DICHIARAZIONE DI APPLICABILITÀ (STATEMENT OF APPLICABILITY - SoA)

Conforme alla Norma ISO/IEC 27001:2022

Organizzazione: Forma Farm S.r.l.
Sede Legale: Via Savona 10, 20144 Milano (MI)
Modello Operativo: 100% Full Remote / Distributed Organization
Infrastruttura: Cloud Hosting AWS (Amazon Web Services) & Servizi Managed SaaS
Versione Documento: 1.0
Data del Documento: Ottobre 2026

---

1. INTRODUZIONE E CRITERI DI SELEZIONE

Il presente documento costituisce la **Dichiarazione di Applicabilità (SoA)** del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di **Forma Farm S.r.l.**, redatta in conformità ai requisiti della norma **ISO/IEC 27001:2022** (Allegato A).

1.1 Contesto e Specificità Operative

Forma Farm S.r.l. sviluppa, eroga e gestisce in modalità SaaS la piattaforma e-learning *Forma Cloud LMS*, i relativi plugin e servizi integrati. L'organizzazione adotta un modello **100% Full Remote**, privo di server o data center fisici di proprietà; l'intera infrastruttura applicativa e di memorizzazione dati è ospitata presso il Cloud Provider **AWS (Amazon Web Services)**.

1.2 Criteri di Inclusione ed Esclusione dei Controlli

I controlli dell'Allegato A della norma ISO/IEC 27001:2022 sono stati valutati e selezionati in base a:

1. Risultati della valutazione dei rischi (Risk Assessment) declinati nel *Registro dei Rischi* e nel *Piano di Trattamento del Rischio (RTP)*.
2. Requisiti cogenti e normativi (es. Regolamento UE 2016/679 - GDPR, normative sul diritto d'autore e proprietà intellettuale).
3. Obblighi contrattuali stipulati con i clienti (SLA, Data Processing Agreement - DPA).
4. Esigenze operative del modello di business SaaS/Cloud e lavoro da remoto.

---

2. MATRICE DEI CONTROLLI ISO/IEC 27001:2022

Sezione A.5 — Controlli Organizzativi (Organizational Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.1	Politiche per la sicurezza delle informazioni	**Sì**	Implementato	Politica di Sicurezza delle Informazioni definita e approvata dalla Direzione.
A.5.2	Ruoli e responsabilità per la sicurezza	**Sì**	Implementato	Assegnazione formale delle responsabilità SGSI (Direzione, Lead Dev, Admin, DPO).
A.5.3	Segregazione dei compiti	**Sì**	Implementato	Separazione dei ruoli tra ambienti di dev/test e produzione cloud AWS.
A.5.4	Responsabilità della direzione	**Sì**	Implementato	Coinvolgimento attivo nei Riesami della Direzione e nell'allocazione delle risorse SGSI.
A.5.5	Contatto con le autorità	**Sì**	Implementato	Procedure di contatto per Data Breach con il Garante Privacy e CSIRT Italia.
A.5.6	Contatto con gruppi di interesse speciale	**Sì**	Implementato	Partecipazione a community Open Source (Forma LMS) e forum sulla sicurezza cloud.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.7	Threat intelligence	**Sì**	Implementato	Monitoraggio di bollettini CVE, feed di sicurezza AWS e dipendenze software.
A.5.8	Sicurezza delle informazioni nella gestione dei progetti	**Sì**	Implementato	Integrazione della sicurezza nella roadmap di prodotto e nello sviluppo plugin.
A.5.9	Inventario delle informazioni e degli altri asset associati	**Sì**	Implementato	Inventario formale degli asset (codice, account cloud, dati clienti, laptop aziendali).
A.5.10	Uso ammissibile delle informazioni e degli asset	**Sì**	Implementato	Definizione dell'Acceptable Use Policy nell'Information Security Policy e contratti.
A.5.11	Restituzione degli asset	**Sì**	Implementato	Procedura di offboarding con revoca utenze e restituzione/wipe dei dispositivi.
A.5.12	Classificazione delle informazioni	**Sì**	Implementato	Definizione di 4 livelli di riservatezza (Pubblico, Interno, Confidenziale, Dati Personali).
A.5.13	Etichettatura delle informazioni	**Sì**	Implementato	Applicazione di tag e criteri logici sui repository Git, DB e bucket S3.
A.5.14	Trasferimento di informazioni	**Sì**	Implementato	Utilizzo esclusivo di canali cifrati (TLS/HTTPS, SSH) e clausole contrattuali DPA.
A.5.15	Controllo degli accessi	**Sì**	Implementato	Principio del minimo privilegio gestito via IAM policy e ruoli ruotati.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.16	Gestione delle identità	**Sì**	Implementato	Processo formalizzato di provisioning e de-provisioning delle utenze aziendali.
A.5.17	Informazioni per l'autenticazione	**Sì**	Implementato	Gestione credenziali tramite Password Manager aziendale e obbligo di password complesse.
A.5.18	Diritti di accesso	**Sì**	Implementato	Revisione periodica (semestrale) delle ACL e delle policy IAM su AWS e GitHub.
A.5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	**Sì**	Implementato	Valutazione della sicurezza dei fornitori critici (AWS, SaaS terzi).
A.5.20	Indirizzamento della sicurezza nei contratti con i fornitori	**Sì**	Implementato	Clausole di sicurezza e riservatezza nei contratti e sottoscrizione DPA.
A.5.21	Gestione della sicurezza nella catena di fornitura ICT	**Sì**	In corso	Procedura di due diligence e verifica della sicurezza delle librerie Open Source.
A.5.22	Monitoraggio, riesame e gestione dei servizi dei fornitori	**Sì**	Implementato	Verifiche continue sugli SLA dei Cloud Provider e sui report di conformità SOC/ISO.
A.5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	**Sì**	Implementato	Configurazione conforme alle best-practice di sicurezza cloud AWS (CIS Benchmark).
A.5.24	Gestione degli incidenti per la sicurezza delle informazioni	**Sì**	Implementato	Procedura formale per rilevazione, escalation e notifica di incidenti/Data Breach.
A.5.25	Valutazione e decisione sugli eventi di sicurezza	**Sì**	Implementato	Criteri di classificazione della gravità degli eventi correlati alle risorse Cloud.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.26	Risposta agli incidenti di sicurezza	**Sì**	Implementato	Piani di risposta rapida per isolamento istanze, ripristino backup e patch emergenti.
A.5.27	Apprendimento dagli incidenti di sicurezza	**Sì**	Implementato	Post-mortem analysis e aggiornamento dei controlli a seguito di anomalie/incidenti.
A.5.28	Raccolta di prove	**Sì**	Implementato	Tracciabilità dei log di audit AWS CloudTrail e audit log di sistema per uso forense.
A.5.29	Sicurezza delle informazioni durante l'interruzione	**Sì**	Implementato	Piano di Continuità Operativa e Disaster Recovery per la piattaforma LMS.
A.5.30	PR di ICT per la continuità operativa	**Sì**	Implementato	Replicazione multi-AZ dei dati e procedure automatizzate di failover su AWS.
A.5.31	Requisiti legali, statutari, normativi e contrattuali	**Sì**	Implementato	Registro di conformità normativa (GDPR, Proprietà Intellettuale, Contratti Clienti).
A.5.32	Diritti di proprietà intellettuale	**Sì**	Implementato	Tutela del codice proprietario (Forma Factory/Plugin) e rispetto licenze Open Source.
A.5.33	Protezione dei registri (records)	**Sì**	Implementato	Conservazione sicura e immutabile dei log e dei documenti fiscali/legali.
A.5.34	Privacy e protezione dei dati personali (PII)	**Sì**	Implementato	Nomina a Responsabile del Trattamento (DPA), nomina DPO e rispetto del GDPR.
A.5.35	Riesame indipendente della sicurezza	**Sì**	Implementato	Audit interni programmati e verifiche da parte di enti di certificazione terzi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.36	Conformità con politiche e standard di sicurezza	**Sì**	Implementato	Verifiche periodiche sull'applicazione delle policy da parte del personale.
A.5.37	Procedure operative documentate	**Sì**	Implementato	Documentazione tecnica di deploy, gestione server, backup e manutenzione LMS.

Sezione A.6 — Controlli sulle Persone (People Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.6.1	Screening	**Sì**	Implementato	Verifiche pre-assunzione (curriculum, referenze, assenza di condanne) per nuovi assunti.
A.6.2	Termini e condizioni di impiego	**Sì**	Implementato	Clausole di riservatezza (NDA) ed etica professionale integrate nei contratti di lavoro.
A.6.3	Consapevolezza, istruzione e formazione	**Sì**	In corso	Piano di formazione annuale in *Security Awareness* e simulazioni di phishing.
A.6.4	Processo disciplinare	**Sì**	Implementato	Richiamo al CCNL applicabile per le violazioni delle politiche di sicurezza.
A.6.5	Responsabilità post-impiego	**Sì**	Implementato	Obbligo di riservatezza permanente e revoca totale degli accessi al termine del rapporto.
A.6.6	Accordi di riservatezza o non divulgazione	**Sì**	Implementato	Sottoscrizione di NDA con tutti i dipendenti, collaboratori esterni e fornitori terzi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.6.7	Lavoro da remoto (Remote working)	**Sì**	Implementato	**Controllo critico:** Regolamento di Telelavoro/Smart Working, uso VPN/TLS e dispositivi protetti.
A.6.8	Segnalazione di eventi di sicurezza	**Sì**	Implementato	Canale di segnalazione interno tempestivo per anomalie, phishing o smarrimento dispositivi.

Sezione A.7 — Controlli Fisici (Physical Controls)

> **Nota metodologica sul modello Full Remote:** Poiché Forma Farm S.r.l. non gestisce server o perimetri fisici di data center (interamente in outsourcing ad AWS), i controlli fisici perimetrali tradizionali sono dichiarati **Non Applicabili (Esclusi)** o adattati esclusivamente alla sicurezza delle postazioni di lavoro domiciliari/nomadi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.1	Perimetri di sicurezza fisica	**No**	Escluso	**Non applicabile:** Assenza di perimetri fisici aziendali o server locali (infrastruttura 100% AWS).
A.7.2	Ingresso fisico	**No**	Escluso	**Non applicabile:** Inesistenti aree ad accesso controllato o sale server proprie.
A.7.3	Mantenimento di uffici, stanze e strutture	**No**	Escluso	**Non applicabile:** Organizzazione operativamente 100% distribuita in remote working.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.4	Monitoraggio della sicurezza fisica	**No**	Escluso	**Non applicabile:** Gestito autonomamente da AWS per i propri Data Center (certificati ISO 27001).
A.7.5	Protezione contro minacce fisiche e ambientali	**No**	Escluso	**Non applicabile:** Delega della sicurezza fisica dei server al Cloud Provider (AWS).
A.7.6	Lavoro in aree sicure	**No**	Escluso	**Non applicabile:** Nessuna area ad alto rischio fisico o di produzione gestita in sede.
A.7.7	Scrivania pulita e schermo pulito (Clean desk/screen)	**Sì**	Implementato	Applicabile alle postazioni di lavoro dei remotisti: blocco schermo automatico e no stampe.
A.7.8	Posizionamento e protezione delle apparecchiature	**Sì**	Implementato	Obbligo di custodia fisica e non abbandono dei laptop/dispositivi aziendali in luoghi pubblici.
A.7.9	Sicurezza degli asset fuori dalle sedi	**Sì**	Implementato	Regolamentazione dell'uso dei computer portatili durante trasferte o spostamenti.
A.7.10	Supporti di memorizzazione (Storage media)	**Sì**	Implementato	Divieto d'uso di pendrive/hard-disk USB non cifrati per il trasferimento di dati riservati.
A.7.11	Utenze di servizio (Utilities)	**No**	Escluso	**Non applicabile:** Gestione di energia/climatizzazione affidata interamente al provider AWS.
A.7.12	Sicurezza del cablaggio	**No**	Escluso	**Non applicabile:** Assenza di infrastruttura di rete cablata proprietaria.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.13	Manutenzione delle apparecchiature	**Sì**	Implementato	Manutenzione e sostituzione ordinaria dei laptop di lavoro gestita via Helpdesk/IT.
A.7.14	Smaltimento o riutilizzo sicuro degli asset	**Sì**	Implementato	Wipe crittografico/distruzione sicura dei dischi prima della dismissione dei notebook.

Sezione A.8 — Controlli Tecnologici (Technological Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.1	Dispositivi degli utenti finali (User endpoint devices)	**Sì**	Implementato	Cifratura integrale del disco (BitLocker/FileVault), antivirus e OS sempre aggiornato.
A.8.2	Diritti di accesso privilegiato	**Sì**	Implementato	Restrizione rigorosa dell'accesso Root/Admin su AWS e sistemi di produzione.
A.8.3	Restrizione dell'accesso alle informazioni	**Sì**	Implementato	Isolamento dei DB per cliente e segregazione dell'accesso ai dati di produzione LMS.
A.8.4	Accesso al codice sorgente	**Sì**	Implementato	Accesso ai repository GitHub/GitLab regolato da ruoli, MFA e branch protection.
A.8.5	Autenticazione sicura	**Sì**	Implementato	Obbligo tassativo di Autenticazione a Due Fattori (MFA) su tutte le risorse cloud/SaaS.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.6	Capacity management	**Sì**	Implementato	Autoscaling e monitoraggio risorse via AWS CloudWatch per prevenire saturazioni.
A.8.7	Protezione contro i malware	**Sì**	Implementato	Soluzioni Endpoint Protection (EDR/Antivirus) sulle workstation e scansioni container.
A.8.8	Gestione delle vulnerabilità tecniche	**Sì**	Implementato	Scansione automatizzata di codice e librerie (SAST/DAST) in pipeline CI/CD; patch in 48h.
A.8.9	Gestione della configurazione	**Sì**	Implementato	Infrastruttura definita come codice (IaC) e configurazioni di sicurezza standardizzate.
A.8.10	Cancellazione delle informazioni	**Sì**	Implementato	Script automatizzati per la cancellazione sicura dei dati al termine dei contratti (DPA).
A.8.11	Mascheramento dei dati (Data masking)	**Sì**	Implementato	Anonomizzazione/Pseudonimizzazione dei dati di produzione usati in ambienti di test.
A.8.12	Prevenzione della fuga di dati (DLP)	**Sì**	Implementato	Restrizione dei download, blocco condivisioni pubbliche di bucket S3 e monitoraggio log.
A.8.13	Backup delle informazioni	**Sì**	Implementato	Backup automatici giornalieri multi-regione AWS con test di ripristino periodici.
A.8.14	Ridondanza delle strutture di elaborazione	**Sì**	Implementato	Architettura Cloud distribuita su più Multi-Availability Zone (Multi-AZ AWS).

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.15	Logging	**Sì**	Implementato	Abilitazione di log centralizzati su AWS CloudWatch/CloudTrail e conservazione protetta.
A.8.16	Attività di monitoraggio	**Sì**	Implementato	Allarmi in tempo reale per accessi anomali, errori di sistema o picchi di traffico.
A.8.17	Sincronizzazione dell'ora	**Sì**	Implementato	Sincronizzazione automatica del tempo su server e container tramite NTP (AWS Time Sync).
A.8.18	Uso di programmi di utilità privilegiati	**Sì**	Implementato	Restrizione dell'uso di tool di sistema e tracciamento dei comandi amministrativi.
A.8.19	Installazione di software sui sistemi operativi	**Sì**	Implementato	Blocco dell'installazione di software non autorizzato sulle postazioni di lavoro.
A.8.20	Sicurezza delle reti	**Sì**	Implementato	Utilizzo di VPC (Virtual Private Cloud), subnet private e Security Group su AWS.
A.8.21	Sicurezza dei servizi di rete	**Sì**	Implementato	Utilizzo di HTTPS, firewall applicativi (WAF) e protezione anti-DDoS (AWS Shield).
A.8.22	Segregazione delle reti	**Sì**	Implementato	Separazione logica tra ambienti aziendali, ambienti Dev/Staging e Production Cloud.
A.8.23	Filtraggio web	**Sì**	Implementato	Protezione DNS/Endpoint per prevenire la navigazione su siti malevoli o di phishing.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.24	Uso della crittografia	**Sì**	Implementato	Cifratura dei dati in transito (TLS 1.2/1.3) e a riposo (AES-256 su database e storage).
A.8.25	Ciclo di vita dello sviluppo sicuro (Secure SDLC)	**Sì**	Implementato	Linee guida per lo sviluppo sicuro, code review obbligatoria e test di sicurezza.
A.8.26	Requisiti di sicurezza delle applicazioni	**Sì**	Implementato	Analisi dei requisiti di sicurezza per tutti i nuovi moduli o plugin di Forma LMS.
A.8.27	Architettura dei sistemi sicuri e principi di ingegneria	**Sì**	Implementato	Progettazione basata su principi di *Defense in Depth* e *Zero Trust* .
A.8.28	Coding sicuro	**Sì**	Implementato	Adozione degli standard OWASP Top 10 nelle prassi di programmazione del team Dev.
A.8.29	Test di sicurezza nello sviluppo e nell'accettazione	**Sì**	Implementato	Scansioni SAST/DAST e test di collaudo prima di ogni release in produzione.
A.8.30	Sviluppo esternalizzato	**Sì**	Implementato	Controllo del codice e review rigorosa per i plugin forniti da terzi/freelance.
A.8.31	Separazione degli ambienti di sviluppo, test e produzione	**Sì**	Implementato	Ambienti cloud separati e isolati; nessun dato reale di produzione in dev/test.
A.8.32	Gestione del cambiamento (Change management)	**Sì**	Implementato	Flusso di approvazione e tracciamento delle modifiche al codice e all'infrastruttura.
A.8.33	Informazioni di test	**Sì**	Implementato	Utilizzo esclusivo di dati sintetici o pseudonimizzati per gli ambienti di test.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.34	Protezione dei sistemi di informazione durante i test	**Sì**	Implementato	Limitazione e monitoraggio degli accessi agli ambienti di staging e collaudo.

3. SINTESI E APPROVAZIONE

- **Totale controlli ISO/IEC 27001:2022:** 93
- **Controlli Dichiarati Applicabili:** 86
- **Controlli Esclusi (Non Applicabili):** 7 (tutti relativi alla sicurezza fisica perimetrale, motivati dall'architettura 100% Cloud e dal modello organizzativo Full Remote).

La presente Dichiarazione di Applicabilità è approvata dalla Direzione di **Forma Farm S.r.l.** ed è soggetta a riesame almeno annuale o in coincidenza con modifiche rilevanti dell'infrastruttura tecnologica e dei processi di business.

Milano, Ottobre 2026
Forma Farm S.r.l. — La Direzione

Revision #2
Created 2026-10-18 19:15:26 UTC by Alberto Pastorelli
Updated 2026-10-19 14:02:34 UTC by Alberto Pastorelli