# Governance - Politiche e Quadro di Riferimento


- POLITICA DI SICUREZZA DELLE INFORMAZIONI
- POLITICHE SPECIFICHE DI DOMINIO
- Ruoli e Responsabilità
- Assegnazione Ruoli e Responsabilità SGSI

# POLITICA DI SICUREZZA DELLE INFORMAZIONI

## Obiettivi e Scopo

La Direzione di Forma Farm S.r.l. (con sede legale in Via Savona 10, Milano) riconosce la sicurezza delle informazioni, la protezione dei dati personali e la continuità dei servizi e-learning erogati tramite Forma Cloud LMS come elementi strategici fondamentali per il successo aziendale e per la tutela della fiducia dei propri clienti, partner e utenti. Il presente documento stabilisce i principi guida, le responsabilità e il quadro di riferimento per la sicurezza delle informazioni all'interno dell'organizzazione, in conformità agli standard internazionali ISO/IEC 27001 e al Regolamento UE 2016/679 (GDPR).

## Campo di Applicazione (Scope)

La presente politica si applica a:

- Tutti i dipendenti, collaboratori, consulenti e fornitori terzi di Forma Farm S.r.l.
- Tutti gli asset informativi aziendali, inclusi i sistemi di cloud hosting, le infrastrutture di rete, i codici sorgente dei plugin e della piattaforma Forma Lms, i dati dei clienti e la documentazione tecnica e amministrativa.
- Tutti i processi aziendali legati allo sviluppo software, alla gestione dell'assistenza tecnica (Helpdesk), al monitoraggio dei server e all'erogazione dei servizi SaaS.

## Principi Fondamentali della Sicurezza

Forma Farm S.r.l. adotta e persegue i tre pilastri classici della sicurezza delle informazioni:

1. **Confidenzialità**: Garantire che l'accesso alle informazioni e ai dati dei clienti sia consentito esclusivamente ai soggetti autorizzati.

2. **Integrità**: Salvaguardare l'accuratezza e la completezza delle informazioni, dei dati di training e del software da modifiche non autorizzate o accidentali.
3. **Disponibilità**: Assicurare che i sistemi e le piattaforme cloud siano accessibili e utilizzabili dagli utenti autorizzati secondo i livelli di servizio concordati.

# Impegni della Direzione

La Direzione si impegna a:

1. Definire, riesaminare periodicamente e aggiornare gli obiettivi di sicurezza delle informazioni.
2. Garantire adeguate risorse finanziarie, tecnologiche e umane per la gestione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
3. Promuovere una cultura aziendale orientata alla sicurezza attraverso piani di formazione e sensibilizzazione (Security Awareness) rivolti al personale.
4. Garantire il rispetto degli obblighi di conformità legale, statutaria e contrattuale.

# Aree di Controllo e Sicurezza Operativa

Per proteggere il proprio ecosistema digitale, Forma Farm adotta misure tecniche e organizzative specifiche, tra cui: Sicurezza dell'Infrastruttura Cloud: Utilizzo di infrastrutture cloud globali certificate (es. ambienti AWS gestiti da personale qualificato), protette da meccanismi di cifratura dei dati in transito (HTTPS) e a riposo. Controllo degli Accessi e IAM: Adozione del principio del minimo privilegio (least privilege), gestione sicura delle credenziali di autenticazione e tracciabilità degli accessi amministrativi alle piattaforme. Gestione delle Vulnerabilità e Patch Management: Monitoraggio costante della sicurezza del software, aggiornamento regolare dei sistemi operativi, dei componenti open source e dei plugin per prevenire vulnerabilità. Backup e Disaster Recovery: Esecuzione di copie di sicurezza periodiche dei dati e test di ripristino per garantire la continuità operativa in caso di incidenti. Gestione degli Incidenti (Incident Management): Adozione di procedure chiare per la rilevazione tempestiva, la segnalazione e la mitigazione di eventuali violazioni di sicurezza o anomalie tecniche.

# Violazioni della Policy

Il mancato rispetto delle disposizioni contenute nella presente Information Security Policy e nelle procedure operative ad essa collegate può comportare conseguenze disciplinari, oltre a eventuali responsabilità civili e penali previste dalle normative vigenti.

# Riesame e Aggiornamento

La presente Information Security Policy è soggetta a revisione almeno annuale da parte della Direzione, o in occasione di cambiamenti significativi dell'infrastruttura tecnologica, del business o del contesto normativo di riferimento, al fine di garantirne la costante idoneità ed efficacia nel tempo.

---

Data di approvazione: Ottobre 2026
Forma Farm S.r.l. – La Direzione

# POLITICHE SPECIFICHE DI DOMINIO

Le **Politiche Specifiche di Dominio** a supporto del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) per **Forma Farm S.r.l.** definiscono le regole operative e i comportamenti richiesti in aree specifiche dell'organizzazione.

# Controllo degli Accessi e IAM (Identity and Access Management)

- **Scopo:** Regolare le modalità di profilazione, autorizzazione e gestione delle credenziali per l'accesso ai sistemi aziendali e agli ambienti di produzione cloud.
- **Principi chiave:**
  - Adozione rigorosa del principio del *minimo privilegio* (*least privilege*) per tutti gli operatori e amministratori.
  - Obbligo di utilizzo di meccanismi di autenticazione forte (es. autenticazione a due fattori - MFA) per l'accesso agli ambienti cloud critici, ai server e ai pannelli di controllo della piattaforma LMS.
  - Revisione periodica dei permessi e immediata revoca delle credenziali in caso di cessazione del rapporto di lavoro o cambio di mansione.

# Utilizzo dei Dispositivi Mobili e dello Smart Working (Mobile

# Device & Teleworking Policy)

- **Scopo:** Regolamentare la sicurezza e la protezione delle informazioni aziendali al di fuori del perimetro fisico tradizionale della sede di Via Savona a Milano.
- **Principi chiave:**
  - Obbligo di protezione mediante password robuste, PIN o biometria e cifratura del disco per tutti i dispositivi (notebook, smartphone, tablet) utilizzati per accedere ai sistemi di Forma Farm.
  - Divieto di utilizzo di reti Wi-Fi pubbliche o non protette senza l'uso di una connessione sicura (VPN aziendale).
  - Obbligo di custodire i dispositivi con cura e di segnalare immediatamente eventuali smarrimenti o furti al team tecnico.

# Classificazione e Gestione delle Informazioni

- **Scopo:** Stabilire le regole per trattare, etichettare e proteggere i dati e gli asset aziendali (in particolare i dati dei clienti, i contenuti formativi e i codici sorgente dei plugin e di Forma Lms).
- **Principi chiave:**
  - Classificazione delle informazioni in base alla criticità e alla confidenzialità (es. Pubblico, Interno, Confidenziale, Strettamente Confidenziale/Dati Personali GDPR).
  - Regole per la gestione sicura, la conservazione e la distruzione o cancellazione sicura dei dati al termine del ciclo di vita o dei contratti di servizio (*Data Processing Agreement*).

# Clean Desk e Clean Screen

- **Scopo:** Garantire la protezione fisica delle informazioni sensibili e dei dati dei clienti sia all'interno degli uffici sia durante il lavoro da remoto, prevenendo accessi non autorizzati o la visualizzazione accidentale di dati critici.
- **Principi chiave:**
  - Obbligo di bloccare lo schermo (*screen lock*) ogni volta che si lascia incustodito il terminale di lavoro.
  - Rimozione e archiviazione sicura di documenti cartacei o supporti di memorizzazione rimovibili dalle scrivanie al termine dell'orario di lavoro o in caso di assenza prolungata.

# Sicurezza delle Password e Autenticazione

- **Scopo:** Definire standard robusti di accesso ai sistemi informatici per prevenire violazioni derivanti da credenziali deboli o compromesse.
- **Principi chiave:**
  - Requisiti minimi di complessità per le password (lunghezza minima, uso di caratteri misti, numeri e simboli) o adozione di password manager aziendali approvati.
  - Divieto assoluto di condivisione delle credenziali personali o di scrittura delle password su supporti cartacei non protetti.

# Sicurezza dello Sviluppo e delle Operazioni Cloud (Integrazione DevOps / Secure SDLC)

- **Scopo:** Assicurare che la piattaforma *Forma Cloud LMS* e i relativi plugin siano sviluppati, aggiornati e gestiti in sicurezza.
- **Principi chiave:**
  - Separazione rigorosa tra gli ambienti di sviluppo, test e produzione.
  - Gestione costante delle vulnerabilità e applicazione tempestiva degli aggiornamenti di sicurezza (*Patch Management*) sui componenti open source e sulle infrastrutture cloud.

# Ruoli e Responsabilità

# Ruoli e responsabilità del Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

## 1. Scopo

Il presente documento definisce i ruoli funzionali e i relativi ambiti di responsabilità nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Forma Farm Srl.

L'obiettivo è assicurare che le responsabilità e le autorità rilevanti per la gestione della sicurezza delle informazioni siano chiaramente identificate, assegnate e comunicate, in coerenza con i requisiti della norma ISO/IEC 27001:2022.

Il modello organizzativo è proporzionato alle dimensioni e alla struttura di Forma Farm, che opera attraverso i propri soci e una rete di collaboratori e professionisti esterni, senza personale dipendente.

## 2. Principi organizzativi

L'organizzazione del SGSI si basa sui seguenti principi:

- **Attribuzione chiara delle responsabilità:** ogni funzione rilevante per la sicurezza delle informazioni deve avere responsabilità e autorità definite.
- **Flessibilità organizzativa:** uno stesso soggetto può ricoprire più ruoli funzionali, compatibilmente con le competenze necessarie e con l'eventuale presenza di conflitti di

interesse.
- **Collaborazione tra soci e professionisti esterni:** le attività possono essere svolte da soci o collaboratori, nel rispetto degli incarichi, degli accordi contrattuali e delle autorizzazioni assegnate.
- **Separazione delle responsabilità:** ove necessario e proporzionato ai rischi, le funzioni di esecuzione, approvazione e verifica sono distinte. Quando la separazione non è concretamente possibile, sono previsti adeguati controlli compensativi.
- **Indipendenza delle verifiche:** le attività di audit interno sono organizzate in modo da garantire obiettività e imparzialità.

I ruoli descritti nel presente documento sono funzioni organizzative e non necessariamente posizioni lavorative o incarichi professionali autonomi.

# 3. Ruoli e responsabilità funzionali

La seguente tabella identifica i ruoli funzionali previsti nell'organizzazione del SGSI e ne descrive il rispettivo ambito di responsabilità.

| Codice | Ruolo | Ambito di responsabilità |
|---|---|---|
| DIR | Direzione / Amministratore | Indirizzo e supervisione del SGSI; approvazione delle politiche e degli obiettivi di sicurezza; assegnazione delle risorse; approvazione delle decisioni di competenza in materia di gestione dei rischi; riesame delle prestazioni del SGSI. |
| RSI | Responsabile del SGSI | Coordinamento e mantenimento del SGSI; supporto all'analisi e al trattamento dei rischi; gestione della documentazione; monitoraggio degli obiettivi e delle azioni di miglioramento; coordinamento delle attività di verifica e reporting alla Direzione. |
| TEC | Responsabile tecnico e infrastrutture | Gestione della sicurezza delle infrastrutture e degli ambienti tecnologici; configurazioni e aggiornamenti; gestione tecnica degli accessi; backup e ripristino; monitoraggio; gestione delle vulnerabilità e degli interventi tecnici di sicurezza. |

| Codice | Ruolo | Ambito di responsabilità |
|---|---|---|
| SWD | Responsabile sviluppo software | Sicurezza del processo di sviluppo; gestione del codice sorgente e dei repository; controllo delle modifiche; gestione delle dipendenze software; verifiche e test; sicurezza dei rilasci e manutenzione applicativa. |
| PRI | Referente privacy e protezione dei dati | Coordinamento degli aspetti relativi alla protezione dei dati personali; supporto nella gestione degli adempimenti privacy, delle richieste degli interessati e delle violazioni di dati personali, in coordinamento con la Direzione e con le funzioni coinvolte. |
| COM | Responsabile commerciale e marketing | Gestione sicura delle informazioni commerciali; protezione dei dati di clienti e prospect; utilizzo sicuro degli strumenti CRM e marketing; riservatezza delle offerte e dei contratti; condivisione autorizzata delle informazioni con clienti e soggetti esterni. |
| HD | Responsabile helpdesk e assistenza clienti | Gestione e classificazione delle richieste di assistenza; supporto agli utenti; gestione dei ticket; accesso alle informazioni e ai sistemi dei clienti secondo le autorizzazioni ricevute; documentazione degli interventi e segnalazione di anomalie e incidenti. |
| VER | Verificatore / auditor interno | Pianificazione ed esecuzione delle verifiche interne sul SGSI; valutazione della conformità e dell'efficacia dei controlli; documentazione dei risultati degli audit e verifica delle azioni correttive, assicurando obiettività e imparzialità. |

I ruoli possono essere ricoperti da più soggetti contemporaneamente. In particolare, le funzioni operative possono essere svolte da collaboratori esterni, mentre le responsabilità di coordinamento, supervisione e approvazione possono rimanere in capo ai soci o ad altri soggetti formalmente incaricati.

# 3.1 Collaboratori e fornitori esterni

Le attività affidate a collaboratori e fornitori esterni sono svolte nell'ambito degli incarichi e degli accordi contrattuali definiti con Forma Farm.

I collaboratori che partecipano alle attività del SGSI o che accedono a informazioni, sistemi e infrastrutture aziendali o dei clienti sono tenuti a:

- rispettare le politiche e le procedure di sicurezza applicabili;
- utilizzare esclusivamente gli accessi e le autorizzazioni assegnati;
- proteggere le informazioni e i dati trattati nello svolgimento delle attività;
- rispettare gli obblighi contrattuali di riservatezza e gli eventuali obblighi in materia di protezione dei dati personali;
- segnalare tempestivamente incidenti, anomalie o sospette violazioni della sicurezza.

La qualifica di socio o collaboratore non determina automaticamente l'attribuzione di specifiche responsabilità o autorizzazioni: queste sono definite in funzione dei ruoli effettivamente ricoperti e degli incarichi assegnati.

# 4. Assegnazione nominativa delle responsabilità

L'assegnazione dei ruoli funzionali ai singoli soggetti è documentata mediante una specifica matrice nominativa delle responsabilità RACI, riportata nel documento **«Matrice RACI – Assegnazione delle responsabilità SGSI»**.

La matrice associa le persone ai ruoli funzionali definiti nel presente documento, specificando per ciascun ruolo il livello di responsabilità attribuito:

- **A – Accountable:** responsabile ultimo del risultato e delle decisioni di propria competenza;
- **R – Responsible:** responsabile dell'esecuzione delle attività;
- **C – Consulted:** soggetto da consultare per competenze o contributi pertinenti;
- **I – Informed:** soggetto da informare sulle attività o decisioni rilevanti;
- **–:** nessuna responsabilità assegnata per il ruolo.

La matrice consente di rappresentare anche situazioni in cui uno stesso ruolo è ricoperto da più persone con livelli di responsabilità differenti, ad esempio quando un collaboratore svolge le attività operative e un socio mantiene la responsabilità ultima della funzione.

Per ciascun ruolo e per le responsabilità pertinenti deve essere identificato il soggetto dotato dell'autorità necessaria, evitando ambiguità nell'attribuzione delle decisioni.

# 5. Separazione dei compiti e controlli compensativi

Considerate le dimensioni dell'organizzazione e la possibilità che uno stesso soggetto ricopra più ruoli, Forma Farm valuta la separazione dei compiti in funzione della natura delle attività e dei rischi associati.

Particolare attenzione è riservata a:

- assegnazione e gestione delle autorizzazioni di accesso;
- attività tecniche con privilegi amministrativi;
- modifiche alle infrastrutture e agli ambienti di produzione;
- gestione degli incidenti di sicurezza;
- approvazione e verifica delle attività rilevanti;
- esecuzione degli audit interni.

Quando non è possibile realizzare una separazione diretta tra chi esegue e chi approva o verifica un'attività, possono essere adottati controlli compensativi, quali registrazione delle operazioni, revisione successiva, approvazione da parte della Direzione o verifica indipendente.

Le modalità di applicazione dei controlli sono definite nelle procedure operative pertinenti e documentate attraverso le relative evidenze.

# 6. Aggiornamento e riesame

Il presente documento e la relativa matrice RACI sono mantenuti aggiornati dal Responsabile del SGSI e sottoposti all'approvazione della Direzione.

Sono riesaminati in occasione di:

- variazioni nella composizione dei soci o dei collaboratori;
- assegnazione o cessazione di incarichi e responsabilità;
- modifiche significative all'organizzazione o ai servizi erogati;
- introduzione di nuove attività o sistemi che comportino responsabilità rilevanti per la sicurezza;
- riesame periodico del SGSI o rilevazione di criticità nell'attribuzione delle responsabilità.

Le modifiche alle assegnazioni nominative sono riportate nella matrice RACI, mentre il presente documento viene aggiornato quando cambiano i ruoli funzionali o i rispettivi ambiti di responsabilità.

# 7. Riferimenti

- ISO/IEC 27001:2022 – Clausola 5.3: Organizational roles, responsibilities and authorities.
- ISO/IEC 27001:2022 – Clausola 5.1: Leadership and commitment.
- ISO/IEC 27001:2022 – Clausola 7.2: Competence.
- ISO/IEC 27001:2022 – Clausola 7.3: Awareness.
- ISO/IEC 27001:2022 – Clausola 9.2: Internal audit.
- Matrice RACI – Assegnazione delle responsabilità SGSI.
- Politica per la sicurezza delle informazioni.
- Procedura di gestione degli accessi.
- Procedura di gestione degli incidenti di sicurezza.

# Assegnazione Ruoli e Responsabilità SGSI

Di seguito la versione aggiornata di GOV-03, con Giuseppe Nucifora aggiunto e Alessandro Vivona indicato come responsabile ultimo dello sviluppo software.

# GOV-03 – Matrice RACI: assegnazione delle responsabilità SGSI

## 1. Scopo

La presente matrice identifica l'assegnazione delle responsabilità relative ai ruoli funzionali del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di Forma Farm Srl.

La matrice integra il documento GOV-02 – Ruoli e responsabilità del SGSI, che descrive gli ambiti e le responsabilità associati a ciascun ruolo.

L'assegnazione è effettuata a livello di ruolo funzionale e non di singola attività. Le responsabilità operative di dettaglio possono essere ulteriormente specificate nelle procedure del SGSI.

## 2. Legenda

| Sigla | Significato | Descrizione |
|---|---|---|
| A | Accountable | Responsabile ultimo del ruolo e dei relativi risultati; assicura che le responsabilità siano presidiate e assume le decisioni di competenza. |

| | | |
|---|---|---|
| R | Responsible | Svolge operativamente le attività associate al ruolo. |
| C | Consulted | È consultato prima delle decisioni o delle attività rilevanti. |
| I | Informed | È informato sulle decisioni o sulle attività rilevanti. |
| – | Non assegnato | Non ha responsabilità attribuite per il ruolo. |

Una stessa persona può ricoprire più ruoli. Per ciascun ruolo deve essere chiaramente individuata la responsabilità ultima (A), ove applicabile. La stessa persona può ricoprire sia il ruolo A sia quello R (A/R).

# 3. Matrice persone / ruoli

| Persona | Qualifica | DIR | RSI | TEC | SWD | PRI | COM | HD |
|---|---|---|---|---|---|---|---|---|
| Alberto Pastorelli | Amministratore | A | A/R | – | – | A/R | – | A |
| Alessandro Affronto | Socio | – | – | A/R | – | – | – | – |
| Massimiliano Ferrari | Socio | – | – | – | – | – | A | – |
| Manuele Frau | Collaboratore – Marketing e Commerciale | – | – | – | – | – | R | – |
| Francesca Scalinci | Collaboratore – Marketing e Commerciale | – | – | – | – | – | R | – |
| Luisiana Garau | Collaboratore – Helpdesk | – | – | – | – | – | – | R |
| Alessandro Vivona | Collaboratore – Developer | – | – | – | A/R | – | – | – |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Marco Urzi | Collaboratore – Developer | – | – | – | R | – | – | – |
| Giuseppe Nucifora | Collaboratore – Developer | – | – | – | R | – | – | – |

# 4. Ruoli e responsabilità da completare

Il ruolo SWD – Responsabile sviluppo software è assegnato ad Alessandro Vivona come responsabile ultimo (A) e operativo (R).

Marco Urzi e Giuseppe Nucifora sono indicati come responsabili operativi (R) delle attività di sviluppo.

L'eventuale attribuzione di ulteriori responsabilità ai soci e ai collaboratori sarà formalizzata in occasione del successivo aggiornamento della matrice.

# 5. Audit interni

La funzione di verificatore / auditor interno (VER) non è prevista come ruolo funzionale permanente nella presente matrice.

Gli audit interni richiesti dal punto 9.2 della ISO/IEC 27001:2022 sono pianificati ed eseguiti da persone incaricate in funzione dell'audit specifico, garantendo obiettività e imparzialità.

La persona incaricata non deve verificare autonomamente attività o processi di cui è direttamente responsabile. Quando non sia possibile garantire adeguata indipendenza all'interno dell'organizzazione, Forma Farm può ricorrere a un auditor esterno.

# 6. Aggiornamento

La matrice è mantenuta aggiornata dal Responsabile del SGSI e sottoposta alla Direzione in occasione delle modifiche organizzative o del riesame del SGSI.

Deve essere aggiornata in caso di:

- ingresso o uscita di soci e collaboratori;
- modifica delle funzioni o delle responsabilità assegnate;
- attribuzione o cessazione di un ruolo funzionale;
- modifiche organizzative che incidano sulla gestione della sicurezza delle informazioni.