

Politica per la Sicurezza delle Informazioni

Rev.	Data	Descrizione	Autore
1.0	04/05/2026	Prima emissione pubblica	F. Greggio

LISTA DI DISTRIBUZIONE	
Sito Internet	offlineagency.it
Personale	Archivio condiviso aziendale
Clienti e terze parti	Su richiesta + sito web
Organismo di certificazione	ICIM S.p.a.

Emesso da	Approvato dalla Direzione	Approvato in data
F. Greggio	<ul style="list-style-type: none">- G. Fabbian- L. Fabbian- M.R. Moschitta	05/05/2026

1. Premessa

Offline Agency SRL è una società specializzata nello sviluppo software, nell'hosting e nella gestione di applicazioni web e mobile per clienti pubblici e privati. I nostri servizi comprendono la progettazione e lo sviluppo di applicazioni su misura, la gestione di infrastrutture cloud, la manutenzione evolutiva di piattaforme digitali e l'erogazione di servizi SaaS. Operiamo principalmente per enti pubblici (Comuni e Province, Autorità di sistema portuale, Università, etc.), aziende e organizzazioni che ci affidano lo sviluppo e la gestione dei propri sistemi informativi.



La natura della nostra attività ci porta a trattare quotidianamente informazioni di significativo valore: codice sorgente e segreti industriali dei clienti, dati personali degli utenti finali delle applicazioni da noi gestite, informazioni riservate di natura contrattuale e progettuale. In qualità di Responsabile del Trattamento (PII Processor) ai sensi del GDPR, Offline Agency tratta dati personali per conto dei propri clienti con la massima attenzione alla riservatezza e alla conformità normativa.

Per queste ragioni, la sicurezza delle informazioni non è per noi un adempimento formale, ma un valore fondamentale e un elemento distintivo del servizio che offriamo. Siamo convinti che la fiducia dei nostri clienti si costruisca ogni giorno attraverso comportamenti responsabili, misure tecniche adeguate e una governance documentata e verificabile.

2. Impegno della Direzione e obiettivi del SGSI

La Direzione di Offline Agency SRL ha deciso di istituire, implementare e mantenere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001:2022, con le estensioni ISO/IEC 27017:2015 per la sicurezza dei servizi cloud e ISO/IEC 27018:2025 per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici. Il sistema è integrato con il Sistema di Gestione per la Qualità ISO 9001:2015, nell'ambito di un approccio unitario e coerente alla gestione dell'organizzazione.

La certificazione ISO/IEC 27001:2022 con le estensioni cloud rappresenta per Offline Agency la dimostrazione concreta, verificata da un organismo terzo indipendente, del proprio impegno verso clienti, partner e collaboratori in materia di sicurezza delle informazioni.

Gli obiettivi che la Direzione si prefigge attraverso il SGSI sono:

- disporre di una visione complessiva e strutturata della sicurezza aziendale, che integri aspetti tecnologici, organizzativi e umani secondo un approccio olistico;
- proteggere le informazioni dei clienti, dei collaboratori e dell'organizzazione stessa dalle minacce interne ed esterne, attraverso un processo continuo di valutazione e trattamento del rischio;
- dimostrare la propria capacità di erogare servizi conformi ai requisiti dei clienti, agli standard internazionali, alle leggi e ai regolamenti applicabili;



- garantire la continuità dei servizi erogati, minimizzando l'impatto di eventi avversi sulle attività dei clienti;
- incrementare la soddisfazione dei clienti attraverso l'efficace applicazione del SGSI e il miglioramento continuo dei processi;
- promuovere una cultura della sicurezza diffusa, attraverso formazione periodica, simulazioni e sensibilizzazione continua di tutto il personale e dei collaboratori, nella consapevolezza che la protezione delle informazioni è responsabilità di ciascuno.

3. Dichiarazione di Politica per la Sicurezza delle Informazioni

Offline Agency ritiene che la sicurezza delle informazioni rappresenti un fattore critico di successo tanto per la qualità dei processi di progettazione e sviluppo di soluzioni tecnologiche quanto per l'affidabilità dell'erogazione dei servizi. Per le caratteristiche dei servizi cloud che offriamo e per il valore che le informazioni rivestono nel nostro business, la **Politica per la Sicurezza delle Informazioni costituisce un indirizzo strategico fondamentale e prioritario.**

Offline Agency impegna la propria organizzazione, e specificatamente tutte le persone che lavorano e collaborano con noi, a rispettare i seguenti principi fondamentali:

1. Riservatezza: per assicurare che le informazioni siano accessibili esclusivamente ai soggetti e ai processi debitamente autorizzati e che non vengano rese disponibili o divulgate a persone o entità non autorizzate. Ogni accesso alle informazioni è regolato dal principio del minimo privilegio e della necessità di sapere.

2. Integrità: per salvaguardare la completezza e la correttezza delle informazioni e garantire che non subiscano modifiche, cancellazioni o alterazioni non autorizzate, sia a seguito di azioni volontarie, sia a causa di malfunzionamenti o eventi accidentali.

3. Disponibilità: per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai sistemi quando ne fanno richiesta, garantendo la continuità operativa dei servizi erogati e salvaguardando il patrimonio informativo dei clienti.

4. Controllo: per assicurare che la gestione delle informazioni avvenga sempre attraverso processi documentati, strumenti sicuri e verificati, e che ogni accesso fisico o logico sia autorizzato, monitorato e tracciato.



5. Privacy e protezione dei dati personali: per garantire che il trattamento dei dati personali, sia nei casi in cui Offline Agency operi come Titolare, sia nei casi in cui operi come Responsabile del Trattamento per conto dei clienti, avvenga nel pieno rispetto del Regolamento (UE) 2016/679 (GDPR), della normativa nazionale applicabile e dei requisiti specifici della ISO/IEC 27018:2025.

6. Sicurezza cloud: per garantire che tutti i servizi cloud erogati e fruiti da Offline Agency siano gestiti in conformità alle responsabilità definite nel modello di responsabilità condivisa, in linea con i requisiti della ISO/IEC 27017:2015, e che gli ambienti dei diversi clienti siano rigorosamente segregati.

4. Il Sistema di Gestione per la Sicurezza delle Informazioni

Per dare attuazione alla presente Politica, Offline Agency SRL ha sviluppato e si impegna a mantenere e migliorare continuamente un SGSI conforme ai requisiti delle norme ISO/IEC 27001:2022, ISO/IEC 27017:2015 e ISO/IEC 27018:2025, certificate da un organismo di certificazione accreditato.

Nell'ambito della gestione dei servizi offerti, il SGSI di Offline Agency garantisce che:

- l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti periodicamente la loro criticità, al fine di implementare adeguati livelli di protezione proporzionati al valore e al rischio associato;
- l'accesso alle informazioni avvenga in modo sicuro, autorizzato e monitorato, con controlli tecnici e organizzativi adeguati;
- i servizi cloud siano erogati con architetture sicure e segregate, configurazioni baseline conformi agli standard CIS, Infrastructure as Code versionato e monitoraggio continuo degli ambienti;
- i dati personali dei clienti siano trattati esclusivamente su istruzione documentata del Titolare, per le finalità e nei limiti stabiliti contrattualmente, senza utilizzo per finalità proprie e con cancellazione sicura certificata al termine del rapporto;
- le terze parti e i fornitori critici siano selezionati sulla base di garanzie di sicurezza verificabili e contrattualizzati con obblighi equivalenti a quelli assunti da Offline Agency nei confronti dei propri clienti;



- il personale interno e i collaboratori siano adeguatamente formati, sensibilizzati e responsabilizzati sulle tematiche della sicurezza delle informazioni e della protezione dei dati personali;
- le anomalie, gli incidenti e le vulnerabilità siano tempestivamente rilevati e gestiti attraverso procedure formalizzate, con notifica al cliente entro 24 ore dalla scoperta di una violazione dei dati personali e supporto alla notifica al Garante Privacy entro 72 ore;
- la business continuity sia garantita attraverso policy di backup con test di ripristino documentati, architetture ad alta disponibilità e procedure di disaster recovery;
- la conformità con i requisiti di legge, gli standard internazionali e gli impegni contrattuali sia verificata periodicamente attraverso audit interni e riesami della Direzione;
- ogni non conformità identificata sia gestita attraverso azioni correttive documentate, in un processo di miglioramento continuo;
- l'evoluzione del quadro regolatorio europeo in materia di cybersecurity, in particolare la Direttiva NIS2 (UE 2022/2555) e il Cyber Resilience Act, sia monitorata con continuità al fine di recepire tempestivamente eventuali nuovi obblighi applicabili all'attività di Offline Agency.

La presente Politica si applica a tutto il personale dipendente e collaboratore, nonché a tutte le terze parti che, nell'ambito delle proprie attività, trattano informazioni rientranti nel campo di applicazione del SGSI di Offline Agency SRL.

5. Dichiarazione di Impegno

Offline Agency SRL si impegna formalmente a:

- garantire la riservatezza delle informazioni attraverso la definizione puntuale delle responsabilità interne, il controllo degli accessi fisici e logici esclusivamente da parte di personale autorizzato e la gestione sicura delle credenziali e delle identità digitali;
- garantire l'integrità delle informazioni attraverso il controllo degli accessi, la gestione dei backup, il versionamento del codice sorgente e delle configurazioni, e la tracciabilità di ogni modifica ai sistemi;
- garantire la disponibilità delle informazioni e la continuità dei servizi attraverso architetture ridondanti, politiche di backup testate e piani di ripristino verificati periodicamente;



- garantire la protezione dei dati personali dei clienti operando come Responsabile del Trattamento nel pieno rispetto del GDPR, trattando i dati esclusivamente su istruzione documentata del Titolare e garantendone la cancellazione sicura al termine del rapporto contrattuale;
- garantire la sicurezza degli ambienti cloud attraverso configurazioni hardened, segregazione tra ambienti di clienti diversi, monitoraggio continuo e gestione documentata delle vulnerabilità;
- garantire la formazione e la consapevolezza di tutto il personale e dei collaboratori sugli obblighi e sulle responsabilità in materia di sicurezza delle informazioni, e sulle conseguenze in caso di mancato rispetto della presente Politica;
- garantire il rispetto delle leggi e dei regolamenti in materia di sicurezza delle informazioni e protezione dei dati personali applicabili, degli standard internazionali di riferimento e degli impegni contrattuali assunti con i clienti;
- garantire il miglioramento continuo del SGSI attraverso la valutazione periodica del rischio, la gestione strutturata delle non conformità e il riesame annuale della Direzione.

I soggetti terzi che collaborano con Offline Agency e che nell'ambito di tale collaborazione accedono o trattano informazioni rientranti nel perimetro del SGSI sono obbligati ad accettare e rispettare i principi e gli impegni della presente Politica, formalizzando tale impegno attraverso accordi di riservatezza e contratti di servizio.

La presente Politica viene costantemente verificata e aggiornata, con un riesame formale almeno annuale, al fine di assicurarne il continuo allineamento con il contesto di rischio, le evoluzioni normative e gli obiettivi aziendali. E pubblicata sul sito istituzionale e condivisa con tutto il personale, i collaboratori, i clienti e le terze parti.

Ponte San Nicolò, 04/05/2026

