Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P08

VERSIONE 2.0 · DICEMBRE 2026

# Politica di logging e monitoraggio

Che cosa si registra, per quanto tempo, come si protegge, chi lo guarda e quando suona un allarme. Senza mai scrivere nei log il testo dei documenti dei Clienti.

| CODICE | TITOLARE | REVISIONE | STATO |
| --- | --- | --- | --- |
| P08 · POL-08 | Responsabile della sicurezza | Annuale | al 01/12/2026 |

POLITICA P08 · POL-08

# Politica di logging e monitoraggio

Che cosa si registra, per quanto tempo, come si protegge, chi lo guarda e quando suona un allarme.

| CODICE | TITOLARE | APPROVATA DA | VERSIONE |
|---|---|---|---|
| P08 (POL-08) | Responsabile della sicurezza | Organo amministrativo, [data della delibera] | 2.0 del 01/12/2026 |

| REVISIONE | DESTINATARI | CLASSIFICAZIONE |
|---|---|---|
| annuale | personale tecnico; amministratori degli studi; uffici ICT risk e audit dei Clienti | Riservato · per il Cliente |

DOCUMENTI COLLEGATI

P03, P12, P16; procedura 25 (Risposta agli incidenti); documento 11 (Continuità operativa, ripristino e incidenti); documento 55 (Accordo sul livello di servizio)

AMBITO

Log applicativi, di accesso, di sicurezza e di amministrazione della piattaforma; registri consultabili dagli studi; monitoraggio della disponibilità e degli allarmi.

| ISO/IEC 27001:2022, ALLEGATO A | NORME PRINCIPALI |
|---|---|
| 8.15, 8.16, 8.17 | DORA art. 10; Reg. del. (UE) 2024/1774 art. 12; GDPR art. 32 |

## 1 Scopo e ruoli

I log servono a rilevare le anomalie, a ricostruire un incidente e a dimostrare chi ha fatto che cosa. Il Responsabile della sicurezza decide che cosa si registra, ne protegge l'integrità, riceve gli allarmi ed esamina gli eventi di sicurezza; l'amministratore dello studio consulta ed esporta i registri dello studio.

## 2 Che cosa si registra e per quanto

| REGISTRO | CONTENUTO | CONSERVAZIONE |
|---|---|---|
| Accessi HTTP | richieste al proxy: ora, indirizzo, metodo, percorso, esito, durata; mai corpo delle richieste né token | 90 giorni, CloudWatch Logs |
| Applicativi | moduli, identificativi, nomi di file, errori; mai testo dei documenti | 90 giorni, CloudWatch Logs |
| Sicurezza e amministrazione | CloudTrail in tutte le regioni con convalida dell'integrità; sessioni SSM sulla macchina; accessi al backoffice; risultati di GuardDuty | 12 mesi |
| Attività dello studio | chi, che cosa, quando, su quale cliente o atto | per la durata del contratto; esportabile dall'amministratore dello studio |
| Accessi ai fascicoli penali | consultazioni (una all'ora per utente), domande, analisi, confronti fra depositi, timeline, grafi e schede dell'imputato generati | per la durata del contratto; esportabile dal Titolare |
| Accessi del personale al contenuto | richiedente, motivo, pratica, inizio e fine (politica P03) | per la durata del contratto; estratto al Cliente su richiesta |
| Costi | modello, agente, token, importo; mai il testo | per la fatturazione; scollegati dai contenuti alla cancellazione |

## 3 Regole sul contenuto

3.1 I log non contengono testo dei documenti, corpo delle richieste, token, password o segreti. Un messaggio di log nuovo che potrebbe contenerli non supera la revisione del codice (politica P06).

3.2 I registri consultabili dagli studi seguono la stessa visibilità dei dati a cui si riferiscono e si cancellano con lo studio alla cessazione (politica P12).

3.3 Gli orologi sono sincronizzati con Amazon Time Sync Service (chrony, predefinito di Amazon Linux 2023), così gli eventi di sistemi diversi si confrontano sullo stesso tempo.

## 4 Protezione

I log di sicurezza e amministrazione si conservano con la convalida dell'integrità di CloudTrail e con accesso limitato al Responsabile della sicurezza; ogni modifica o cancellazione di un gruppo di log o di una traccia resta registrata in CloudTrail.

## 5 Monitoraggio e allarmi

5.1 Una sonda esterna controlla ogni minuto `https://app.trailgun.ai/api/health` e l'avvio di una lavorazione: è la misura della disponibilità dell'accordo sul livello di servizio (documento 55).

5.2 Allarmi 24/7 su salute dell'app, spazio disco, CPU, memoria, errori 5xx e scadenza dei certificati; GuardDuty segnala attività sospette sull'account.

5.3 Un allarme raggiunge il reperibile per telefono ed email; ogni allarme si valuta come possibile incidente secondo la procedura 25 e si annota con l'esito.

5.4 Gli eventi di sicurezza (GuardDuty, accessi amministrativi, uso dell'utente root) si esaminano a ogni allarme e, in blocco, a ogni revisione trimestrale degli accessi (procedura 22).

5.5 La pagina «Sistema» del backoffice mostra versione, dimensioni dei database, stato delle migrazioni e spazio disco.

5.6 La scrittura del registro degli accessi penali non blocca mai il lavoro dell'avvocato: se fallisce, l'errore va nei log applicativi e si esamina con gli altri errori.

## 6 Evidenze e registri

| CONTROLLO | EVIDENZA | DOVE E QUANDO |
|---|---|---|
| Log di accesso e applicativi | IN ESSERE gruppi di log con conservazione di 90 giorni | CloudWatch Logs, eu-central-1 |
| CloudTrail, GuardDuty, sessioni SSM | IN ESSERE traccia multi-regione con convalida dell'integrità, 12 mesi | account AWS di Trailgun |
| Sonda e allarmi | IN ESSERE sonda ogni minuto; allarmi su salute, disco, CPU, memoria, 5xx, certificati | prova di un allarme a ogni riesame annuale |
| Registri per lo studio | IN ESSERE attività e accessi penali, esportabili | dall'app, per la durata del contratto |

## 7 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione ammette testo dei documenti nei log. Riferimenti: DORA art. 10; Reg. del. (UE) 2024/1774 art. 12; GDPR art. 32; ISO/IEC 27001:2022 controlli 8.15, 8.16, 8.17.