Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 22



VERSIONE 2.0 · DICEMBRE 2026

Procedura di revisione degli accessi

Come Trailgun rivede ogni tre mesi chi può entrare nei sistemi che reggono il servizio: AWS, GitHub, backoffice, Google Workspace, console dei fornitori e account di servizio. E come lo studio rivede i propri utenti dall'Organizzazione.

CADENZA	AMBITO	ESITO	STUDIO
trimestrale	accessi privilegiati e di servizio	modello 44, firmato	utenti e ruoli dall'Organizzazione

PROCEDURA 22 · PROC-22

Revisione degli accessi

Un accesso resta solo se c'è una persona, un ruolo e un motivo. La revisione lo controlla per ogni sistema, ogni trimestre, e lo mette per iscritto.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-22	Responsabile della sicurezza (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale	Responsabile della sicurezza, organo amministrativo; ICT risk e audit dei Clienti; amministratori degli studi

DOCUMENTI COLLEGATI

politica P03; documento 21, Ingresso e uscita del personale; documento 23, Chiavi e segreti; documento 44, Revisione degli accessi (modello); documento 42, Inventario degli asset; documento 05, Sicurezza delle informazioni

1 Scopo e ambito

1.1 La revisione accerta che ogni accesso privilegiato e ogni account di servizio ai sistemi di Trailgun corrisponda a una persona o a un servizio identificati, a un ruolo attuale e al minimo necessario, con l'autenticazione a più fattori dove c'è una persona.

1.2 Si svolge ogni trimestre. La prima revisione è verbalizzata sul modello 44 il [data]. Si ripete in più dopo un incidente che coinvolge credenziali, dopo un cambiamento significativo dei sistemi di accesso e a ogni uscita di una persona con accessi privilegiati, limitatamente ai suoi.

1.3 Gli utenti degli studi non sono nell'ambito: li gestisce e li rivede lo studio (paragrafo 6).

2 Ruoli

- **Responsabile della sicurezza**: estrae gli elenchi, li confronta con l'elenco degli accessi autorizzati, esegue le correzioni, compila il modello 44.
- **Organo amministrativo**: riceve il modello compilato, ne prende atto e lo controfirma; poiché il Responsabile della sicurezza rivede anche i propri accessi, la controfirma è il controllo indipendente.

3 Che cosa si rivede

SISTEMA	CHE COSA SI CONTROLLA	DA DOVE SI PRENDE L'ELENCO
AWS	utenti e gruppi di IAM Identity Center e i loro insiemi di permessi per ambiente; utente root con MFA e senza chiavi, non usato; assenza di utenti IAM con chiavi statiche; ruoli dell'integrazione continua, uno per ambiente e solo per il suo branch; ruolo dell'istanza; profilo della prova di ripristino	console di IAM Identity Center e di IAM; rapporto delle credenziali; CloudTrail per l'ultimo uso
GitHub	membri e proprietari dell'organizzazione, 2FA obbligatoria, collaboratori esterni, chiavi di deploy, app autorizzate, segreti delle azioni, regole di protezione dei branch di ambiente	impostazioni dell'organizzazione e del repository; registro di audit
Backoffice della piattaforma	membri dei gruppi Cognito `admin` (amministrazione della piattaforma) e `supporto` (solo ticket e knowledge base)	gruppi del pool degli utenti di production
Google Workspace	account e amministratori; caselle condivise `security@` e `privacy@` e chi le legge; 2FA obbligatoria; deleghe e inoltri	console di amministrazione
Console dei fornitori	utenti con accesso a posta transazionale, firma e visure, banca dati giuridica, notifiche, pagamenti e, per gli studi che lo accendono, riconoscimento del testo di riserva; MFA attiva	pannelli utenti di ciascun fornitore del registro 15
Account di servizio	chiavi e credenziali usate dall'app verso i fornitori: titolare, scopo, ambito minimo, data dell'ultima rotazione (documento 23)	inventario dei segreti, per nome
Accessi al contenuto	registro degli accessi del personale al contenuto delle pratiche: ogni accesso corrisponde a una richiesta del Cliente o a un incidente	registro degli accessi del personale

4 Passi

1 **Elenchi.** Nella prima settimana del trimestre si estraggono gli elenchi aggiornati di ogni sistema della tabella 3 e si conservano con la data.

1 **Confronto.** Ogni voce si confronta con l'elenco degli accessi autorizzati (documento 21): chi è, quale ruolo, quale motivo. Per ogni voce si verifica che l'identità sia nominativa e unica, che l'autenticazione a più fattori sia attiva, che il privilegio sia il minimo per il ruolo e l'ambiente, che l'account sia stato usato dopo la revisione precedente.

1 **Esito** per ogni voce: confermato, ridotto o revocato. Un account non riconducibile a una persona o a un servizio si revoca subito; un account inutilizzato dalla revisione precedente si revoca, salvo un motivo scritto.

1 **Correzioni.** Le revoche si fanno nello stesso giorno. Una correzione che richiede un cambiamento (per esempio un ruolo da ridisegnare) si apre come cambiamento (documento 20) con titolare e data, scritti nel modello.

1 **Accessi al contenuto.** Si rilegge il registro degli accessi del personale al contenuto delle pratiche del trimestre; un accesso senza richiesta del Cliente o senza incidente è un evento di sicurezza e segue il documento 25.

1 **Verbale.** Il modello 44 compilato, con le estrazioni allegate, va all'organo amministrativo, che lo controfirma. Gli esiti entrano nel rapporto ai Clienti che lo chiedono.

5 Regole che la revisione fa rispettare

- Accessi personali: nessun account condiviso fra persone; le caselle condivise si leggono con account personali.
- Autenticazione a più fattori obbligatoria su AWS (root e console), GitHub, Google Workspace, Stripe, Resend e su ogni console di fornitore; per gli utenti degli studi l'app di autenticazione (TOTP) è obbligatoria per tutti.
- Credenziali amministrative AWS solo temporanee, da IAM Identity Center; nessuna chiave statica.
- Privilegi per ambiente: un accesso a development o staging non apre production; l'integrazione continua tocca solo il proprio ambiente.
- Il personale di Trailgun accede al contenuto delle pratiche solo su richiesta del Cliente o per un incidente, e ogni accesso si registra; il backoffice mostra agli amministratori della piattaforma i metadati degli studi, non il contenuto delle pratiche.

6 Gli utenti dello studio

6.1 Lo studio gestisce i propri utenti dall'Organizzazione (Organizzazione → Utenti): inviti, ruoli `admin`, `membro`, `operator` (porta avanti le pratiche, non ne crea) e `viewer` (sola lettura), permessi concessi per membro (richiesta di attenzione, Amministrazione), visibilità dei clienti (dello studio, privati, selezionati), chiavi API e caselle email.

6.2 Trailgun raccomanda allo studio la stessa cadenza trimestrale. L'amministratore dello studio dispone del registro delle attività dello studio (chi, che cosa, quando, su quale cliente o pratica), consultabile ed esportabile, e per i fascicoli penali del registro degli accessi.

6.3 Un utente disattivato non può più entrare: il blocco dei nuovi accessi è immediato e una sessione già aperta dura fino alla scadenza del token d'identità, a scadenza breve. Una chiave API revocata smette subito di funzionare.

7 Evidenze e registri

- Modelli 44 compilati e controfirmati, con le estrazioni datate di ogni sistema.
- Elenco degli accessi autorizzati (documento 21) e registro degli accessi del personale al contenuto delle pratiche.
- CloudTrail (12 mesi, con convalida dell'integrità), registro di audit di GitHub, registro delle attività di Google Workspace.

8 Riferimenti

DORA, art. 9, par. 4, lett. c) e d); Reg. del. (UE) 2024/1774, artt. 19-21; GDPR, art. 32, par. 1, lett. b), e par. 4; ISO/IEC 27001:2022, controlli 5.15 (controllo degli accessi), 5.16 (gestione delle identità), 5.17 (informazioni di autenticazione), 5.18 (diritti di accesso) e 8.2 (diritti di accesso privilegiato).

Trailgun

On target.

In a flash.

Dai documenti al lavoro finito: agenti AI per pratiche legali e finanziarie.

SICUREZZA E INCIDENTI, 24/7
security@trailgun.ai

REPERIBILITÀ PRIORITÀ 1
[+39 ...]

PRIVACY E DPO
privacy@trailgun.ai

Procedura 22 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P03 (controllo degli accessi). Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.