

## Politica per la Sicurezza delle Informazioni

### 1. Scopo e campo di applicazione

La presente Politica per la Sicurezza delle Informazioni definisce i principi, gli obiettivi e le responsabilità di WAIKA S.R.L. in materia di protezione delle informazioni, in conformità alla norma ISO/IEC 27001:2022. La politica si applica a tutto il personale dell'organizzazione (soci, dipendenti e collaboratori), a tutti i processi aziendali e a tutte le informazioni gestite, indipendentemente dal formato (digitale o cartaceo) e dal supporto di memorizzazione.

### 2. Contesto dell'organizzazione

WAIKA S.R.L. opera nel settore della comunicazione, del web marketing e della consulenza digitale. Nell'ambito delle proprie attività, l'azienda gestisce informazioni riservate dei clienti (strategie di marketing, dati di accesso a piattaforme, contenuti creativi, dati analitici) e informazioni aziendali proprie (know-how, tool proprietari, dati amministrativi e contabili). La protezione di queste informazioni è essenziale per la continuità operativa, la reputazione aziendale e la conformità normativa.

### 3. Principi fondamentali

#### 3.1 Riservatezza, Integrità e Disponibilità

WAIKA S.R.L. si impegna a garantire la protezione delle informazioni secondo i tre principi fondamentali della sicurezza delle informazioni:

- **Riservatezza:** le informazioni sono accessibili solo alle persone autorizzate, attraverso un sistema di controllo degli accessi basato su ruoli e livelli differenziati, gestito tramite tool interni proprietari.
- **Integrità:** le informazioni sono accurate e complete, protette da modifiche non autorizzate attraverso controlli tecnici (FileVault, backup RAID 1, ambienti separati sviluppo/produzione) e organizzativi.
- **Disponibilità:** le informazioni e i sistemi sono accessibili quando necessario, garantiti da sistemi di backup multipli (Time Machine, NAS RAID 1, cloud), UPS e procedure di ripristino documentate.

#### 3.2 Approccio basato sul rischio

L'organizzazione adotta un approccio sistematico alla gestione dei rischi per la sicurezza delle informazioni, attraverso l'identificazione, la valutazione e il trattamento dei rischi in modo proporzionato alla natura e alla dimensione dell'attività. L'Analisi dei Rischi viene aggiornata almeno annualmente e in occasione di cambiamenti significativi.

#### 3.3 Protezione delle infrastrutture IT

L'infrastruttura IT è protetta mediante misure tecniche e organizzative adeguate, tra cui sistemi di cifratura, controllo degli accessi, protezione della rete, sistemi di backup e procedure di aggiornamento e monitoraggio della sicurezza.

#### 3.4 Coinvolgimento del personale

Tutto il personale è responsabile della corretta gestione e protezione delle informazioni trattate nell'ambito delle proprie attività, nel rispetto delle politiche e delle procedure del SGSI. L'organizzazione garantisce la formazione e la sensibilizzazione continua del personale attraverso corsi periodici (aggiornamento GDPR, formazione periodica sulla sicurezza informatica) e la diffusione delle politiche e delle procedure di sicurezza.

#### 3.5 Gestione degli accessi e delle credenziali

L'accesso alle informazioni e ai sistemi è regolamentato attraverso: un software proprietario per la gestione centralizzata delle password con livelli di accesso differenziati; autenticazione a due fattori (2FA/MFA) attiva su tutti i servizi che lo permettono; cambio password programmato ogni 3 mesi; cambio immediato di tutte le password entro 48 ore dall'uscita di un collaboratore; un solo utente amministratore per postazione.

#### 4. Obiettivi di sicurezza delle informazioni

Obiettivo	Indicatore	Target
Zero incidenti di sicurezza gravi	Numero incidenti gravi/anno	0
Formazione del personale	Ore formazione sicurezza/anno	≥ 8 ore/persona
Aggiornamento sistemi	Tempo medio applicazione patch critiche	≤ 7 giorni
Disponibilità dei servizi	Uptime servizi critici	≥ 99%
Backup verificati	Test di ripristino effettuati/anno	≥ 2
Conformità normativa	Non conformità audit esterno	0 maggiori
Cambio password	Rispetto scadenza trimestrale	100%

#### 5. Continuità operativa

WAIKA S.R.L. garantisce la continuità operativa attraverso: backup multipli per ogni cliente (cloud + NAS locali in RAID 1); backup giornaliero della posta elettronica su server cloud; backup giornaliero e settimanale del PC Amministrazione su supporti esterni; Time Machine attive su tutte le postazioni Mac; sistemi UPS per la protezione dall'interruzione dell'alimentazione elettrica; procedure di ripristino documentate e testate.

#### 6. Gestione dei fornitori

I fornitori critici di servizi IT e cloud sono selezionati e monitorati secondo le procedure aziendali di gestione dei fornitori, con verifica periodica dei requisiti di sicurezza, delle certificazioni e dei livelli di servizio.

#### 7. Gestione degli incidenti

L'organizzazione dispone di una procedura per la segnalazione, la classificazione e la gestione degli incidenti di sicurezza delle informazioni. Il personale è tenuto a segnalare tempestivamente qualsiasi evento sospetto al RSGSI. Il supporto tecnico specialistico per la gestione degli incidenti è fornito da Nicola Cirillo (Cyber Forensics Associate CFA - EC-Council).

#### 8. Ruoli e responsabilità

Ruolo	Responsabilità principali
Direzione	Approvazione politica, risorse, riesame della direzione
RSGSI	Gestione operativa del SGSI, coordinamento attività.
Supporto tecnico IT & Sicurezza delle Informazioni	Consulenza e supervisione infrastrutture e fornitura di threat intelligence
Gestione Operativa IT (GOIT)	Implementazione e gestione dei controlli tecnici sull'infrastruttura IT, gestione degli aggiornamenti di sicurezza e manutenzione operativa dei sistemi.
Responsabile Amministrativo	Gestione fornitori critici e supervisione aspetti amministrativi
Addetto Amministrativo	Gestione fornitori, licenze, aspetti amministrativi
Responsabile Privacy	Conformità GDPR, protezione dati personali
Tutto il personale	Rispetto politiche e procedure, ed eventuale segnalazione incidenti.

#### 9. Conformità normativa

WAIKA S.R.L. si impegna a rispettare tutti i requisiti legali, regolamentari e contrattuali applicabili alla sicurezza delle informazioni, inclusi il Regolamento UE 2016/679 (GDPR), la normativa nazionale in materia di protezione dei dati personali e gli obblighi contrattuali verso clienti e fornitori.

## **10. Miglioramento continuo**

Il SGSI è soggetto a miglioramento continuo attraverso: il riesame periodico della direzione; gli audit interni condotti con il supporto di Nicola Cirillo; l'analisi degli indicatori di performance; la gestione delle non conformità e delle azioni correttive; l'aggiornamento dell'analisi dei rischi; la formazione continua del personale.

## **11. Comunicazione e diffusione**

La presente politica è comunicata a tutto il personale dell'organizzazione e resa disponibile alle parti interessate pertinenti. Il personale è tenuto a prenderne visione e ad applicarne i contenuti nell'ambito delle proprie attività. La politica è riesaminata almeno annualmente dalla Direzione e aggiornata in caso di cambiamenti significativi.