PIANO DI TRATTAMENTO DEL RISCHIO (RISK TREATMENT PLAN - RTP)

Il presente documento definisce le azioni correttive, i controlli di sicurezza implementati o pianificati, i ruoli di responsabilità e le tempistiche per mitigare, trasferire o accettare i rischi emersi durante la valutazione del rischio (*Risk Assessment*) relativa alla piattaforma *Forma Cloud LMS* e ai servizi correlati.

Tabella Operativa di Trattamento del Rischio

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-01	Codice sorgente (Forma LMS / Plugin)	**9 (Critico)**	**Mitigazione**	Analisi automatizzata SAST/DAST integrata nella pipeline CI/CD (Secure SDLC) e patch management automatizzato.	**Già attiva**	Lead Developer / DevOps	Monitoraggio continuo (Patch entro 48h per falle critiche)	**2 (Basso)**

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-02	Cloud Hosting (AWS) & Database	**6 (Alto)**	**Mitigazione**	Autenticazione a Due Fattori (MFA) obbligatoria per amministratori, politica del minimo privilegio IAM e cifratura dati.	**Già applicata**	System Administrator	Revisione permessi semestrale	**2 (Basso)**
RSK-03	Piattaforma SaaS (Forma Cloud LMS)	**6 (Alto)**	**Mitigazione / Trasferimento**	Accordi SLA con provider AWS, backup automatici multi-regione e test DRP.	**Già attive**	IT Operations Manager	**Test DRP Annuale** (e al cambio di architettura)	**2 (Basso)**
RSK-04	Dati dei Clienti / GDPR	**6 (Alto)**	**Mitigazione**	Cifratura end-to-end in transito (HTTPS/TLS) e a riposo per DB cloud. Sottoscrizione DPA (IT/EN).	**Già attive**	DPO / Legal	Operativo permanente / Aggiornamento contratti	**2 (Basso)**
RSK-05	Dispositivi Dipendenti / Workstation	**4 (Medio)**	**Mitigazione**	Cifratura dischi (BitLocker/FileVault), blocco schermo e policy Clean Screen.	**Già applicata**	IT Helpdesk	Verifiche periodiche sui dispositivi	**1 (Basso)**

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-06	Supply Chain / Fornitori Terzi	**4 (Medio)**	**Mitigazione**	Processo di Due Diligence preventiva e clausole contrattuali di sicurezza nei contratti.	**In corso di formalizzazione**	Management / Legal	Completamento entro 90 giorni	**1 (Basso)**
RSK-07	Reputazione e Proprietà Intellettuale	**3 (Medio)**	**Mitigazione**	Repository Git privati con branch protection, gestione ruoli granulare e backup immutabili.	**Già applicata**	Lead Developer	Operativo permanente	**1 (Basso)**
RSK-08	Personale interno e Collaboratori	**4 (Medio)**	**Mitigazione**	Piano annuale di Security Awareness, formazione e sicurezza e simulazioni di phishing.	**In corso / Pianificato**	HR / Responsabile SGSI	Avvio entro 60 giorni (cadenza annuale)	**1 (Basso)**

Modalità di Riesame e Monitoraggio

1. **Verifica dell'attuazione:** Il Responsabile della Sicurezza verifica lo stato di avanzamento delle azioni correttive definite nell'RTP con cadenza trimestrale.
2. **Aggiornamento del Piano:** Il Piano di Trattamento del Rischio viene riesaminato e aggiornato formalmente almeno una volta all'anno in occasione del *Riesame della Direzione*, oppure a seguito di incidenti di sicurezza significativi o modifiche rilevanti dell'infrastruttura tecnologica.

Revision #4
Created 2026-10-18 18:53:14 UTC by Alberto Pastorelli
Updated 2026-10-18 19:18:25 UTC by Alberto Pastorelli