Allegato D

Misure Tecniche e Organizzative (TOMs), Business Continuity & Disaster Recovery

Definizioni

- **Backup**: copia di sicurezza periodica dei dati (full/incrementale) conservata cifrata per consentire il ripristino.
- **BC/DR (Business Continuity & Disaster Recovery)**: insieme di misure organizzative/tecniche volte a garantire la continuità dei servizi e il ripristino a seguito di eventi critici.
- **Failover**: passaggio controllato del carico verso una risorsa/istanza alternativa in caso di guasto o degrado.
- **Fault Domain**: insieme di risorse che condividono un possibile punto di guasto; l'isolamento tra domini riduce l'impatto dei malfunzionamenti.
- **Hardening**: applicazione di configurazioni e controlli di sicurezza per ridurre la superficie d'attacco di sistemi e applicazioni.
- **KMS (Key Management Service)**: servizio per la generazione, custodia, rotazione e controllo degli accessi alle chiavi crittografiche.
- **Least Privilege (Principio del Minimo Privilegio)**: concessione agli utenti/sistemi dei soli permessi strettamente necessari allo svolgimento delle attività.
- **Multi-Tenant (Isolamento Multi-Tenant)**: architettura in cui più tenant condividono l'infrastruttura applicativa con isolamento logico dei dati e delle configurazioni.
- **NTP (Network Time Protocol)**: protocollo di sincronizzazione oraria usato per allineare i clock dei sistemi e garantire coerenza dei log.

- **Pen-Test (Penetration Test)**: test di sicurezza condotto da terza parte per individuare vulnerabilità sfruttabili e valutarne l'impatto.
- **RPO (Recovery Point Objective)**: massimo intervallo di dati che si può perdere in caso di disastro (obiettivo di punto di ripristino).
- **RTO (Recovery Time Objective)**: tempo massimo entro cui il servizio deve essere ripristinato dopo un disastro (obiettivo di tempo di ripristino).
- **Secure SDLC**: ciclo di vita di sviluppo software che integra controlli di sicurezza (code review, analisi statica/dinamica, gestione dipendenze).
- **Segregazione degli Ambienti**: separazione tra ambienti di sviluppo, test/UAT e produzione, con controlli di accesso e deployment distinti.
- **Snapshot**: cattura puntuale dello stato di dati/volumi per accelerare backup e restore.
- **TOMs (Technical and Organisational Measures)**: misure tecniche e organizzative adottate per sicurezza delle informazioni e conformità.
- **Tombstoning (dei backup)**: marcatura e ciclo di eliminazione controllata dei backup scaduti, nel rispetto delle policy di retention.
- **WAF (Web Application Firewall)**: controllo perimetrale che filtra e monitora il traffico HTTP/HTTPS verso l'applicazione per bloccare pattern malevoli.

1. Scopo, ambito e riferimenti

1.1 Finalità. Il presente Allegato definisce le TOMs per le Piattaforme WMP/VMP e i piani BC/DR.

1.2 Coerenza contrattuale. Si coordina con: MSA §§ 3, 4, 7, 8, 9, 14, 15, 18 e con lo SLA – Allegato C per: oggetto/perimetro (§1), misurazione disponibilità (§2), target e crediti (§3), claim (§4), manutenzioni (§5), esclusioni (§6) e gestione incidenti (§7).

1.3 Ambito soggettivo. Le TOMs si applicano a TimeFlow; gli obblighi della Committente restano quelli di MSA §7.

1.4 Ambito oggettivo. Copre ambienti di produzione WMP/VMP e connettori ufficiali. Ambienti sandbox/UAT sono non produttivi per MSA §2.8 (no dati reali salvo accordo scritto e misure aggiuntive).

2. TOMs – Misure tecniche e organizzative

2.1 Sicurezza dei dati.

a) **Cifratura in transito e a riposo:** TLS 1.2+; HSTS ove applicabile. Tutti i dati persistenti, inclusi quelli nei database e nei backup, sono cifrati tramite algoritmo AES-256.

b) **Gestione chiavi:** KMS in UE/SEE, rotazione ≥ annuale e on-demand; accessi segregati.

2.2 Controllo accessi e identità.

a) Least privilege e segregazione dei compiti; review periodica degli accessi.

b) MFA per account amministrativi TimeFlow e canali privilegiati; SSO/MFA per utenti Committente ove abilitato (cfr. MSA §4.4).

c) Politiche password/sessioni conformi a buone pratiche.

2.3 Isolamento e architettura.

a) Isolamento multi-tenant; separazione dev/test/UAT/prod. Sicurezza fisica demandata al cloud provider.

b) Segmentazione di rete, WAF, controlli d'ingresso; hardening baseline (linee guida CIS ove applicabili).

c) Storage/compute in UE/SEE; eventuali trasferimenti extra-SEE solo ai sensi di MSA §8.3 e Allegato G.

2.4 Sicurezza applicativa e SDLC.

a) Secure SDLC con code review, analisi statica/dinamica, gestione dipendenze.

b) Secrets in vault; nessun segreto in chiaro nel codice.

c) API security: OAuth2/OpenID Connect o SAML 2.0; schema validation; rate-limit/throttling coerenti con MSA §2.4; versionamento e deprecazioni secondo MSA §9.5 (Change management).

2.5 Log, monitoraggio e osservabilità.

a) Log centralizzati (app, sicurezza, audit) con NTP.

b) Telemetria/alerting su eventi critici; integrazione con incident management come da SLA – Allegato C §7.

c) Retention log: ≥ 180 giorni (sicurezza/audit), estendibile fino a 12 mesi ove richiesto; log cifrati e accessibili a ruoli autorizzati.

2.6 Dati non-prod e minimizzazione.

a) Sandbox/UAT: nessun dato reale salvo accordo scritto con misure dedicate (cfr. MSA §2.8).

b) Minimizzazione; masking/pseudonimizzazione ove necessario.

2.7 Servizi terzi (e-mail/SMS, ecc.).

Uso di provider qualificati; parametri e disponibilità governati da Allegato G e dalle Esclusioni SLA (Allegato C §6).

3. Vulnerabilità, patching e test di sicurezza

3.1 Gestione vulnerabilità. Scansioni continue; remediation: Critiche ≤ 7 gg, Alte ≤ 30 gg, Medie ≤ 90 gg, Basse ≤ 180 gg (ammesse mitigazioni compensative documentate).

3.2 Patching. Aggiornamenti sicurezza OS/middleware/DB/app secondo risk-based policy; finestre per SLA – Allegato C §5 (manutenzioni).

3.3 Pen-test e assessment. Almeno annuale con terza parte; executive summary condivisibile su richiesta con oscuramento dei dettagli sensibili (cfr. MSA §9.4).

3.4 Supply-chain. Due diligence su fornitori critici e OSS; distinta dipendenze mantenuta; controlli integrità immagini/container.

3.5 Resilienza & rate-limit. Enforcement rate-limit; degradazione controllata (cache/queue/back-pressure) e blocchi proporzionati su traffico malevolo/DoS; i casi esclusi dal conteggio disponibilità seguono SLA – Allegato C §6.

4. Incident response, comunicazioni e data breach

4.1 Processo incidenti. Rilevazione, triage e severità SEV-1/2/3/4; ack/aggiornamenti/restore secondo SLA – Allegato C §7 (gestione incidenti).

4.2 Notifiche e tempi.

a) Avvisi operativi tramite i canali previsti in SLA – Allegato C §9; RFO entro 24h e RCA entro 5/10 g lavorativi come da SLA – Allegato C §7.

b) Incidenti con dati personali: notifica senza ingiustificato ritardo ed entro 72 ore dalla conoscenza (cfr. MSA §8.5).

4.3 Evidenze e forensics. Conservazione log e catena di custodia; collaborazione ragionevole verso Autorità/interessati (cfr. MSA §8.6).

4.4 Clock-stop e dipendenze. I timer operativi si sospendono in attesa di asset/risposte della Committente o per dipendenze terze, come definito nello SLA – Allegato C (Definizioni "Clock-Stop" e §6, lett. l).

5. Business Continuity & Disaster Recovery

5.1 Architettura e continuità. Ridondanza componenti critiche; backup/snapshot cifrati; isolamento fault-domain; piani di failover documentati.

5.2 Backup e restore. a) **Backup:** almeno giornalieri (full/incrementali) con retention ≥ 30 giorni; cifrati in UE/SEE. b) **Test di restore:** trimestrali su dataset rappresentativi; evidenze disponibili su richiesta.

5.3 Obiettivi di ripristino (DR).

- **Standard:** RPO ≤ 30 min; RTO ≤ 8 ore.
- **Alta disponibilità** (se prevista in Ordine): RPO ≤ 15 min; RTO ≤ 4 ore.

(Gli obiettivi DR sono separati dai target operativi di gestione incidenti dello SLA – Allegato C §7.)

5.4 Esercitazioni DR. Almeno annuali (table-top e/o tecniche) con CAPA su eventuali scostamenti.

5.5 Provider e dipendenze. Outage esclusivamente imputabili al provider cloud/servizi esterni rientrano nelle Esclusioni SLA – Allegato C §6; resta l'obbligo di attivare mitigazioni e piani BC/DR.

5.6 Rollback e coerenza dati. In caso di change non riuscito o difetto bloccante, rollback ove tecnicamente possibile; integrità e tracciabilità prioritarie (MSA §9.5).

6. Ciclo di vita dei dati, portabilità ed exit

6.1 Portabilità ed export. Alla cessazione, su richiesta entro 5 giorni dalla comunicazione della cessazione, export una tantum in CSV/JSON con dizionario campi (MSA §8.7). Formati/estrazioni ulteriori o assistenza exit sono a quotazione.

6.2 Cancellazione e backup (tombstoning). Decorso il termine di cui sopra, cancellazione e tombstoning secondo policy; attestazione su richiesta (MSA §8.7).

6.3 Retention operativa. Dati applicativi per la durata del servizio; retention specifiche dei log in §2.5.

6.4 Dati speciali. Divieto di caricare categorie particolari/giudiziari salvo quanto previsto in MSA §8 e nel DPA (VMP) o informativa WMP.

6.5 Export/copie locali della Committente. Restano sotto responsabilità della Committente (sicurezza/retention) per MSA §7.

7. Fornitori esterni, trasferimenti e audit

7.1 Subfornitori e localizzazione. Elenco e regole in Allegato G; notifiche variazioni e diritto di opposizione (VMP) per MSA §15; flow-down di sicurezza/privacy per MSA §15.

7.2 Trasferimenti extra-SEE. Solo ai sensi del Capo V GDPR (SCC, misure supplementari) per MSA §8.3 e Allegato G.

7.3 Audit e trasparenza. Questionari/attestazioni/audit documentali o on-site nei termini di MSA §9.4, tutelando le informazioni riservate (MSA §13).

8. Ordine di precedenza e aggiornamenti

8.1 Precedenza documenti: Ordine → MSA → SLA (Allegato C) → Allegati tecnici (incl. D).

8.2 Aggiornamenti TOMs. TimeFlow può aggiornare il presente Allegato nei limiti di MSA §18.3 (nessun peggioramento sostanziale, preavviso 30 giorni); variazioni materiali richiedono accordo ai sensi di MSA §18.4. Le modifiche non hanno effetto retroattivo.

Ultima modifica: 18/11/2025 – Versione TOMs-2025-11-18