CONDIZIONI GENERALI DI SERVIZIO

1. Informazioni sulla società

IMSEO Srl

con sede legale in Roma, via Simeto 27, 00198

P.IVA: 11028431002

Sito web: www.imseo.it

Email: amministrazione@imseo.it

PEC: imseo@legalmail.it

Le presenti **Condizioni Generali di Servizio** disciplinano:

- l'utilizzo dei servizi offerti
- i rapporti contrattuali tra IMSEO Srl e i clienti.

2. Definizioni

Ai fini delle presenti condizioni si intende per:

Società

IMSEO Srl.

Cliente

persona fisica o giuridica che richiede o acquista servizi dalla Società.

Servizi

le attività professionali offerte da IMSEO Srl.

3. Oggetto dei servizi

IMSEO Srl fornisce i seguenti servizi professionali nel settore ICT e si occupa sia di sviluppo di applicazioni custom che di system integration, in ambito open source o utilizzando applicazioni commerciali:

- Sviluppo piattaforma e-learning come sistema per erogare corsi di formazione a distanza, sistema che diviene proprietà del cliente

- Sviluppo sito Web come insieme di pagine web correlate, ovvero una struttura ipertestuale di contenuti e documenti che risiede su un server web, sistema che diviene proprietà del cliente
- Sviluppo piattaforma e-commerce come insieme di pagine web correlate, ovvero una struttura ipertestuale di contenuti e documenti che risiedono su un server web, programmate per la commercializzazione con transazione di beni e servizi, sistema che diviene proprietà del cliente
- Sviluppo applicazione custom, sistema che diviene proprietà del cliente.
- Cloud Hosting / Cloud Server / Cloud VPS (Virtual Private Server) / Cloud Infrastructure come predisposizione di risorse fisico/logiche da parte di IMSEO a beneficio del CLIENTE in forma non necessariamente esclusiva
- Backup Dati come servizio di copia di sicurezza dei dati o semplice copia ridondante dei dati
- Web Promotion come servizio di promozione marketing tramite i canali della rete internet, con campagne di Direct Email Marketing (DEM) professionali, ottimizzazione e posizionamento sui motori di ricerca (SEO)

Le caratteristiche specifiche dei servizi sono indicate negli **ordini e nei contratti**.

4. Conclusione del contratto

Il rapporto contrattuale tra la Società e il Cliente si considera concluso quando:

- il Cliente accetta un preventivo o un ordine scritto
- conferma il preventivo o l'ordine via email
- effettua il pagamento richiesto

IMSEO Srl si riserva il diritto di rifiutare richieste di servizi senza obbligo di motivazione.

5. Preventivi e ordini

I preventivi e gli ordini:

- hanno validità di **30 giorni**, salvo diversa indicazione
- sono indicativi fino alla conferma
- possono essere soggetti a revisione qualora cambino le condizioni del progetto

Il preventivo o l'ordine accettato costituisce parte integrante del contratto.

6. Prezzi e condizioni economiche

Tutti i prezzi indicati:

- sono espressi in **Euro**
- si intendono **al netto dell'IVA**, salvo diversa indicazione.

Il pagamento può avvenire tramite:

- bonifico bancario
- sistemi di pagamento elettronici
- altri metodi concordati.

IMSEO Srl può richiedere:

- pagamento anticipato
- acconti
- pagamenti periodici per servizi continuativi e/o a canone.

7. Ritardi di pagamento

In caso di ritardo nei pagamenti:

- potranno essere applicati interessi di mora ai sensi del Decreto Legislativo 231/2002
- la Società potrà sospendere l'erogazione dei servizi

- potranno essere richiesti costi amministrativi per il recupero crediti.

8. Assistenza tecnica e manutenzione

IMSEO Srl provvede alla assistenza tecnica limitatamente al proprio sistema operativo ed ai servizi di base indicati nel contratto. Non rientrano negli oneri del presente accordo interventi causati o inerenti ad anomalie direttamente imputabili ad imperizia del Cliente. È esclusa ogni forma di assistenza tecnica al Cliente su problematiche di programmazione e/o di gestione non direttamente collegate a funzionalità offerte e indicate nel contratto e direttamente riconducibili ai servizi resi da IMSEO.

È previsto un supporto di assistenza tecnica al Cliente per tutto il periodo contrattuale di erogazione del servizio i cui modi di fruizione verranno specificati da IMSEO nel contratto.

9. Procedura di Disaster Recovery e recupero dei dati

La presente procedura di Disaster Recovery si applica a:

- Infrastrutture cloud (IaaS, PaaS, SaaS) di IMSEO srl
- Sistemi di storage e database di IMSEO srl
- Applicazioni mission-critical di IMSEO srl
- Servizi esposti ai clienti di IMSEO srl

Definizioni:

- SLA (Service Level Agreement): livello di servizio garantito
- RTO (Recovery Time Objective): tempo massimo di ripristino
- RPO (Recovery Point Objective): perdita dati massima accettabile
- Disaster Recovery (DR): insieme di misure per ripristino servizi

Requisiti di servizio garantiti da IMSEO srl:

- UPTIME (SLA) ≥ 99,5%
- RTO entro 8 ore

- RPO massimo 24 ore
- Monitoraggio h24, 7/7

Elementi che contraddistinguono l'architettura di continuità operativa dei servizi della IMSEO srl:

1) Ridondanza

- Infrastruttura distribuita su almeno due regioni geografiche
- Configurazione active-active o active-passive

2) Replica dati

- Replica sincrona per dati critici
- Replica asincrona per dati non critici

3) Alta disponibilità

- Load balancing globale
- Failover automatico basato su health check

Gestione dei backup di IMSEO srl:

1) Politiche di backup

- Backup continuo (near real-time)
- Backup incrementali
- Backup completi giornalieri

2) Conservazione

- Breve termine: 7 giorni
- Medio termine: 30 giorni
- Lungo termine: 12 mesi

3) Sicurezza

- Backup immutabili (WORM)
- Crittografia AES-256
- Storage segregato

Monitoraggio e rilevamento incidenti garantito da IMSEO srl:

- Monitoraggio continuo di:
  - Disponibilità servizi
  - Prestazioni
  - Integrità dati
- Alert automatici
- Logging centralizzato

Gestione degli incidenti di IMSEO srl:

1) Classificazione

- Critico: impatto totale servizio
- Alto: degrado significativo
- Medio: impatto limitato

2) Attivazione DR (Disaster Recovery)

- Manuale entro 8 ore

Procedura di Disaster Recovery di IMSEO srl:

Fase 1 - Rilevamento

- Identificazione incidente tramite monitoring
- Apertura ticket

Fase 2 - Attivazione

- Notifica Incident Manager
- Decisione attivazione DR

Fase 3 - Failover

- Attivazione sito secondario
- Switch traffico (DNS / Load Balancer)

Fase 4 - Ripristino

- Ripristino dati da replica o backup
- Validazione integrità

Fase 5 - Verifica

- Test funzionali
- Monitoraggio stabilità

Comunicazione:

- Notifica iniziale: entro 5 minuti
- Aggiornamenti: ogni 15 minuti
- Report finale: entro 24 ore

Test e manutenzione preventiva:

- Test DR: almeno trimestrali
- Simulazioni di guasto
- Verifica RTO/RPO
- Aggiornamento documentazione

Sicurezza delle informazioni:

- Crittografia dati (in transito e a riposo)
- Controllo accessi (IAM)
- Audit log
- Conformità GDPR

Miglioramento continuo:

- Analisi Root Cause (RCA)
- Azioni correttive
- Riesame periodico (almeno annuale)

10. Cancellazione sicura dei file temporanei

I file e i documenti temporanei saranno cancellati entro 30 giorni dalla loro creazione.

11. Servizi a canone

I servizi Cloud Hosting / Cloud Server / Cloud VPS (Virtual Private Server) / Cloud Infrastructure si intendono a canone periodico salvo diversa specifica nella scheda del servizio riportata nel contratto.

La durata del servizio è indicata attraverso la quantità (Q.TA') nel contratto e si intende tacitamente rinnovato allo scadere, a meno che una delle parti non provveda ad effettuare comunicazione di disdetta con un anticipo di 30 giorni sulla data di scadenza dell'accordo, a mezzo email PEC all'indirizzo imseo@legalmail.it .

12. Sospensione della prestazione

IMSEO ha facoltà di sospendere, senza preavviso, l'erogazione del servizio qualora sussista una delle seguenti fattispecie:

a. Il Cliente è in una condizione di morosità derivante dal mancato pagamento dei canoni e/o oneri di attivazione per servizi fatturati e i cui documenti fiscali siano giunti a scadenza. In questo caso la riattivazione del servizio è subordinata all'estinzione totale della morosità.
b. Il Cliente si rende parte attiva in tentativi di violazione dei sistemi informatici di IMSEO o di terzi per mezzo del servizio messo a disposizione da IMSEO
c. Il Cliente costituisce una situazione di pericolo e/o di instabilità a seguito di sue attività di programmazione e/o utilizzo tali da arrecare danno a IMSEO. Qualora la sospensione del servizio sia conseguente ai commi (a),(b) IMSEO si riserva la possibilità di estendere gli effetti della sospensione del servizio anche ad altri rapporti contrattuali distinti dal presente, regolarmente costituiti ed in essere con il Cliente.

La 'sospensione' o 'cessazione' del servizio non comporterà la distruzione immediata del materiale eventualmente presente nei servizi di cui all'art.3, materiale per il quale decorso il termine di giorni 30 dalla data di sospensione e/o cessazione del servizio si intende autorizzata la rimozione dai server di proprietà di IMSEO e la relativa distruzione. Alcuna richiesta di risarcimento danni potrà mai essere avanzata dal Cliente nei confronti di IMSEO a seguito di quanto specificato.

13. Obblighi del cliente

Il Cliente si impegna a:

- fornire informazioni corrette e complete
- fornire accessi tecnici necessari (hosting, CMS, strumenti marketing)
- collaborare durante l'esecuzione dei servizi
- rispettare le tempistiche concordate
- non utilizzare i servizi per attività illegali

Il Cliente è responsabile della **legalità dei dati** forniti a IMSEO Srl.

14. Collaborazione operativa

Per la corretta esecuzione dei servizi il Cliente deve:

- fornire materiali richiesti
- rispondere alle comunicazioni entro tempi ragionevoli
- approvare contenuti o modifiche nei tempi concordati

Eventuali ritardi imputabili al Cliente possono comportare:

- slittamenti del progetto
- revisione delle tempistiche
- eventuali costi aggiuntivi

15. Servizi di terze parti

Alcuni servizi possono coinvolgere piattaforme o strumenti di terze parti, come:

- moduli o plugin
- servizi di hosting
- software in genere

IMSEO Srl non è responsabile sulle componenti di terze parti per eventuali:

- malfunzionamenti
- sospensioni

16. Proprietà dei lavori realizzati

Salvo diverso accordo contrattuale:

- i materiali realizzati per il Cliente diventano di sua proprietà **dopo il completo pagamento delle prestazioni previste nel contratto**
- IMSEO Srl può mantenere il diritto di utilizzo a fini di portfolio o promozione.

17. Riservatezza

Le parti si impegnano a mantenere riservate tutte le informazioni confidenziali scambiate durante il rapporto contrattuale.

18. Protezione dei dati personali

Il trattamento dei dati personali avviene nel rispetto del Regolamento Generale sulla Protezione dei Dati. Le modalità di trattamento sono descritte nella **Privacy Policy** pubblicata sul sito.

19. Limitazione di responsabilità

IMSEO Srl non potrà essere ritenuta responsabile per:

- danni indiretti
- perdita di profitto
- perdita di dati
- interruzioni di attività

La responsabilità complessiva della Società non potrà mai superare l'importo pagato dal Cliente per il servizio oggetto della controversia.

20. Forza maggiore

IMSEO Srl non sarà responsabile per ritardi o inadempimenti dovuti a cause di forza maggiore, tra cui:

- eventi naturali
- interruzioni di rete
- attacchi informatici
- eventi fuori dal controllo della Società.

21. Durata e recesso

Per i servizi continuativi:

- il contratto ha durata definita nel preventivo o ordine
- il Cliente può recedere con **preavviso di 30 giorni**, salvo diversa indicazione.

In caso di recesso anticipato potrebbero essere dovuti i costi delle attività già svolte.

22. Modifiche alle condizioni

IMSEO Srl si riserva il diritto di modificare le presenti condizioni. Le modifiche saranno pubblicate sul sito www.imseo.it.

23. Legge applicabile

Le presenti condizioni sono regolate dalla legge italiana.

24. Foro competente

Per ogni controversia sarà competente il **Foro della sede legale di IMSEO Srl**, salvo diversa disposizione di legge.

IMSEO Srl
I www.imseo.it - E info@imseo.it - P.IVA 11028431002
Sede legale: Via Simeto, 27 - 00198 - Roma (RM)
Tel. 0645427880

ALLEGATO - CLOUD SECURITY E PROTEZIONE DEI DATI

Addendum contrattuale ai servizi cloud

Il presente Allegato disciplina le misure di sicurezza, le responsabilità e le modalità di gestione dei dati personali nell'ambito dei servizi cloud forniti al Cliente.
Le disposizioni del presente Addendum integrano il contratto principale di fornitura dei servizi cloud e si applicano a tutti i sistemi e servizi erogati tramite infrastrutture cloud.

Fornitore: _____

Cliente: _____

1. Ruoli condivisi e responsabilità nell'ambiente cloud

(ISO/IEC 27017 – CLD.6.3.1)

Le Parti riconoscono che l'erogazione dei servizi cloud avviene secondo un modello di responsabilità condivisa tra:

- Cloud Service Provider (CSP)
- Fornitore del servizio cloud
- Cliente del servizio cloud

Al fine di garantire un'efficace gestione della sicurezza delle informazioni, i ruoli e le responsabilità delle parti sono chiaramente stabiliti, documentati e comunicati. In particolare:
Responsabilità del Cloud Service Provider
Il Cloud Service Provider è responsabile della sicurezza dell'infrastruttura cloud sottostante, inclusi:

- infrastruttura fisica dei data center
- sicurezza ambientale e controllo accessi fisici
- infrastruttura hardware e virtualizzazione

- disponibilità e resilienza della piattaforma cloud
- sicurezza della rete cloud e dei servizi di base

Responsabilità del Fornitore del servizio cloud

Il Fornitore è responsabile della configurazione e gestione dei servizi cloud erogati al Cliente, inclusi:

- configurazione delle risorse cloud
- gestione dei sistemi operativi e delle piattaforme applicative
- implementazione delle misure di sicurezza logiche
- monitoraggio dei sistemi e gestione degli incidenti
- gestione delle vulnerabilità e aggiornamenti di sicurezza

Responsabilità del Cliente

Il Cliente mantiene la responsabilità per:

- utilizzo corretto dei servizi cloud
- gestione degli utenti e delle credenziali di accesso
- classificazione e protezione dei dati caricati nei sistemi
- sicurezza dei dispositivi degli utenti finali
- conformità normativa relativa ai dati trattati

Le Parti possono definire inoltre accordi per:

- nominare un Responsabile del Trattamento dei dati (DPA)
- sottoscrivere una matrice RACI (Responsible, Accountable, Consulted, Informed) per documentare nel dettaglio la distribuzione delle responsabilità relative alla sicurezza dei servizi cloud

2. Rimozione delle risorse e dei dati del cliente dal servizio cloud

(ISO/IEC 27017 – CLD.8.1.5)

Alla cessazione del contratto o dell'accordo di servizio cloud il Fornitore provvede alla rimozione delle risorse e dei dati del Cliente tramite:

- restituzione dei dati in formato interoperabile e comunemente utilizzato se previsto in un contratto
- rimozione delle macchine virtuali e delle risorse allocate
- eliminazione delle configurazioni associate ai servizi cloud
- cancellazione sicura dei dati residui presenti nei sistemi attivi

La rimozione delle risorse e dei dati avverrà entro un periodo di 30 giorni, salvo diversa disposizione contrattuale.

3. Cooperazione per l'esercizio dei diritti degli interessati

(ISO/IEC 27018 – A.2.1)

Il Fornitore si impegna a cooperare con il Cliente al fine di consentire l'esercizio dei diritti degli interessati in relazione al trattamento dei dati personali effettuato tramite i servizi cloud.
Il Fornitore si impegna a mettere a disposizione strumenti per:

- l'accesso ai dati personali
- la rettifica o l'aggiornamento dei dati
- la cancellazione dei dati personali
- la limitazione del trattamento
- la portabilità dei dati

4. Informativa sul trattamento dei dati personali

Il Fornitore garantisce che le informazioni relative al trattamento dei dati personali effettuato nell'ambito dei servizi cloud siano rese disponibili al Cliente in modo trasparente.
L'informativa sul trattamento dei dati in capo al Fornitore include:

- comunicazioni circa la finalità del trattamento dei dati
- comunicazioni circa le categorie di dati trattati
- comunicazioni circa le modalità di trattamento
- comunicazioni circa le misure di sicurezza adottate
- comunicazioni circa eventuali trasferimenti internazionali di dati
- comunicazioni circa i tempi di conservazione dei dati

5. Cancellazione sicura dei file temporanei

(ISO/IEC 27018 – A.5.1)

I file e i documenti temporanei generati durante l'erogazione dei servizi cloud sono gestiti dal Fornitore in conformità alle seguenti procedure di sicurezza:

- i file temporanei contenenti dati personali sono sempre eliminati o distrutti in modo sicuro
- la cancellazione da parte del Fornitore avviene entro un periodo di 30 giorni, salvo diversa disposizione contrattuale
- non sono possibili accessi non autorizzati ai file temporanei

6. Notifica della diffusione dei dati personali (PII)

(ISO/IEC 27018 – A.6.1)

Il Fornitore ha previsto garanzie contrattuali e procedure operative per la gestione delle richieste di divulgazione di dati personali (Personally Identifiable Information – PII).
In particolare, il Fornitore avviserà tempestivamente il Cliente in caso di comunicazione di dati personali a terze parti, incluse autorità pubbliche, salvo divieto legale.
In caso di richiesta di divulgazione dei dati personali, il Fornitore adotta le seguenti azioni:
Per richieste non supportate da ordini giudiziari validi

- il Fornitore consulta preventivamente il Cliente del servizio cloud
- qualora il Cliente autorizzi la divulgazione, il Fornitore accetta la richiesta
- al Cliente viene notificata l'avvenuta divulgazione entro 24 ore

Richieste legalmente vincolanti
Nel caso di richieste provenienti da autorità competenti o supportate da provvedimenti giudiziari:

- il Fornitore verifica la validità legale della richiesta
- la divulgazione avviene solo nei limiti previsti dalla normativa applicabile
- il Cliente viene informato ove possibile e senza violare eventuali obblighi legali di riservatezza

7. Procedura per la restituzione, trasferimento ed eliminazione dei dati personali

(ISO/IEC 27018 – A.10.3)

La procedura si applica a:

- tutti i dati personali trattati dall'organizzazione in qualità di responsabile o titolare del trattamento
- tutti i sistemi informativi, archivi digitali e supporti fisici contenenti dati personali
- tutti i dipendenti, collaboratori e fornitori coinvolti nel trattamento dei dati

IMSEO Srl
I www.imseo.it - E info@imseo.it - P.IVA 11028431002
Sede legale: Via Simeto, 27 - 00198 - Roma (RM)
Tel. 0645427880

Ruoli e responsabilità:

- titolare del trattamento (autorizza le operazioni di restituzione, trasferimento o cancellazione)
- responsabile del trattamento / IT (esegue tecnicamente le operazioni)
- DPO, se nominato (verifica la conformità e fornisce consulenza)
- utenti autorizzati (segnalano richieste e garantiscono la corretta gestione)

La restituzione dei dati può avvenire in caso di:

- termine del contratto con il cliente
- richiesta esplicita del titolare
- cambio di fornitore o servizio

Modalità operative:

- identificazione e raccolta dei dati richiesti
- verifica dell'integrità e completezza
- esportazione in formato strutturato, leggibile e interoperabile (es. CSV, JSON, XML)
- trasferimento tramite canali sicuri (es. SFTP, HTTPS, supporti cifrati)

Sicurezza del trasferimento:

- Cifratura dei dati durante il trasferimento
- Autenticazione del destinatario
- Tracciamento dell'operazione

Il trasferimento dei dati è consentito solo se:

- Autorizzato dal titolare
- Conforme ai requisiti normativi (es. trasferimenti extra UE)
- Supportato da adeguate misure di sicurezza

Il processo del trasferimento deve avvenire rispettando questi step di esecuzione:

- valutazione del rischio del trasferimento

- definizione del metodo di trasporto sicuro
- applicazione di tecniche di cifratura e pseudonimizzazione (se necessario)
- verifica della corretta ricezione

Ogni trasferimento dei dati deve essere registrato indicando:

- data e ora
- tipologia di dati
- destinatario
- metodo utilizzato

I casi di eliminazione diretta dei dati personali avvengono dopo non oltre 30 giorni dalla:

- fine del periodo di conservazione
- revoca del consenso
- richiesta dell'interessato (diritto all'oblio)
- termine del contratto

I metodi di eliminazione diretta dei dati personali sono:

- dati digitali: cancellazione sicura (wipe) con sovrascrittura
- supporti fisici: distruzione certificata (triturazione, degaussing)
- backup: eliminazione secondo le politiche di retention

La verifica della eliminazione diretta dei dati avviene tramite:

- controllo dell'effettiva cancellazione
- test di non recuperabilità
- redazione di evidenze documentali

Tutte le operazioni sopra descritte devono essere tracciate, ossia registrate e conservate. I log devono includere utente, data, azione e sistema coinvolto. Le attività di tracciamento sono soggette a verifiche periodiche e audit interni

Nella gestione degli incidenti eventuali anomalie (es. perdita dati, accessi non autorizzati) devono essere:

- segnalate immediatamente
- gestite secondo la procedura di gestione degli incidenti
- comunicate, se necessario, alle autorità competenti

La conservazione delle evidenze delle operazioni (log, report, certificati di cancellazione) devono essere conservate secondo i requisiti normativi.

La procedura è soggetta a revisione periodica per:

- Adeguamento normativo
- Miglioramento dei controlli di sicurezza
- Ottimizzazione dei processi

8. Validità del presente allegato

Il presente Addendum entra in vigore alla data di sottoscrizione del contratto principale e rimane valido per tutta la durata del rapporto contrattuale tra le Parti.