Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO P03



VERSIONE 2.0 · DICEMBRE 2026

Politica di controllo degli accessi

Chi può accedere a che cosa, come si autentica, come si concedono, rivedono e revocano gli accessi: per gli utenti degli studi, per il personale di Trailgun e per i servizi.

CODICE	TITOLARE	REVISIONE	STATO
P03 · POL-03	Responsabile della sicurezza	Annuale · accessi ogni trimestre	al 01/12/2026

POLITICA P03 · POL-03

Politica di controllo degli accessi

Chi accede a che cosa e come: utenti degli studi, personale di Trailgun, servizi e integrazione continua.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
P03 (POL-03)	Responsabile della sicurezza	Organo amministrativo, [data della delibera]	2.0 del 01/12/2026

REVISIONE	DESTINATARI	CLASSIFICAZIONE
annuale; accessi privilegiati ogni trimestre	personale e collaboratori; amministratori degli studi; uffici ICT risk e audit dei Clienti	Riservato · per il Cliente

DOCUMENTI COLLEGATI

P01, P04, P13; procedure 21 (Ingresso e uscita del personale), 22 (Revisione degli accessi), 23 (Gestione delle chiavi e dei segreti); modello 44 (Revisione degli accessi)

AMBITO

Gli accessi all'app, al backoffice, all'API pubblica e alle caselle email d'ingresso; gli accessi all'account AWS, a GitHub, a Google Workspace e alle console dei fornitori; i ruoli dei servizi e della CI.

ISO/IEC 27001:2022, ALLEGATO A	NORME PRINCIPALI
5.15-5.18, 7.2, 8.2-8.5	DORA art. 9(4)(c)-(d); Reg. del. (UE) 2024/1774 artt. 19-21; GDPR art. 32

1 Scopo e principi

Un accesso si concede solo se serve al compito, al livello minimo, a un'identità personale riconducibile a una persona, con autenticazione a più fattori. Le regole le applica il server: l'interfaccia nasconde ciò che un ruolo non può fare, ma il controllo è sempre lato server, a ogni richiesta.

2 Ruoli

2.1 **Responsabile della sicurezza.** Concede, rivede e revoca gli accessi del personale, dei servizi e dei fornitori; tiene il registro degli accessi del personale al contenuto e il modello 44.

2.2 **Amministratore dello studio.** Concede, rivede e revoca gli accessi dei propri utenti dall'Organizzazione, ne sceglie il ruolo e configura la visibilità dei clienti dello studio.

3 Utenti degli studi

3.1 **Ingresso solo su invito** dell'amministratore dello studio o della piattaforma: non esiste registrazione libera. Il pool Amazon Cognito consente la creazione degli utenti solo agli amministratori.

3.2 **Autenticazione forte.** Protocollo SRP (la password non transita né si conserva presso Trailgun); password di almeno 10 caratteri con maiuscole, minuscole e cifre; password temporanea valida 7 giorni; messaggi che non rivelano l'esistenza di un utente; autenticazione a più fattori con app TOTP obbligatoria per tutti gli utenti.

3.3 **Verifica a ogni richiesta.** Ogni chiamata a `/api/*` verifica il token d'identità (firma sulle chiavi del pool, scadenza, destinatario) e confronta l'utente della richiesta con quello del token.

3.4 **Ruoli dello studio. admin** (vede l'Organizzazione), **membro**, **operator** (porta avanti le pratiche esistenti, non ne crea di nuove) e **viewer** (sola lettura: nessuna scrittura, niente assistente, niente esportazione in Word). Le regole dei ruoli stretti stanno in un solo punto del codice e valgono per ogni richiesta. Permessi aggiuntivi per singolo membro: richiesta di attenzione e Amministrazione.

3.5 **Visibilità per cliente.** Ogni cliente dello studio è visibile a tutto lo studio, solo a chi l'ha creato o a persone selezionate. Un unico predicato decide la visibilità di ogni dato di un cliente, coperto da test sull'isolamento fra studi.

3.6 **Chiavi API dello studio.** Agiscono per conto di un utente; se ne conservano solo l'hash SHA-256 e il prefisso; limite di 120 richieste al minuto per chiave; revoca immediata dall'Organizzazione; rotazione consigliata ogni 12 mesi, a cura dello studio.

3.7 **Caselle email d'ingresso.** Ogni casella ha un token; le mail da mittenti non riconosciuti restano trattenute finché un utente non le approva; le mail di operatori e viewer non aprono pratiche.

3.8 **Sessione e disattivazione.** Il token d'identità ha una scadenza breve, [1 ora]. La disattivazione di un utente blocca subito i nuovi accessi; una sessione già aperta termina alla scadenza del token.

4 Personale di Trailgun

4.1 **Backoffice.** Protetto dal login Cognito con autenticazione a più fattori e dall'appartenenza al gruppo `admin`. L'amministratore della piattaforma vede studi, utenti, impostazioni, prompt e i metadati di pratiche e costi (titoli, stati, importi), mai il contenuto delle pratiche: il predicato di visibilità vale anche per lui.

4.2 **Assistenza.** Il gruppo `supporto` vede solo i ticket e la knowledge base.

4.3 **Accesso al contenuto.** Il personale accede al contenuto di una pratica solo su richiesta del Cliente o per gestire un incidente. Ogni accesso si annota nel registro degli accessi del personale con richiedente, motivo, dati consultati, inizio e fine; il Cliente interessato ne riceve l'estratto su richiesta.

4.4 **Infrastruttura.** L'accesso alla macchina e ai dati del volume è riservato a chi ne ha bisogno per gestire la piattaforma, con credenziali temporanee e sessioni registrate (§ 5); l'elenco nominativo è nel modello 44 e si rivede ogni trimestre.

5 Accessi privilegiati e autenticazione forte

5.1 Autenticazione a più fattori obbligatoria su AWS (utente root e console), GitHub (obbligo a livello di organizzazione), Google Workspace, Stripe, Resend e ogni console di fornitore.

5.2 Agli accessi amministrativi ad AWS si accede solo con credenziali temporanee di AWS IAM Identity Center, legate alla persona: nessuna chiave d'accesso statica.

5.3 L'utente root dell'account AWS non si usa per l'operatività: credenziali e dispositivo MFA sono custoditi come accesso di emergenza, il cui uso si registra (CloudTrail) e si comunica all'organo amministrativo.

5.4 Nessun accesso SSH: l'istanza non ha la porta 22 aperta e si amministra con AWS Systems Manager; ogni sessione si registra e si conserva 12 mesi (politica P08).

6 Servizi e integrazione continua

6.1 L'istanza ha un ruolo a privilegi limitati: lettura delle immagini, scrittura dei log, bucket temporaneo, Textract e Transcribe, modelli su Bedrock nelle sole regioni UE, parametri del proprio prefisso, gestione degli utenti del proprio pool.

6.2 GitHub Actions non ha chiavi AWS: ogni ambiente ha un ruolo OIDC assumibile solo dal branch omonimo, limitato al proprio ambiente; l'infrastruttura non si modifica dalla CI.

6.3 I segreti dei fornitori stanno in SSM Parameter Store cifrato, mai nel codice o nell'immagine; si ruotano ogni 12 mesi e subito dopo un sospetto di compromissione o l'uscita di una persona che vi aveva accesso (procedura 23).

7 Ciclo di vita degli accessi

1 **Richiesta.** Chi ha bisogno di un accesso lo chiede al Responsabile della sicurezza con il motivo e il livello; per l'ingresso di una persona vale la procedura 21.

2 **Condizioni.** Impegno di riservatezza, designazione al trattamento, verifica dei precedenti per chi accede alla produzione, formazione all'ingresso (politica P13).

3 **Concessione.** Identità personale, livello minimo, autenticazione a più fattori attiva prima del primo uso; l'accesso si annota con data e approvatore.

4 **Cambio di ruolo.** Gli accessi del ruolo precedente si revocano nello stesso giorno in cui si concedono i nuovi.

5 **Revisione trimestrale.** Accessi privilegiati (AWS, GitHub, backoffice, gruppi Cognito `admin` e `supporto`, Google Workspace, console dei fornitori) e account di servizio, secondo la procedura 22; esito e correzioni nel modello 44; ogni accesso non più giustificato si revoca.

6 **Uscita.** Revoca di tutti gli accessi entro 24 ore dalla cessazione del rapporto, rotazione dei segreti a cui la persona aveva accesso, verbale (procedura 21).

8 Accesso fisico

Trailgun non ha sale server: i sistemi sono nei data center di Amazon Web Services, la cui sicurezza fisica è attestata nei rapporti ISO/IEC 27001 e SOC 2 di AWS, disponibili su richiesta tramite AWS Artifact. I dispositivi del personale seguono la politica P14.

9 Evidenze e registri

CONTROLLO	EVIDENZA	DOVE E QUANDO
MFA per gli utenti	IN ESSERE TOTP obbligatorio nel pool di production	configurazione del pool

CONTROLLO	EVIDENZA	DOVE E QUANDO
Verifica del token, ruoli, visibilità, chiavi API	IN ESSERE applicati lato server, con test automatici	a ogni verifica della CI
MFA e credenziali temporanee per il personale	IN ESSERE IAM Identity Center; MFA su tutte le console; 2FA obbligatoria su GitHub	modello 44
Sessioni sulla macchina	IN ESSERE sessioni SSM registrate	12 mesi (P08)
Registro degli accessi del personale	IN ESSERE ogni accesso al contenuto con motivo e durata	a ogni accesso; estratto al Cliente su richiesta
Revisione degli accessi	IN ESSERE trimestrale, prima revisione verbalizzata il [data]	modello 44, ogni trimestre

10 Eccezioni e riferimenti normativi

Eccezioni secondo P01 § 8; nessuna eccezione all'autenticazione a più fattori sugli accessi privilegiati. Riferimenti: DORA art. 9, par. 4, lett. c) e d); Reg. del. (UE) 2024/1774 artt. 19-21 (identità unica e autenticazione forte del personale del fornitore); GDPR art. 32; ISO/IEC 27001:2022 controlli 5.15-5.18, 7.2, 8.2-8.5.