DESCRIZIONE SAAS HOPEX

I SERVIZI QUI DESCRITTI SONO APPLICABILI SOLO ALLA VERSIONE STANDARD DI HOPEX. SE IL CLIENTE DESIDERA CHE SIANO APPLICABILI A SVILUPPI E PERSONALIZZAZIONI SPECIFICHE, DEVE SOTTOSCRIVERE L'OPZIONE DI MANUTENZIONE PREMIUM.

IL CLIENTE RICONSOSCE CHE IL RIFIUTO DI MIGRARE A UNA VERSIONE SUPPORTATA, OLTRE A NON BENEFICIARE DEI SERVIZI DI MANUTENZIONE, COMPRESA LA FORNITURA DI PATCH, ESPONE A PROBLEMI DI SICUREZZA. MEGA NON SARÀ MAI RITENUTA RESPONSABILE PER EVENTUALI CONSEGUENZE CHE SI SAREBBERO POTUTE EVITARE SE IL CLIENTE AVESSE MIGRATO A UNA VERSIONE SUPPORTATA O AVESSE ACCETTATO L'INSTALLAZIONE DI UN PACCHETTO CORRETTIVO O DI UN HOTFIX.

1. DEFINIZIONI

TERMINE	DEFINIZIONE
Sviluppo specifico / Customizzazione	Qualsiasi sviluppo specifico o parametrizzazione del prodotto HOPEX che modifica il suo funzionamento in base ai requisiti funzionali specifici del Cliente. Le modifiche possono riguardare la struttura dei dati, le schermate, i flussi di lavoro, le regole di accesso ai dati, le interfacce che richiedono lo sviluppo, le esportazioni specifiche come un sito web intranet o una reportistica complessa che richiede la programmazione. La gestione degli utenti e le configurazioni effettuate dagli utenti finali (come le preferenze di visualizzazione, le query, le funzioni di reporting standard) non sono considerate personalizzazioni, ma solo configurazioni di base del prodotto standard.
Errore	Comportamento del Servizio non conforme alla Documentazione. Ogni errore deve essere riproducibile, presentare sintomi chiaramente identificabili e generare conseguenze funzionali sul servizio standard.
Soluzione	Modalità operativa alternativa per mitigare un Errore.
Incidente	Un evento che non fa parte dell'operatività standard dei servizi e che interrompono il Servizio in produzione o ne diminuiscono la qualità.
Caso	Istanza utilizzata dal supporto tecnico di MEGA per seguire un incidente notificato dal Cliente.
Periodo di indisponibilità o interruzione del servizio	L'intervallo di tempo all'interno del periodo di applicabilità dell'Contratto sul livello di servizio durante il quale il servizio non è disponibile per gli utenti.
Release o nuova versione	Nuova versione del software, con nuove funzionalità.
Fix	Indica una modifica del servizio, sviluppata da MEGA per correggere un errore. I Fix sono sempre raggruppati in un Pack Correttivo o, in casi eccezionali, in un Hotfix.
Pack Correttivo (CP) o versione minore	Significa aggiornamenti per rendere HOPEX più affidabile. CP fornisce un insieme coerente di correzioni, nonché miglioramenti della sicurezza e delle prestazioni applicabili a una release di supporto a lungo termine.
Hotfix	Fix impostato e fornito da MEGA al di fuori del contesto di una Release o di un CP. Gli hotfix rispondono solitamente a errori critici e possono essere installati solo sull'ultimo CP di una release.

2. ACCESSO AL SERVIZIO

L'accesso al Servizio è limitato agli indirizzi IP predefiniti forniti dal Cliente. Gli indirizzi IP devono essere pubblici (instradabili), statici e elencati.
Gli utenti in roaming si collegheranno prima al sito di relay di un Cliente, che fornirà loro un indirizzo IP a cui MEGA consente l'accesso, e poi si collegheranno al Servizio.
Il Cliente segnala inoltre immediatamente a MEGA qualsiasi incidente relativo all'accesso al Servizio. Il Cliente si impegna a non interferire o disturbare il Servizio, compresi i server di MEGA o del fornitore di hosting di MEGA, e a rispettare le raccomandazioni, le procedure e le regole comunicate di volta in volta da MEGA per l'uso appropriato del Servizio.

3. CREDENZIALI UTENTE

MEGA fornirà le credenziali utente all'amministratore del Cliente, responsabile dell'impostazione delle credenziali per gli utenti.

Il Cliente deve adottare tutte le misure necessarie per garantire la riservatezza delle credenziali dell'utente. MEGA non è responsabile di eventuali danni derivanti dall'utilizzo del servizio da parte di terzi non autorizzati. In caso di perdita o divulgazione da parte di un utente delle proprie informazioni di accesso a terzi non autorizzati, il Cliente ne informa MEGA per iscritto senza alcun indugio. Per motivi di sicurezza, MEGA può in qualsiasi momento richiedere al Cliente di cambiare una password o di cancellare un ID utente senza previo consenso.

4. DISPONIBILITÀ DEL SERVIZIO

MEGA compirà ogni ragionevole sforzo per rendere disponibili i servizi come indicato nel presente documento, ad eccezione di:

- Durante i periodi di manutenzione. La manutenzione programmata è soggetta a un ragionevole preavviso, mentre la manutenzione non programmata sarà soggetta a un preavviso di un giorno lavorativo (tranne in caso di incidenti di sicurezza);
- A seguito di circostanze al di fuori del controllo di MEGA, come ad esempio l'interruzione di Internet e qualsiasi altro evento di Forza Maggiore;
- In caso di problemi di sicurezza, come l'uso anomalo, fraudolento o abusivo dei Servizi, qualsiasi intrusione, accesso fraudolento ai Servizi da parte di terzi, o estrazione illegale di tutti o parte dei dati, ecc, il Cliente è tenuto a pagare i costi sostenuti dai Servizi.

MEGA farà del suo meglio per ridurre al minimo le conseguenze e ripristinare il Servizio dopo la cessazione delle cause di cui sopra.

DISPONIBILITÀ DEL SERVIZIO	SVILUPPO	PRODUZIONE
Durata massima dell'interruzione non programmata	1 giorno lavorativo	3 ore lavorative
Interruzione massima mensile non programmata	1 giorno lavorativo	4 ore lavorative

Tutti i periodi di indisponibilità sono computati nel calcolo dell'interruzione di cui sopra, ad eccezione di:

- Periodi di indisponibilità programmati, come ad esempio periodi autorizzati in anticipo dal Cliente nell'ambito delle operazioni di gestione del cambiamento
- Periodi di indisponibilità non programmati derivanti dall'esclusione di responsabilità di cui alla presente sezione.

L'interruzione viene calcolata dal momento in cui il Cliente contatta MEGA: dichiarazione di *impossibilità di accesso* dalla sezione Supporto della nostra Community (https://community.mega.com).

In caso di mancato rispetto degli impegni di disponibilità, il Cliente può richiedere un credito di servizio. Un credito di servizio rappresenta il numero di giorni aggiuntivi di Servizio (oltre al periodo di abbonamento in corso) concessi al Cliente per l'interruzione. Qualsiasi credito di servizio deve essere richiesto per iscritto. Tale richiesta deve essere effettuata entro i 3 mesi successivi alla data dell'evento generatore. Il credito di servizio è l'unico ed esclusivo rimedio del Cliente in caso di indisponibilità del servizio.

Il periodo di disponibilità del Servizio va dalle 9.00 alle 18.00, dal lunedì al venerdì, esclusi i giorni festivi.

5. LIMITAZIONE DELLA RESPONSABILITÀ DI MEGA

La responsabilità di MEGA sarà limitata o esclusa nei seguenti casi:

- Mancata osservanza da parte del Cliente delle istruzioni per l'uso del servizio, come indicato nella Documentazione e nella Guida dell'utente;
- Degrado delle prestazioni dovuto alla configurazione di rete del Client e ai dispositivi di sicurezza;
- Incidente dovuto a un prodotto software installato sul sistema informatico del Cliente.
- Indisponibilità del punto di contatto del Cliente durante un'interruzione.
- Rifiuto del Cliente di fornire tempestivamente le informazioni (o l'autorizzazione ad accedervi) che potrebbero consentire a MEGA di risolvere un Incidente o un Errore.

6. GRAVITÀ DELL'INCIDENTE E TEMPI DI RISPOSTA

GRAVIDANZA	SITUAZIONE	TEMPI DI RISPOSTA E ASPETTATIVE
Nessun accesso	Problemi di sicurezza Piattaforma disattivata/impossibilità di accesso per tutti gli utenti	1 ora lavorativa
Critico	Significativo deterioramento di una o più funzionalità Forte impatto sull'attività.	Cliente contattato entro 4 ore lavorative. Sforzo continuo tutti i giorni, durante l'orario lavorativo. Rapido accesso al Servizio di Assistenza Tecnica e ai gruppi responsabili della gestione del prodotto. Tempestiva assegnazione delle risorse adeguate. Definizione di un piano d'azione. A seconda della complessità dell'Errore, verrà fornita una soluzione temporanea o sviluppato un Workaround per ridurre i tempi di interruzione dell'attività.
Moderato	Degrado della funzionalità. Il lavoro può continuare in modo soddisfacente, ma compromesso. Impatto moderato sull'attività.	Cliente contattato entro 1 giorno lavorativo. Assegnazione delle risorse adeguate durante l'orario lavorativo. Può essere fornito un piano d'azione.
Minore	Degrado minore di una o più funzionalità. Nessun impatto sull'attività.	Cliente contattato entro 2 giorni lavorativi. "Best effort" durante l'orario lavorativo.

Il tempo di risposta è calcolato a partire dal giorno successivo alla notifica dell'errore da parte del Cliente a MEGA tramite il Centro di assistenza accessibile dalla Community online.
Il supporto tecnico di MEGA può abbassare il livello di gravità se il Cliente non è in grado di fornire le risorse o le risposte necessarie per consentire a MEGA di continuare i suoi sforzi per risolvere l'incidente.
I servizi di supporto standard non comprendono l'assistenza in loco. In casi specifici, e previa approvazione da parte del Cliente dei termini e delle condizioni dell'intervento di MEGA, quest'ultima può intervenire sul sito del Cliente a sua discrezione. Il Cliente fornisce a MEGA l'accesso alle risorse del Cliente e a personale sufficientemente qualificato per fornire tutte le informazioni necessarie. Il Cliente mette a disposizione i dati necessari per il supporto e garantisce di possedere tutti i diritti di proprietà intellettuale sugli articoli di terzi messi a disposizione di MEGA.

7. POLITICA DEL CICLO DI VITA

DEFINIZIONE	DESCRIZIONE
Release (Sostegno a lungo termine)	Nuova versione di Hopex mantenuta nei seguenti periodi: in Full Support per un periodo di 27 mesi, poi in Limited Support per un periodo di 9 mesi, e regolarmente migliorata da CP.
Full Support	Periodo durante il quale il Cliente riceve servizi di manutenzione e assistenza che includono il miglioramento delle funzionalità esistenti, l'aggiunta di nuove funzionalità e prodotti e le patch.
Limited Support	Periodo successivo al periodo di Full Support, durante il quale gli Incidenti critici del Cliente possono essere risolti solo tramite Hotfix.

8. PIANO DI BACKUP E DISASTER RECOVERY (DRP)

8.1. Backup.
Nell'ambito dei servizi di hosting (non facoltativi), MEGA si impegna a eseguire il numero di backup dei dati indicato in questa sezione.
In caso di disastro che interessi i suoi server di hosting, MEGA si impegna a ripristinare i Servizi entro i tempi definiti nel presente documento.
Per impostazione predefinita, il ripristino viene eseguito a partire dall'ultimo backup. Tutti gli altri backup conservati secondo i termini di questo documento sono considerati archivi e possono essere ripristinati.

BACKUP	GIORNALE	SETTIMANALE	MENSILE
Periodo di conservazione dei backup da un backup periodico	7 giorni	4 settimane	6 mesi
Tempo di ripristino	Ultimo backup: 4 ore lavorative Archivio: 6 ore lavorative		

8.2. Piano di ripristino di emergenza.
Il Cliente beneficia di un piano di Disaster Recovery nel caso in cui un errore interessi il database o un problema interessi i server che ospitano la Piattaforma, le soluzioni e/o i dati del Cliente.
MEGA si impegna a:

- Eseguire i backup dei dati del Cliente secondo una frequenza predefinita. Quest'ultima si riferisce all'ultimo backup, che viene utilizzato per eseguire il piano di ripristino (RPO),
- Ripristinare i dati del Cliente dall'ultimo backup entro i tempi definiti di seguito. Questo tempo di ripristino (RTO) richiesto da MEGA per ripristinare i servizi.

Il Cliente può sottoscrivere, a sua esclusiva discrezione, l'opzione "DRP avanzato" per beneficiare di una maggiore frequenza di backup e/o di tempi di ripristino più brevi.

	Obiettivo di tempo di recupero (RTO)	Obiettivo del piano di recupero (RPO)
Offerta standard	1 settimana	25 ore
Con l'opzione DRP avanzato	24 ore	25 ore

9. TEST DI PENETRAZIONE

MEGA condurrà annualmente dei test di penetrazione di terzi sul suo Servizio SaaS. Tali test saranno eseguiti sulle release di Full Support (ultimo CP), disponibili sul mercato il giorno del test di penetrazione. Qualsiasi altra richiesta del Cliente può essere soggetta a costi aggiuntivi. Su richiesta, MEGA fornirà al Cliente una lettera di opinione e un rapporto riassuntivo dei risultati di tali test di penetrazione.

10. RICHIESTE DI SERVIZIO

Una richiesta di servizio è una richiesta formalizzata di intervento sulla/e piattaforma/e SaaS del Cliente.
Le uniche persone autorizzate ad eseguire i Servizi di Richiesta sono quelle designate dal Cliente come "Contatti MEGA".

10.1. Servizi inclusi nello standard.

Categoria di servizio	Nome del dipartimento	Descrizione del servizio	Frequenza/Quantità max	Tempo di risposta
Gestione delle versioni	Aggiornamento dell'applicazione	Distribuire un aggiornamento HOPEX su una delle piattaforme SaaS (DEV; PRE-PROD; PROD); HotFix, Patch, Release.	4 all'anno	HotFix, Pack Correttivo 2 giorni lavorativi (PPROD FIRST) Versione Deve essere pianificato in anticipo
Gestione degli utenti	Accesso utente	Fornire un file di log (formato TXT) che riporti tutte le connessioni degli utenti, comprese le licenze, i nomi utente, i profili e la disponibilità della piattaforma.	1 al mese	1 giorno lavorativo
	Riassegnare un utente/profilo a una licenza token	Con le licenze nominative, riassegnare un utente a un modello di licenza basato su token. Un utente può essere: utente principale, collaboratore o lettore. Questo servizio non si applica alle licenze fluttuanti.	10 riassegnazioni (tutti gli utenti) all'anno	
Gestione degli accessi	Modificare il nome di dominio del servizio	Cambiare l'URL di accesso a HOPEX Cloud dal nome di dominio "aaa.hopexcloud.com" a "bbb.hopexcloud.com".	2 modifiche all'anno	2 giorni lavorativi
	Dichiarare intervalli di indirizzi IP aggiuntivi nell'elenco degli accessi consentiti	Aggiungere fino a 5 intervalli di indirizzi IP aggiuntivi all'elenco degli indirizzi IP che possono accedere al pacchetto software HOPEX.	3 richieste all'anno	1 giorno lavorativo
Gestione dell'integrazione	Pianificazione delle attività	Programmare attività ricorrenti con upload o download (se applicabile) da e verso l'ambiente del Cliente utilizzando un protocollo di trasferimento sicuro dei file (SFTP). Le attività programmate sono principalmente l'importazione/esportazione e la generazione di siti web statici. La progettazione, la realizzazione e la convalida degli elementi da pianificare restano sotto la responsabilità del Cliente.	6 richieste all'anno	2 giorni lavorativi (PPROD FIRST)
	Distribuzione dei servizi web	Distribuire un servizio Web in produzione. La progettazione, la realizzazione e la convalida di un Servizio Web restano responsabilità del Cliente.		3 giorni lavorativi (PPROD FIRST)
Negozio HOPEX	Distribuzione di un modulo	Elenco dei moduli in evoluzione: https://store.mega.com/modules	10 richieste all'anno	2 giorni lavorativi (PPROD FIRST)

Le richieste di servizi sono soggette al presente Contratto sul livello dei servizi.
Qualsiasi modifica della frequenza e/o della quantità massima di richieste di servizio è soggetta a costi aggiuntivi.
Inoltre, MEGA può essere impegnata in richieste di servizio solo se:

- La richiesta di assistenza è aperta dal sito web di MEGA Community (non saranno elaborate richieste di assistenza inviate per e-mail);
- Il contatto MEGA riconosce di aver fornito a MEGA tutte le informazioni necessarie per attuare una richiesta di servizio. Il tempo necessario per raccogliere le informazioni sarà dedotto.

Per le richieste non elencate nel catalogo delle richieste di servizio:

- Tempo di risposta stimato entro 2 giorni lavorativi
- Studio e trattamento in base alla richiesta

10.2. Livelli di servizio del "Pacchetto piattaforma SaaS".

Livelli di servizio	Tipo di piattaforma	Numero di avviamenti di produzione
Avviamento	Pre-produzione e produzione	1 all'anno
Standard	Sviluppo, pre-produzione e produzione	4 all'anno
Avanzato	Sviluppo, pre-produzione e produzione	12 all'anno

11. OPZIONI

11.1. Manutenzione Premium

Oggetto	Descrizione
Supporto Premium	
Follow-up mensile proattivo	Riunioni mensili per riferire sulla risoluzione dei casi con un unico punto di contatto
Monitoraggio degli indicatori di salute	Revisione mensile degli indicatori di salute, compreso il numero di casi e gli SLA.
Manutenzione delle personalizzazioni	
Correzione delle configurazioni/personalizzazioni, compresa la documentazione	Supportare e correggere le modifiche apportate esclusivamente da MEGA. Ciò include anche le modifiche necessarie per aggiornare il servizio.
Gestione degli aggiornamenti	
Aggiornamento-Convalida funzionale	Eseguire la convalida funzionale della configurazione dopo l'aggiornamento all'ultima versione di HOPEX.
Gestire l'impatto dei Release minori sugli utenti	Valutare l'impatto di qualsiasi modifica dell'aggiornamento dell'utente sulla base di utenti. Ciò comporterà attività quali la comunicazione con gli utenti e l'identificazione degli utenti che necessitano di una formazione supplementare.

11.2. Pacchetto adozione

Oggetto	Descrizione
Valutazione e monitoraggio della maturità	
Workshop di valutazione della maturità	Workshop funzionali annuali finalizzati a migliorare l'adozione, l'utilizzo di HOPEX e la dimostrazione del valore, basati sulla metodologia di valutazione della maturità MEGA, tra cui un esperto di prevendita e un CSM
Seguito delle raccomandazioni	Monitoraggio dell'adozione di HOPEX attraverso indicatori chiave e attuazione delle raccomandazioni degli esperti.
e-Learning	
Sessioni di eLearning	Sessioni di eLearning per aumentare l'adozione all'interno del team

11.3. Amministrazione Hopex

Oggetto	Descrizione
Gestione degli accessi	
Gestione della modalità di autenticazione HOPEX	Gestire la modalità di autenticazione degli utenti HOPEX.
Gestire i ruoli aziendali	Assegnare i ruoli aziendali. Un ruolo aziendale definisce la funzione di una persona o di un gruppo di persone nell'impresa. Un ruolo aziendale è definito a livello di repository.
Gestire i gruppi di persone	Impostare, rimuovere e configurare gruppi di persone in un gruppo che condivide la stessa connessione. Un gruppo di persone è un elenco di persone appartenenti allo stesso gruppo.
Gestione degli accessi e dei gruppi di utenti	Impostare, rimuovere, configurare utenti, gruppi di utenti, profili di utenti, livelli di accesso e di autorizzazione.
Definire le regole di accesso ai dati	Impostare, rimuovere e configurare le strutture di autorizzazione degli utenti.
Reimpostare la password di un utente	Impostare/ripristinare la password dell'utente (questo include solo la reimpostazione della password per gli utenti MEGA).
Gestione dei contenuti - Lavoro degli utenti	
Gestire gli oggetti duplicati	Identificare gli oggetti duplicati (collaborando con i proprietari dei contenuti), convalidare i duplicati ed eseguire azioni per rimuoverli, ad esempio unire o eliminare.
Gestire gli oggetti isolati	Identificare gli oggetti isolati per consentire l'assegnazione della proprietà, l'identificazione per l'eliminazione, la segnalazione di oggetti non presenti nei diagrammi (dove ci si aspetta che siano descritti dai diagrammi), la segnalazione di oggetti non inclusi nelle associazioni.
Gestire gli oggetti da eliminare	Eliminare gli oggetti, dove l'utente modellatore non ha i privilegi per eliminare gli oggetti creati al di fuori delle sue transazioni correnti. Gli oggetti possono essere contrassegnati per l'eliminazione dagli utenti.
Gestire la fusione di oggetti	Unire gli oggetti (cioè i duplicati) all'interno di un repository.
Gestire l'accesso ai dati	Impostare e mantenere i livelli di autorizzazione degli oggetti che consentono/disconsentono la modifica degli oggetti da parte di un determinato utente/profilo utente.
Gestire la protezione degli oggetti	Attivare o disattivare la protezione di oggetti specifici all'interno di un repository.
Gestione dei contenuti - Amministrazione	
Confronto e allineamento di repository/sottoinsieme di contenuti	Confronto e promozione di oggetti/ambiti di oggetti da repository separati. Il repository di destinazione può essere allineato al repository di base.
Backup logico del gruppo di contenuti	Creare una baseline logica per uno specifico gruppo di contenuti (ambito, ad esempio biblioteca, progetto, ecc.), consentendo la creazione di baseline indipendenti di segmenti del contenuto del repository.
Gestire le biblioteche	Impostare e mantenere le librerie e garantire una chiara struttura dei contenuti all'interno del repository. Le librerie possono essere utilizzate per separare logicamente i contenuti del repository.
Creare query e report	Scrivere query registrate e disponibili per il riutilizzo da parte di tutti gli utenti dell'ambiente. Configurare i report in base alle funzionalità di Report Studio.
Gestione dei flussi di lavoro	Gestire la transizione dei flussi di lavoro per supportare l'approvazione, l'autorizzazione e lo spostamento degli oggetti. Monitorare le azioni e le riassegnazioni dei flussi di lavoro.
Importazione dei dati	Gestire l'importazione regolare di dati utilizzando i modelli XLS esistenti.
Gestione degli incidenti	
Gestire il supporto interno	Gestire il primo livello di supporto sui casi d'uso funzionali del Cliente, in un contesto di piattaforma personalizzata.
Gestire il follow-up dei casi	Creare, dare priorità e seguire i casi con il supporto tecnico MEGA. Fornite loro tutti gli elementi necessari per diagnosticare il problema sollevato.
Supporto funzionale	
Guida	Fornire le migliori pratiche e una guida standard sull'utilizzo di HOPEX.
Modello di trascrizione	Gestire la trascrizione manuale di modelli esistenti (MS Word, PPT, Visio, ...) o di dati strutturati (formato XLS) in HOPEX Non applicabile per il carico di massa.
Gestire la manutenzione dei diagrammi	Aggiornare i diagrammi esistenti sulla base di una richiesta di modifica formalizzata. Gestire l'impatto sui disegni delle modifiche apportate ai concetti fondamentali dei dati.
Guida	Fornire le migliori pratiche e una guida standard sull'utilizzo di HOPEX.
Integrazione e formazione degli utenti	Integrazione e formazione di nuovi utenti sulla base della documentazione e dei materiali di formazione esistenti.
Modellazione EA	Dal colloquio con lo SME alla convalida del vostro asset EA sui diagrammi di HOPEX
Formazione e onboarding degli utenti	Intraprendere e fornire formazione ai nuovi utenti finali sulla base del corso di formazione e della documentazione esistente per i Clienti.

12. CONTATTI E GOVERNANCE

Al momento della stipula del Contratto, il Cliente nomina un massimo di 3 referenti designati, formati sui servizi e ai quali MEGA fornirà servizi di supporto. I contatti designati devono essere in grado di svolgere almeno le seguenti funzioni:

- Gestire gli utenti e la loro assegnazione ai diversi profili della/e soluzione/i MEGA che costituiscono il Servizio;
- In caso di incidente:
  - Dichiarare un caso sul portale MEGA raccogliendo e fornendo tutte le informazioni necessarie relative alle circostanze in cui si è verificato l'incidente;
  - Segnalare immediatamente qualsiasi problema di sicurezza con i mezzi più appropriati;
- Per una maggiore efficienza operativa, partecipate alle riunioni di gestione e di arbitrato organizzate da MEGA .

13. REVERSIBILITÀ

I dati del Cliente vengono conservati per un periodo di 3 mesi dalla data di cessazione o scadenza dei Servizi. Durante questo periodo, il Cliente non avrà più accesso ai servizi. L'unico scopo di questo periodo è quello di consentire al Cliente di impostare un periodo di reversibilità in caso di necessità. Al termine di questo periodo di 3 mesi, i dati vengono cancellati definitivamente.
Il Cliente può richiedere:

- Solo la conservazione dei dati per un periodo che va oltre il suddetto periodo di 3 mesi.
- Oppure per eseguire i servizi di reversibilità, come definito di seguito.

Qualsiasi estensione del periodo di conservazione e/o dei servizi di reversibilità deve pervenire a MEGA entro e non oltre 2 mesi dalla data effettiva di cessazione o scadenza dei servizi.
L'estensione dei servizi di ritenzione e/o reversibilità sarà fatturata secondo il listino prezzi MEGA in vigore alla data in cui MEGA invia il proprio preventivo al Cliente.
Lo scopo dei servizi di reversibilità è il recupero dei dati del Cliente all'interno del database HOPEX.
MEGA offre due tipi di servizi di reversibilità: quello di base e quello complesso.

- Reversibilità di base: MEGA fornisce al Cliente backup dei dati di produzione per il ripristino nella stessa versione di MS-SQL-Server DBMS per l'utilizzo con la stessa soluzione HOPEX nella stessa versione.
  I dati saranno (i) messi a disposizione del Cliente su un server FTP MEGA per il download, oppure (ii) inviati (SFTP) sul server del Cliente o del suo fornitore. È responsabilità esclusiva del Cliente concedere il diritto di accesso al repository. MEGA raccomanda una formazione adeguata per l'amministrazione della soluzione.
- Reversibilità complessa: questi servizi sono applicabili quando la reversibilità di base non soddisfa le esigenze del Cliente. Possono essere appropriati quando i dati devono essere caricati su una soluzione software alternativa.
  Lo scopo di una reversibilità complessa è quello di fornire.
  - Un'esportazione XML codificata UTF-8 del dump del database;
  - Una documentazione su come elaborare il formato XML;
  - Riconosciuto trasferimento di competenze sia funzionali che tecniche al team incaricato dell'acquisizione, per la comprensione del modello di dati della soluzione, nonché delle specificità della soluzione implementata e dell'esportazione fornita.

  È responsabilità del Cliente approvare che i dati acquisiti siano accurati e che si integrino completamente nella nuova soluzione.
  La reversibilità complessa è soggetta a un prezzo fisso.
- Altro: Se il Cliente desidera ordinare servizi supplementari, dovrà inviare a MEGA la sua richiesta scritta e dettagliata. MEGA condurrà uno studio di fattibilità e/o invierà un preventivo.

14. CALCOLO DEL TEMPO

Quando un periodo è indicato in ore, è calcolato 7 giorni alla settimana e 24 ore al giorno.
Quando un periodo è espresso in ore lavorative, viene calcolato per ogni giorno lavorativo, dalle 9 alle 18, ora di Milano.
Non si tiene conto del momento in cui si verifica l'evento o la notifica che fa decorrere il termine.
Quando un periodo è espresso in giorni lavorativi, viene calcolato considerando solo i giorni della settimana, dal lunedì al venerdì, esclusi i giorni festivi francesi.
Non si tiene conto del giorno dell'evento o della notifica che fa decorrere il termine.
Quando un periodo è indicato in mesi, viene calcolato considerando la data.
Non si tiene conto del giorno dell'evento o della notifica che fa decorrere il termine.
In assenza di una data simile, il periodo è esteso al primo giorno lavorativo successivo, fino alla mezzanotte.
Quando un periodo è indicato in ore, scade alla fine dell'ora.
Quando un periodo è indicato in giorni o mesi, scade alla fine dell'ultimo giorno alle ore 12.00.
Un periodo indicato in giorni che scadrebbe di sabato, domenica o giorno festivo è esteso al primo giorno lavorativo successivo, fino a mezzanotte.
Per le notifiche a mezzo raccomandata con ricevuta di ritorno fa fede la data di prima presentazione della lettera con ricevuta di ritorno, il timbro postale.

15. L'IMPEGNO DI MEGA PER LA SICUREZZA

15.1. SICUREZZA GLOBALE

Oggetto	Descrizione
TLS	Necessario sulle piattaforme HOPEX Cloud per garantire la sicurezza delle transazioni tra il front-end web e il terminale del Cliente. Il certificato basato sulla crittografia TLS 1.2 AES256-SHA256 è interamente a carico del team MCS (MEGA Cloud Services).
Whitelist di IP pubblici	Gli indirizzi IP pubblici dei Clienti devono essere forniti a MEGA in anticipo per poter accedere ai servizi.
Piattaforma monoutente	Tutte le piattaforme dei Clienti sono completamente Singletenant. Gli ambienti di ciascun Cliente sono installati su un server dedicato, in una VLAN dedicata e completamente segregata l'una dall'altra.
Vengono distribuite piattaforme virtuali totalmente separate l'una dall'altra.	Le piattaforme HOPEX Cloud sono tipicamente distribuite in modalità standard con un server virtuale per Client per l'ambiente di produzione. Quando si sottoscrive il "Pacchetto piattaforma SaaS" di livello Standard o Premium, vengono distribuite tre istanze isolate, come : • SVILUPPO: Server dedicato che consente al Cliente di personalizzare le soluzioni HOPEX e di testare gli aggiornamenti; • PRE-PRODUZIONE: server dedicato sincronizzato su richiesta con la piattaforma di produzione, che consente al Cliente di convalidare e testare gli aggiornamenti prima della loro implementazione in produzione (ad esempio, impostazioni tecniche e funzionali, patch correttive CP); • PRODUZIONE: I contenuti distribuiti in produzione sono stati precedentemente testati e approvati nella piattaforma di pre-produzione.
Crittografia dei dati	Crittografia standard dello storage da Microsoft Azure SSE con crittografia AES-256 bit

15.2. Organizzazione e gestione della sicurezza delle informazioni .

Oggetto	Descrizione
Organizzazione della sicurezza delle informazioni e gestione del rischio informatico	MEGA ha implementato una politica di sicurezza delle informazioni che comprende tutto il personale. I ruoli principali del personale MEGA sono: • L'alta direzione approva, incoraggia e sostiene le misure di miglioramento della sicurezza dei sistemi informativi; • Il Responsabile della sicurezza (CISO) è responsabile della sicurezza, della disponibilità e dell'integrità del sistema informativo; • Il Responsabile IT (CIO) è responsabile del funzionamento e della direzione strategica del sistema informativo; • I comitati per la sicurezza sono formati per affrontare tutti i temi della sicurezza, i rischi, gli incidenti e la conformità.
Gestione del rischio aziendale	MEGA ha progettato e implementato un programma di Enterprise Risks Management per analizzare e mitigare i rischi in modo proattivo per tutte le attività MEGA.
Standard di garanzia indipendente valutazione	L'offerta HOPEX Cloud Enterprise è soggetta a un audit annuale SOC2 da parte di una terza parte indipendente.

15.3. Politiche di sicurezza delle informazioni.

Oggetto	Descrizione
Politica di sicurezza dei sistemi informativi	Questa è la politica di sicurezza del sistema informativo che è stata implementata e convalidata dalla direzione di MEGA e comunicata alle parti interessate. Questo documento viene rivisto annualmente.
Procedure e politiche	Le politiche di sicurezza delle informazioni (classificazione dei dati, crittografia, password, ecc.), gli standard, le procedure e le linee guida sono pubblicati sull'intranet, rivisti e comunicati su base annuale.
Certificazione SOC 2 di tipo 2	MEGA certifica che, alla data della firma del presente Contratto, i servizi sono conformi ai criteri per la certificazione SOC2 di tipo 2. Per chiarezza, MEGA non si impegna a mantenere questa conformità per tutta la durata dell'accordo.

15.4. Gestione patrimoniale.

Oggetto	Descrizione
Responsabilità per le attività	MEGA identifica i beni dell'organizzazione (inventario, proprietà, uso accettabile e restituzione) e definisce le responsabilità di protezione appropriate.
Classificazione delle informazioni	MEGA ha implementato una serie di procedure appropriate per l'etichettatura delle informazioni in conformità con lo schema di classificazione delle informazioni.
Gestione dei media	MEGA ha apportato un miglioramento alla politica di sicurezza per tutti i team IT del CSM. Sulle piattaforme non sono ammessi dispositivi di archiviazione rimovibili.

15.5. Sicurezza delle risorse umane .

Oggetto	Descrizione
Prima dell'assunzione	MEGA esegue i necessari controlli e verifiche su tutti i candidati all'assunzione in conformità alle leggi, ai regolamenti e all'etica applicabili e commisurati alle esigenze dell'azienda, alla classificazione delle informazioni a cui si accede e ai rischi percepiti.
Durante l'impiego	I dipendenti e gli utenti esterni di MEGA seguono un programma di sensibilizzazione alla sicurezza. Ricevono istruzioni, formazione e aggiornamenti regolari sulle politiche e sulle procedure di sicurezza, come richiesto dalla loro funzione lavorativa.
Cessazione e modifica del rapporto di lavoro	MEGA dispone di un processo di gestione delle risorse umane per gestire qualsiasi cessazione o cambiamento di impiego.

15.6. Sicurezza fisica e ambientale .

Oggetto	Descrizione
Aree sicure	MEGA ha definito i perimetri di sicurezza e la politica fisica per proteggere le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni.
Apparecchiature	MEGA ha implementato misure fisiche per proteggere le proprie apparecchiature da accessi non autorizzati e interruzioni di corrente. Tutti i supporti di memorizzazione vengono analizzati prima del riutilizzo o della dismissione per garantire che i dati sensibili e il software con licenza siano stati rimossi o sovrascritti in modo sicuro. MEGA ha adottato una politica di sicurezza informatica per le postazioni di lavoro: protezione dei documenti cartacei e dei supporti di memorizzazione rimovibili, blocco dello schermo. L'offerta HOPEX Cloud Enterprise è costruita su un'infrastruttura Microsoft Azure, che soddisfa un'ampia gamma di standard internazionali di conformità specifici del settore, come ISO 27001, HIPAA, FedRAMP, SOC 1 e SOC 2, nonché standard specifici del paese, come Australia IRAP, Regno Unito G-Cloud e Singapore MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

15.7. Controllo degli accessi.

Oggetto	Descrizione
Controllo dell'accesso	La politica di accesso globale di MEGA si basa sul principio del minor privilegio. Le revisioni periodiche sono condotte dal CISO (Chief Information Security Officer).
Gestione dell'accesso degli utenti	L'amministrazione delle piattaforme HOPEX Cloud è accessibile solo dal team MCS (MEGA Cloud Services) attraverso un server bastion che registra (log e video) tutte le azioni eseguite sulle piattaforme del Cliente. L'indirizzo IP pubblico del Cliente deve essere fornito al team MCS per la connessione al servizio.
Responsabilità degli utenti	A ogni Cliente viene concesso un accesso come amministratore funzionale di HOPEX, che consente al Cliente di gestire tutti gli utenti all'interno del repository HOPEX. Questo amministratore è anche il contatto tra l'azienda del Cliente e MEGA.
Controllo dell'accesso a sistemi e applicazioni	L'autenticazione al servizio HOPEX Cloud può essere effettuata tramite un SSO utilizzando i protocolli SAML 2.0 e OpenID Connect (OIDC).

15.8. Sicurezza operativa - Sicurezza del sistema.

Oggetto	Descrizione
Procedure operative e responsabilità	MCS ha documentato tutte le procedure operative seguendo le Best Practice ITIL (CAB) per mantenere le piattaforme del Cliente in condizioni ottimali.
Protezione dal malware	MEGA ha implementato controlli di rilevamento, prevenzione e ripristino per proteggere dalle minacce informatiche. Questa misura tecnica è combinata con un'adeguata consapevolezza da parte degli amministratori.
Backup	Sulle piattaforme cloud di HOPEX vengono eseguiti regolarmente backup automatici criptati che consentono di recuperare i dati di produzione del Cliente in caso di incidente.
Registrazione e monitoraggio	Sulle piattaforme HOPEX Cloud Enterprise, oltre allo strumento di monitoraggio HOPEX Server Supervisor integrato in tutte le piattaforme dei Clienti che consente all'amministratore HOPEX di seguire ogni azione eseguita sul sistema (ad esempio, autenticazione utente riuscita/fallita, modifica del profilo utente/diritti, ecc.), tutti i log della piattaforma vengono registrati attraverso una soluzione di terze parti MCS per l'analisi. Il team MCS monitora costantemente la disponibilità delle piattaforme di ciascun Cliente attraverso un sistema di monitoraggio dedicato che consente di avvisare gli amministratori MCS in caso di anomalie.
Controllo del software operativo	MCS gestisce il sistema informativo secondo le raccomandazioni ITIL (gestione del cambiamento, ecc.).
Gestione della vulnerabilità tecnica	MEGA R&D utilizza la soluzione Coverity per eseguire la scansione delle vulnerabilità sul codice sorgente di HOPEX (controllo quotidiano). Per ogni release principale viene eseguita una verifica da parte di terzi. MEGA ha progettato un processo di vulnerabilità per gestire in modo efficace e tempestivo le minacce e le vulnerabilità di sistemi, software e applicazioni, mitigando il rischio di potenziale sfruttamento e compromissione.
Considerazioni sull'audit dei sistemi informativi	Manutenzione programmata (OS, hardware, ecc.): La manutenzione del sistema e del software viene eseguita durante il fine settimana per un paio d'ore. Manutenzione non programmata: Le patch, le personalizzazioni o gli aggiornamenti critici di HOPEX possono essere eseguiti al di fuori dell'orario di lavoro e pianificati congiuntamente con il Cliente.

15.9. Sicurezza delle comunicazioni - Sicurezza delle reti.

Oggetto	Descrizione
Gestione della sicurezza di rete	Tutte le piattaforme Client sono dedicate (Singletenant). Ogni piattaforma Client è installata su un server dedicato isolato l'uno dall'altro all'interno di una VLAN separata. Ogni piattaforma ha il proprio firewall (MS Azure Network Security Group) per imporre e controllare il traffico di rete.
Trasferimento di informazioni	Le transazioni web devono essere crittografate con TLS per proteggere le transazioni tra i server web e i siti Client. Il certificato TLS 1.2 basato sulla crittografia AES256-SHA256 è interamente gestito dal servizio MCS (MEGA Cloud Services). Inoltre, gli indirizzi IP pubblici del Cliente devono essere forniti a MEGA per poter accedere al servizio. Questa misura tecnica è accompagnata da una sensibilizzazione alla sicurezza dei dati per gli amministratori e da un accordo di riservatezza e non divulgazione. Nel caso di un trasferimento di dati, questi devono essere trasmessi tramite un trasferimento di tipo SFTP.

15.10. Acquisizione, sviluppo e manutenzione del sistema.

Oggetto	Descrizione
Requisiti di sicurezza dei sistemi informativi	MEGA fornisce versioni principali ogni 18-24 mesi e versioni minori ogni 3 mesi, comprese tutte le patch di sicurezza e le evoluzioni.
Sicurezza nei processi di sviluppo e supporto	La progettazione di HOPEX è interamente gestita da MEGA. La R&S di MEGA ha un SSM (Software Security Manager) incaricato di: • Definire le migliori pratiche di codifica dal punto di vista della sicurezza; • Esaminare le specifiche di tutti i progetti di sviluppo dal punto di vista della sicurezza; • Gestire personalmente lo sviluppo di moduli legati alla sicurezza (autenticazione, ecc.); • Gestione di campagne di scansioni di codici e follow-up di mitigazione. MEGA non ricorre allo sviluppo in outsourcing per progettare la propria soluzione. Nel caso in cui i Clienti debbano personalizzare la propria piattaforma HOPEX (ad esempio, modifiche al metamodello), è necessario un HOPEX Cloud Workbench opzionale.
Dati del test	MEGA utilizza un database di prova con dati fittizi.

15.11. Aspetto della sicurezza delle informazioni nella gestione della continuità operativa .

Oggetto	Descrizione
Continuità della sicurezza delle informazioni	L'integrità dei dati è garantita dalla tecnologia Geo-Redundant Storage (GRS) che consente di replicare i dati di backup in un datacenter secondario con lo stesso livello di sicurezza del datacenter primario.
Ridondanza	MEGA Ha implementato tutti i servizi di fornitura di dispositivi per garantire un'elevata disponibilità.
Piano di continuità aziendale	MEGA ha progettato e implementato un piano di continuità aziendale. 9 scenari di alto livello che potrebbero mettere a rischio la continuità aziendale, insieme a risposte predefinite per una gestione ottimale dei problemi.

15.12. Gestione degli incidenti di sicurezza delle informazioni .

Oggetto	Descrizione
Gestione degli incidenti e dei miglioramenti della sicurezza delle informazioni	MEGA ha implementato un processo di gestione degli incidenti per ripristinare il normale funzionamento del servizio il più rapidamente possibile e ridurre al minimo l'impatto negativo sulle operazioni aziendali, garantendo così il mantenimento dei migliori livelli possibili di qualità e disponibilità del servizio. Questo processo comprende una procedura di escalation.

15.13. SICUREZZA AGGIUNTIVA SOC 2

Oggetto	Descrizione
Archivio di crittografia	Le piattaforme del Cliente si trovano su archivi crittografati.
CyberArk Bastion	Le sessioni degli amministratori sulle piattaforme del Cliente vengono registrate tramite bastion.