniture :
  - D'un export XML encodage UTF-8 du contenu de la base de données au format propriétaire ;
  - Le transfert de compétence fonctionnel et technique vers l'équipe en charge de la reprise, pour la compréhension du modèle de données de la solution, des spécificités de la solution mise en place et de l'export fourni.

  La validation de la cohérence des données reprises ainsi que son intégration dans le nouvel outil sont à la charge de l'équipe du Client.
  Cette prestation de réversibilité peut être proposée sous la forme d'un forfait.

Autre Réversibilité : Pour tout autre demande du Client, ce dernier devra adresser à MEGA un cahier des charges détaillé afin de permettre à MEGA de procéder à une étude de faisabilité et, le cas échéant, lui adresser un devis.

13. COMPUTATION DES DELAIS

Lorsqu'un délai est exprimé en heures, il se calcule, 7 jours sur 7 et 24 heures sur 24.
Lorsqu'un délai est exprimé en heures ouvrées, il se calcule pour chaque jour ouvré, de 9 heures à 18 heures, heures françaises.
L'heure de l'acte, de l'événement, ou de la notification qui fait courir le délai ne compte pas.

Lorsqu'un délai est exprimé en jours ouvrés, il se calcule en prenant compte uniquement les jours de la semaine, du lundi au vendredi, sauf les jours fériés ou chômés en France.
Le jour de l'acte, de l'événement, ou de la notification qui le fait courir ne compte pas.

Lorsqu'un délai est exprimé en mois, il se calcule de quantième à quantième.
Le jour de l'acte, de l'événement ou de la notification qui fait courir le délai ne compte pas.
A défaut d'un quantième identique, le délai est prolongé jusqu'à la fin du premier jour ouvrable qui suit, à minuit.

Lorsqu'un délai est exprimé en heures, il expire à la fin de l'heure considérée.
Lorsqu'un délai est exprimé en jours ou en mois, il expire le dernier jour à vingt-quatre heures.
Le délai exprimé en jours qui expirerait normalement un samedi, un dimanche ou un jour férié ou chômé, est prolongé jusqu'à la fin du premier jour ouvré qui suit, à minuit.

Pour toute notification faite par lettre recommandée avec accusé de réception, il est tenu compte de la date de première présentation de ladite lettre recommandée avec accusé de réception, cachet de la poste faisant foi.

ENGAGEMENTS EN TERME DE SECURITE

14.1. Sécurité générale

OBJET	DESCRIPTION
TLS	Requis sur les plateformes HOPEX Cloud afin d'assurer la sécurité des transactions entre le web front-end et le terminal du Client. Le certificat basé sur le chiffrement TLS 1.2 AES256-SHA256 est entièrement à la charge de l'équipe du MCS (MEGA Cloud Services).
Autorisation des IP publiques	Les adresses IP publiques des clients doivent être préalablement fournies à MEGA afin d'accéder aux services.
Plateforme dédiées	Chaque instance HOPEX des clients sont installées sur un serveur dédié isolé les uns des autres au sein d'un VLAN distinct.
Plateformes virtuelles isolées les unes des autres	Les plateformes HOPEX Cloud sont déployées en mode standard avec un serveur virtuel par client pour l'environnement de Production. En cas de souscription au niveau de Services « SaaS Platform Package » Standard ou Premium, trois instances isolées les unes des autres sont déployées, tels que : • DEVELOPPEMENT : instance dédiée permettant au Client de personnaliser les solutions HOPEX et de tester les mises à jour ; • PRE-PRODUCTION : l'instance HOPEX dédiée sera synchronisée à la demande avec celle de Production afin de permettre au Client de valider et tester les mises à jour avant d'être implémentées en Production (ex : Configuration, mises à jours cumulées, CP) ; • PRODUCTION : le contenu déployé en Production est préalablement testé et approuvé sur l'instance de PRE-PRODUCTION.
Chiffrement des données	Les espaces de stockage sont chiffrés AES-256 bits via la solution Microsoft Azure SSE (Storage Service Encryption).

14.2. Organisation et gestion de la sécurité de l'information.

OBJET	DESCRIPTION
Organisation de la sécurité et de la gestion des risques associées à l'information	MEGA a mis en place une politique de sécurité de l'information incluant tout son personnel. Les principaux rôles du personnel MEGA sont les suivants : • La direction approuve, encourage et veille à améliorer la sécurité du système d'information ; • Le responsable sécurité du système d'information (RSSI) est responsable de la sécurité, de la disponibilité et de l'intégrité du système d'information ; • Le directeur du système d'information (DSI) est chargé de l'exploitation et de l'orientation stratégique du système d'information ; • Les comités de sécurité sont formés pour répondre aux questions de sécurité, de risques, d'incidents et de manquements.
Gestion des risques de l'entreprise	MEGA a conçu et mis en place un programme de gestion des risques d'entreprise afin d'analyser et de réduire les risques de façon proactive sur l'ensemble des activités MEGA.
Audit indépendant des contrôles sécurité	L'offre HOPEX Cloud Enterprise fait l'objet d'un audit annuel SOC2 de la part d'un tiers indépendant.

14.3. Politiques de sécurité du système d'information.

OBJET	DESCRIPTION
Politique de sécurité du système d'information	Il s'agit de la politique de sécurité du système d'information mise en place et validée par la direction de MEGA et communiquée aux parties concernées. Ce document est révisé chaque année.
Procédures et politiques	Les politiques relatives à la sécurité de l'information (classification des données, cryptographie, mot de passe, etc.), les normes, les procédures et les directives sont publiées sur l'intranet, revues et communiquées sur une base annuelle.
Certification SOC 2 Type 2	MEGA certifie qu'au jour de la signature du Contrat, les services sont conformes aux critères de la certification SOC2 Type 2. MEGA ne s'engage pas à maintenir cette conformité tout au long du contrat.

14.4. Gestion des ressources.

OBJET	DESCRIPTION
Responsabilités des ressources informatiques	MEGA identifie les ressources informatiques (inventaire, propriété, utilisation acceptable et restitutions) et définit les devoirs de protection appropriés.
Classification de l'information	MEGA dispose d'une politique de classification documentée traitant notamment du niveau de classification des documents, mails etc. de leur création, leur impression, leur stockage, leur transmission ainsi que de leur destruction.
Traitement des supports de stockage	MEGA a effectué un renforcement de ses règles de sécurité pour l'ensemble des équipes informatiques du MCS. Aucun dispositif de stockage amovible n'est autorisé sur les plateformes.

14.5. Sécurité des ressources humaines.

OBJET	DESCRIPTION
Avant l'embauche	MEGA effectue des contrôles et vérifications nécessaires pour tous les candidats à l'embauche, conformément aux lois, aux réglementations et à l'éthique applicables et proportionnés aux besoins de l'entreprise, à la classification des informations accessibles et aux risques perçus.
Au cours de l'emploi	Les employés MEGA et les utilisateurs externes suivent un programme de sensibilisation à la sécurité. Ils reçoivent des instructions, une formation ainsi que des mises à jour régulières en matière de politiques et de procédures de sécurité dans la mesure où leur fonction l'exige.
Fin ou changement d'emploi	MEGA a mis en place un processus RH afin de gérer toute fin de contrat ou de changement d'emploi.

14.6. Sécurité physique et environnementale.

OBJET	DESCRIPTION
Zones sécurisées	MEGA a établi des périmètres et des mesures de sécurité physiques afin de protéger les zones qui traitent et contiennent des informations considérées comme sensibles et/ou critiques.
Equipement	MEGA a mis en place des mesures physiques pour protéger ses équipements des accès non autorisés et des coupures de courant. Tous les supports de stockage sont analysés avant d'être réutilisés ou décommissionnés afin de garantir que les données sensibles et les logiciels sous licence ont été supprimés ou écrasés de manière sécurisée. MEGA a adopté une politique de sécurité de l'information sur les postes de travail : protection des documents papiers et supports de stockage amovibles, verrouillage d'écran. L'offre HOPEX Cloud Enterprise repose sur les infrastructures Microsoft Azure, répondant à un large éventail de normes de conformité internationales spécifiques à l'industrie, telles que ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, ainsi que des normes propres à chaque pays, telles que Australia IRAP, UK G-Cloud, and Singapore MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

14.7. Contrôle d'accès.

OBJET	DESCRIPTION
Contrôle d'accès	La politique globale d'accès MEGA repose sur le principe du moindre privilège. Des revues périodiques sont établies par le RSSI (Responsable de la Sécurité des Systèmes d'Information).
Gestion des accès utilisateurs	L'administration des plateformes HOPEX Cloud n'est accessible que par l'équipe MCS (MEGA Cloud Services) par le biais d'un serveur bastion enregistrant (log et vidéo) toutes les actions réalisées sur les plateformes client. L'adresse IP publique du Client doit être au préalable fourni au service MCS afin de joindre le service.
Responsabilités des utilisateurs	Chaque client dispose d'un accès Administrateur Fonctionnel HOPEX, permettant entre autres de gérer l'ensemble des utilisateurs au sein du référentiel HOPEX. Celui-ci constitue également le point de contact principal entre votre organisation et MEGA.
Contrôle d'accès des systèmes et applications	L'authentification au service HOPEX Cloud peut être réalisé par le biais d'un SSO utilisant notamment les protocoles SAML 2.0, OpenID Connect (OIDC).

14.8. Sécurité opérationnelle – sécurité du système.

OBJET	DESCRIPTION
Procédures opérationnelles et responsabilités	L'ensemble des procédures documentées du MCS suivent notamment les bonnes pratiques ITIL permettant de maintenir les plateformes clients dans les meilleures conditions opérationnelles.
Protection contre les programmes malveillants	MEGA a mis en place des mécanismes de détection, de prévention et de contrôle afin de contrer tous programmes malveillants. Ces mesures techniques s'accompagnent d'une sensibilisation des administrateurs à la sécurité.
Sauvegarde	Des sauvegardes automatiques sont réalisées de façon régulière sur les plateformes HOPEX Cloud afin de pouvoir restaurer les données de production des clients en cas d'incident.
Enregistrement et contrôle	Au sein des plateformes HOPEX Cloud, en plus de l'outil de contrôle HOPEX Server Supervisor embarqué nativement par la solution et permettant aux administrateurs HOPEX de suivre chaque action menée sur le système (ex : authentifications réussies/échouées, modifications des utilisateurs/des droits etc.), tous les fichiers journaux de la plateforme sont enregistrés et soumis à analyse via une solution tierce du MCS. L'équipe MCS contrôle continuellement la disponibilité des plateformes clients à l'aide un dispositif notifiant les administrateurs en cas d'anomalie.
Contrôle des opérations logicielles	MCS gère le système d'information selon les recommandations ITIL (Gestion des changements, etc.).
Gestion de la vulnérabilité technique	Le service MEGA R&D utilise la solution Coverity pour l'analyse du code source d'HOPEX (contrôle journalier). De plus un audit est réalisé par une tierce partie sur chaque version majeure. Au niveau infrastructure, MEGA a élaboré un processus de gestion des menaces et de vulnérabilité des systèmes, logiciels et applications afin de réduire les risques d'exploitation et de nuisance.
Considérations relatives à l'audit des systèmes d'information	Maintenance programmée (OS, matériel, etc.) : maintenances système et logicielle réalisées durant le weekend. Maintenance non programmée : Correctifs de sécurité HOPEX (patchs), personnalisations ou déploiement de mises à jour critiques réalisés en dehors des horaires habituels et planifiés avec le Client.

14.9. Sécurité communication et réseau.

OBJET	DESCRIPTION
Gestion de la sécurité réseau	Toutes les instances HOPEX des clients sont dédiées. Chaque instance HOPEX client est installée sur un serveur dédié isolé les uns des autres au sein d'un VLAN distinct. Chaque serveur dispose de son propre pare-feu (MS Azure Network Security Group) permettant de renforcer et contrôler le trafic réseau.
Transfert d'information	Les transactions web sont obligatoirement chiffrées TLS afin de sécuriser les transactions entre le(s) serveur(s) web et le(s) site(s) client. Le certificat TLS 1.2 basé sur un chiffrage de type AES256-SHA256 est entièrement géré par le service MCS (MEGA Cloud Services). De plus, les adresses IP publiques du Client doivent être préalablement fournies à MEGA afin de joindre le service. Cette mesure technique s'accompagne d'une sensibilisation des administrateurs à la sécurité des données et d'un accord de confidentialité et de non-divulgation. Dans le cas d'un transfert données, les données doivent transiter via un transfert de type SFTP.

14.10. Acquisition de système, développement et maintenance.

OBJET	DESCRIPTION
Exigences de sécurité des systèmes d'information	MEGA livre des versions majeures tous les 18 à 24 mois ainsi que des Services Packs tous les 3 mois qui incluent des correctifs de sécurité.
Sécurité des processus de développement et de support	Le design d'HOPEX est entièrement conçu par MEGA. MEGA R&D a un SSM (Software Security Manager) chargé de : • Définir les meilleures pratiques de codage du point de vue de la sécurité ; • Vérifier les spécifications de projets de développement du point de vue de la sécurité ; • Gérer le développement de modules relatifs à la sécurité (authentification, etc.) ; • Gérer les campagnes d'analyse de code et le suivi des mesures d'atténuation. MEGA ne fait pas appel à la sous-traitance pour développer ses solutions. Dans le cas où des clients souhaitent personnaliser la plateforme HOPEX (ex : changements dans le métamodèle), le niveau de services « SaaS Platform Package » Standard ou Premium est nécessaire.
Données de test	MEGA utilise une base de test avec des données factices.

14.11. Sécurité de l'information dans la gestion de la continuité des opérations.

OBJET	DESCRIPTION
Continuité de la sécurité de l'information	L'intégrité des données est garantie par la technologie Geo-Redundant Storage (GRS) des plateformes Microsoft Azure permettant de sauvegarder les données dans un second datacenter avec un niveau de sécurité identique au site principal.
Redondance	MEGA a mis en place les dispositifs nécessaires pour assurer une haute disponibilité des services.
Plan de continuité d'activité	MEGA a conçu et mis en place un plan de continuité d'activité, qui établit 9 scénarios de haut niveau susceptibles de compromettre la continuité des activités, ainsi que des réponses prédéfinies pour traiter les problèmes de façon optimale.

14.12. Gestion des incidents de sécurité de l'information.

OBJET	DESCRIPTION
Incidents de sécurité de l'information et des améliorations	MEGA a mis en place un processus de gestion des incidents afin de pouvoir restaurer aussi vite que possible un service opérationnel normal et minimiser l'impact négatif sur les opérations métier, veillant ainsi à maintenir aussi haut que possible le niveau de qualité et de disponibilité du service. Ce processus inclut une procédure d'escalade.

14.13. Chiffrement et bastion

OBJET	DESCRIPTION
Chiffrement des supports de stockage	Les instances HOPEX des clients sont déployées sur des supports de stockage cryptés.
Bastion CyberArk	Les sessions d'administration des plateformes clients sont enregistrées au travers d'un bastion.

15. OPTIONS DES EXTENDED SERVICES

15.1. Premium Maintenance

MEGA propose plusieurs Services SaaS disponibles sur option, notamment la Premium Maintenance, l'Adoption Package et l'Hopex Administration, qui sont décrits ci-après. Ces services, dénommés Extended Services, ont pour objet de fournir au Client un support premium et d'autres services post-implémentation.

Objet	Description
Premium Support	
Suivi mensuel	Suivi mensuel des Cases et de leur avancement avec un point de contact unique.
Suivi des indicateurs de performance	Suivi mensuel des indicateurs de performance, notamment le nombre de Cases traités et encore ouverts et les niveaux de service.
Maintenance des spécifiques	
Correction et documentation des personnalisations	Maintien en conditions opérationnelles des personnalisations faites par MEGA, y compris suite aux mises à jour applicatives (CP / nouvelles versions).
Gestion des mises à jour	
Validation des mises à jour fonctionnelles	Validation fonctionnelle de la configuration après la migration vers la dernière version de HOPEX.
Gestion de l'impact des versions mineures sur les utilisateurs	Evaluation de l'impact du changement sur les utilisateurs. Cela comprend par exemple la communication vers les utilisateurs et l'identification de leurs besoins de formation complémentaire.

15.2. Adoption Package

Objet	Description
Évaluation et suivi de la maturité	
Ateliers d'évaluation de la maturité	Ateliers fonctionnels annuels ayant pour objet d'améliorer l'adoption, l'utilisation et la démonstration de la valeur d'Hopex, sur la base de la méthodologie d'évaluation de la maturité MEGA, incluant l'intervention de consultants avant-vente, d'experts métiers ou techniques et d'un Customer Success Manager.
Suivi des recommandations	Suivi de l'adoption d'HOPEX au moyen d'indicateurs clés et mise en œuvre des recommandations des experts.
e-Learning	
Sessions d'e-learning	Sessions d'e-Learning afin de faciliter et d'augmenter l'adoption d'HOPEX au sein de l'équipe

15.3. Managed Services

Objet	Description
Gestion des accès	
Gestion du mode d'authentification HOPEX	Gestion du mode d'authentification des utilisateurs d'HOPEX.
Gestion des rôles métier	Attribution des rôles métier. Un rôle métier définit la fonction d'une personne ou d'un groupe de personnes dans l'entreprise. Un rôle métier est défini au niveau d'un référentiel.
Gestion des groupes de personnes	Création, suppression et configuration des groupes de personnes ayant des caractéristiques de connexion communes.
Gestion des accès/groupes d'utilisateurs	Création, suppression, configuration des utilisateurs, des groupes d'utilisateurs, des profils d'utilisateurs, des niveaux d'accès et d'autorisation.
Définition des règles d'accès aux données	Création, suppression et configuration des structures d'autorisation des utilisateurs
Réinitialisation d'un mot de passe utilisateur	Initialisation/réinitialisation d'un mot de passe utilisateur dans le cadre du mode d'authentification MEGA.

Gestion du contenu - Travail des Utilisateurs	
Gestion des doublons	Identification des doublons (en collaboration avec les propriétaires de la donnée), fusion ou suppression.
Gestion des objets isolés	Identification des objets isolés pour permettre l'attribution de leur propriété, l'identification pour la suppression, établir la liste des objets ne figurant pas dans les diagrammes (lorsqu'ils sont censés être décrits par des diagrammes), établir la liste des objets non-inclus dans les associations.
Gestion des suppressions des objets	Suppression des objets lorsque le modélisateur n'a aucun privilège afin de supprimer des objets créés en dehors de sa transaction courante. Les objets peuvent également être marqués pour être supprimés par les utilisateurs.
Gestion de la fusion d'objets	Fusion des doublons dans un référentiel.
Gestion du l'accès aux données	Configuration et gestion des niveaux d'autorisation des objets qui permettent/empêchent leur modification par un utilisateur/profil spécifique.
Gestion de la protection des objets	Activation et désactivation de la protection d'objets spécifiques dans un référentiel.
Gestion de contenu – Administration	
Comparaison et alignement de référentiels/ sous-ensembles de référentiels	Comparaison et promotion d'objets ou de groupes d'objets provenant de référentiels distincts. Le référentiel cible doit être aligné sur le référentiel source.
Sauvegarde logique d'un ensemble d'objets	Création d'une base de référence pour un ensemble d'objets (périmètre : bibliothèque, projet, etc.), permettant sa réplication dans un autre référentiel.
Gestion des librairies	Création et maintenance des bibliothèques et garantie d'avoir une structuration des données claire au sein du référentiel. Les bibliothèques peuvent être utilisées pour la séparation logique du contenu du référentiel.
Création de requêtes et de rapports	Rédaction de requête enregistrées et réutilisables par l'ensemble des utilisateurs de l'environnement. Configuration de rapport en s'appuyant sur les capacités de Report Studio.
Gestion des workflows	Gestion de la transition des workflows, prise en charge, approbation, autorisation et avancement des transitions. Contrôle des actions et réaffectations des workflows.
Import de données	Gestion de l'import régulier de données en utilisant les modèles existants.
Gestion des incidents	
Gestion du support interne	Gestion du premier niveau de support sur les Cases relatifs à l'utilisation fonctionnelle du client, dans un contexte de plateforme personnalisée.
Gestion du suivi des Cases	Création, priorisation et suivi des Cases avec le support technique de MEGA. Fourniture des éléments nécessaires pour diagnostiquer le problème reporté.
Coaching et support	
Bonnes pratiques	Fourniture des meilleures pratiques et des conseils standards sur l'utilisation de HOPEX
Reprise de modélisation existante	Gestion de la transcription manuelle de modèles existants (MS Word, PPT, Visio, ...) ou de données structurées (format XLS) vers HOPEX. Non applicable pour le chargement en masse.
Gestion de la maintenance des diagrammes	Mise à jour des diagrammes existants. Une telle mise à jour ne peut avoir lieu que sur la base d'une demande de changement formalisée. Gestion de l'impact sur les diagrammes des modifications apportées aux données du référentiel.
Modélisation	De l'interview du sachant à la validation des données et des diagrammes modélisés.
Intégration et formation des utilisateurs	Intégration et formation des nouveaux utilisateurs sur la base de la documentation et des supports de formation existants.
Evolution de l'existant	
Configuration	Evolution de la configuration existante.