

ALLEGATO – SPECIFICHE TECNICHE

Sicurezza delle informazioni, Business Continuity e Conformità ISO/IEC 27001

Premessa

La piattaforma **Moby** è erogata in modalità **Software as a Service (SaaS)**, accessibile via web, senza installazioni locali, con aggiornamenti centralizzati e gestione completa dell'infrastruttura a carico del fornitore.

1. Sicurezza delle informazioni e Business Continuity

La continuità operativa del software **Moby** è garantita dal provider del data center/hosting, ubicato sul territorio italiano, certificato secondo i seguenti standard internazionali:

- **ISO 9001:2015** – Sistema di Gestione per la Qualità
- **ISO 14001:2015** – Sistema di Gestione Ambientale
- **ISO/IEC 27001:2022** – Sistema di Gestione della Sicurezza delle Informazioni
- **ISO/IEC 27018:2019** – Protezione dei dati personali nei servizi cloud
- **ISO/IEC 50001:2018** – Sistema di Gestione dell'Energia

Il data center è inoltre dotato di certificazione **Facility TIER III**, con disponibilità infrastrutturale garantita pari al **99,982%** (SLA infrastrutturale del data center) su base mensile, operativa **24x7**.

Disponibilità del servizio

Servizio	Disponibilità	SLA (su base mensile)
Raggiungibilità della piattaforma Moby	24x7	99,9%

2. Backup e protezione del dato

2.1 Backup infrastrutturali

- Esecuzione di **backup incrementali giornalieri** delle macchine virtuali (VM)
- Pianificazione: **giornaliera alle ore 23:00**
- Politica di conservazione:
 - ultimi **7 giorni**: tutti i backup
 - da **7 a 30 giorni**: ultimo backup settimanale
 - da **30 giorni a 2 mesi**: ultimo backup mensile
 - mantenimento minimo di **5 punti di ripristino** per ciascuna finestra di retention
 - I backup sono conservati su **host separato**, appartenente al medesimo provider

2.2 Backup del database

- Backup del database tramite **Binary log (MariaDB/MySQL compatible)**
- Supporto alla **Point-in-Time Recovery (PITR)**, per il ripristino del dato a uno specifico istante temporale
- Retention allineata a quella dei backup infrastrutturali

3. SLA

3.1 Ripristino del dato

Evento	Tempo massimo di riconsegna del dato
Ripristino backup database	Entro 2 giorni lavorativi

Le richieste di ripristino devono essere inoltrate tramite il canale ufficiale di supporto:

support@mobyweb.it

I tempi indicati si intendono **come tempi di riconsegna del dato** e **non** come tempi di completa riattivazione del servizio.

3.2 Ripristino del servizio

Evento	Tempo massimo di ripristino servizio
Host down	Entro 48 ore *
Fermo applicativo Moby	Entro 2 giorni lavorativi**

*garantito dal fornitore hosting

** Il ripristino può prevedere l'utilizzo di un backup.

4. Gestione della sicurezza operativa

- Applicazione delle **patch di sicurezza** del sistema operativo e dei componenti applicativi con cadenza **quindicinale**
- Attività eseguite **manualmente**, compatibilmente con la disponibilità del servizio e garantendo **zero downtime** ove tecnicamente possibile
- Eventuali finestre di manutenzione programmata comunicate con almeno **5 giorni lavorativi di preavviso**
- Prima del rilascio delle **major release** vengono eseguiti test di sicurezza sul codice applicativo secondo le linee guida **OWASP**

5. Vulnerability Assessment

Vengono effettuati **Vulnerability Assessment (VA)** periodici di tipo **infrastrutturale**, mediante scansioni di rete sugli host esposti, finalizzate all'individuazione di:

- vulnerabilità note (CVE)
- configurazioni non sicure
- servizi di rete esposti

Sono previste **almeno 3 verifiche annue**.

Ambito e limitazioni delle VA

- **non includono** penetration test
 - **non includono** attività di brute force, privilege escalation o sfruttamento attivo delle vulnerabilità
- Eventuali azioni correttive (remediation) sono valutate ed eseguite sulla base delle evidenze emerse.

6. Architettura applicativa

Il sistema adotta un'architettura **RESTful**, composta da:

- **Web application** sviluppata in **Laravel**, responsabile della business logic e della persistenza del dato su **MariaDB (MySQL compatibile)**
- **Applicativi client** sviluppati in **Angular**, dedicati alla presentazione e alla gestione dell'interfaccia utente

7. Autenticazione e controllo accessi

L'autenticazione avviene tramite **JSON Web Token (JWT)**.

Il processo prevede l'autenticazione di tutti gli utenti (sia amministratori che non) mediante credenziali e **token OTP tramite App Authenticator o simili (autenticazione MFA)**.

Il token JWT è composto da:

- **Header** (metadati e algoritmo di firma)
- **Payload** (informazioni contestuali)
- **Signature**, generata tramite algoritmo di firma (es. HMAC o RSA) con chiave nota esclusivamente ai sistemi autorizzati

Le prime due parti sono codificate in formato **Base64URL**.

La firma garantisce autenticità e integrità del token.

8. Requisiti di accesso

- Software **web-based**, senza necessità di installazioni lato client
- Browser di riferimento per sviluppo e test: **Google Chrome**
- Compatibilità con i principali browser moderni basati su **Chromium, Firefox** ed **Edge**
- Sistema operativo: qualsiasi OS in grado di eseguire un browser moderno (Windows, macOS, Linux)

9. Integrazione con altri sistemi

Moby espone **API REST** per l'interscambio di dati con sistemi terzi (es. SAP).

Le integrazioni possono avvenire tramite:

- web services (es. Synlab)
- connettori applicativi, previa analisi tecnica e definizione del modello di integrazione

10. Restituzione dei dati

In caso di cessazione del contratto, i dati presenti nel database vengono messi a disposizione del Committente entro **30 giorni lavorativi**, in uno dei seguenti formati standard:

- CSV/Excel
- SQL
- PDF

La restituzione avviene nel rispetto del **Regolamento UE 679/2016 (GDPR)**