Trailgun

PACCHETTO DI CONFORMITÀ · DOCUMENTO 21

VERSIONE 2.0 · DICEMBRE 2026

Procedura di ingresso e uscita del personale

Che cosa succede prima che una persona tocchi un sistema di Trailgun, quando cambia ruolo e quando se ne va: riservatezza e designazione, verifica dei precedenti, formazione, accessi personali e minimi, revoca, rotazione dei segreti e verbale.

PRIMA DELL'ACCESSO	PRODUZIONE	REVOCA ALL'USCITA	SEGRETI
riservatezza, designazione, formazione	verifica dei precedenti	entro 24 ore	ruotati all'uscita

PROCEDURA 21 · PROC-21

Ingresso e uscita del personale

Nessuno accede a un sistema o a un dato di Trailgun o dei Clienti prima di aver firmato, essere stato designato e formato; nessuno conserva un accesso dopo l'uscita.

CODICE	TITOLARE	APPROVATA DA	VERSIONE
PROC-21	Legale rappresentante (Franco Puppo, CEO)	Organo amministrativo, [data della delibera]	2.0 · stato al 01/12/2026

REVISIONE	DESTINATARI
annuale	dipendenti, amministratori, soci con ruoli operativi, collaboratori e consulenti con accesso a sistemi o dati; audit e HR dei Clienti

DOCUMENTI COLLEGATI

politiche P13 e P03; documento 22, Revisione degli accessi; documento 23, Chiavi e segreti; documento 43, Registro della formazione; documento 44, Revisione degli accessi (modello); documento 09, AI Act e uso dell'IA nella professione

1 Scopo e ambito

1.1 La procedura fissa i passi obbligatori all'ingresso, al cambio di ruolo e all'uscita di chiunque lavori per Trailgun con accesso a sistemi o dati, perché ogni accesso sia personale, giustificato, minimo e revocato in tempo.

1.2 Vale per ogni forma di rapporto: lavoro dipendente, amministrazione, collaborazione, consulenza, fornitura di personale. Per i consulenti esterni che accedono a dati dei Clienti valgono in più gli obblighi del documento 29 (valutazione dei fornitori).

2 Ruoli

- **Legale rappresentante**: firma gli impegni, decide l'ingresso e l'uscita, conserva i fascicoli del personale.
- **Responsabile della sicurezza**: concede e revoca gli accessi, ruota i segreti, verifica la formazione, firma il verbale di uscita.
- DPO [DPO esterno: nome o società]: consultato sulla verifica dei precedenti e sulle istruzioni al trattamento.
- **Responsabile diretto** della persona: indica il ruolo e gli accessi necessari, segnala per tempo cambi di ruolo e uscite.

3 Ingresso

1 **Ruolo e accessi.** Il responsabile diretto descrive il ruolo e, per ciascun sistema, l'accesso che serve e perché. Si parte dal minimo: un accesso a production si concede solo a chi lo richiede il ruolo.

2 **Riservatezza.** La persona firma l'impegno scritto di riservatezza, che copre il segreto professionale e bancario dei dati dei Clienti e sopravvive alla fine del rapporto.

3 **Designazione.** La persona riceve la designazione al trattamento con le istruzioni scritte (art. 29 GDPR, art. 2-quaterdecies del Codice privacy), comprese le regole del regime dei fascicoli penali (politica P16) e l'accesso al contenuto delle pratiche solo su richiesta del Cliente o per un incidente, sempre registrato.

4 **Verifica dei precedenti**, per chi accede a production, nei limiti dell'art. 8 della L. 20 maggio 1970, n. 300 e dell'art. 10 GDPR: identità, titoli e percorso professionale dichiarati; il certificato del casellario giudiziale solo dove la legge lo consente. L'esito si conserva nel fascicolo del personale, senza copie superflue.

5 **Formazione all'ingresso**, prima del primo accesso: le politiche P01–P17, riconoscimento del phishing, credenziali e autenticazione a più fattori, segnalazione degli eventi di sicurezza, protezione dei dati, regime dei fascicoli penali, alfabetizzazione sull'IA (art. 4 AI Act). La sessione si annota nel registro della formazione (documento 43).

6 **Account personali.** Il Responsabile della sicurezza crea gli account, sempre nominativi e con l'autenticazione a più fattori: casella Google Workspace; organizzazione GitHub (2FA obbligatoria); AWS tramite IAM Identity Center, con credenziali temporanee e il solo insieme di permessi del ruolo; backoffice della piattaforma (gruppo Cognito `admin` o `supporto`) solo se il ruolo lo richiede; console dei fornitori solo se necessarie. Nessun account condiviso, nessuna chiave statica.

7 **Dispositivi.** Il dispositivo di lavoro ha il disco cifrato, il blocco dello schermo, il sistema aggiornato; la persona riceve le regole d'uso (politica P14).

8 **Registrazione.** Gli accessi concessi si annotano nell'elenco degli accessi autorizzati, la base della revisione trimestrale (documento 22).

4 Durante il rapporto e al cambio di ruolo

4.1 Formazione su sicurezza e protezione dei dati e alfabetizzazione sull'IA ogni anno, annotate nel registro della formazione (documento 43). Trailgun partecipa, alle condizioni concordate, ai programmi di sensibilizzazione e formazione dei Clienti DORA (art. 13, par. 6, e art. 30, par. 2, lett. i), DORA).

4.2 A ogni cambio di ruolo gli accessi si rifanno sul nuovo ruolo: si concede ciò che serve e, nello stesso giorno, si toglie ciò che non serve più. Il passaggio si annota nell'elenco degli accessi autorizzati.

4.3 Le violazioni delle politiche si valutano secondo il contratto e la legge applicabile, con un procedimento che rispetta le garanzie della persona.

5 Uscita

1 **Preavviso.** Il responsabile diretto comunica la data di uscita al Responsabile della sicurezza appena la conosce. Per un'uscita improvvisa, il conteggio delle 24 ore parte dalla comunicazione.

2 **Revoca entro 24 ore** di tutti gli accessi, nell'ordine: AWS (IAM Identity Center e sessioni attive); GitHub; backoffice e gruppi Cognito, con la disconnessione globale; console dei fornitori; Google Workspace (la casella si sospende e la posta passa al responsabile diretto); reperibilità e gruppi di comunicazione.

3 **Rotazione dei segreti** a cui la persona aveva accesso, con la procedura del documento 23: chiavi dei fornitori, segreti dei webhook, credenziali di servizio.

4 **Dispositivi e dati.** Restituzione dei dispositivi di Trailgun, oppure cancellazione verificata dei dati di Trailgun e dei Clienti da quelli personali; restituzione di documenti e supporti.

5 **Obblighi che continuano.** Promemoria scritto della riservatezza e del segreto professionale che proseguono dopo il rapporto.

6 **Verbale di uscita**, firmato dal Responsabile della sicurezza (tabella 6), e aggiornamento dell'elenco degli accessi autorizzati. La revisione trimestrale successiva controlla che nulla sia rimasto attivo.

6 · VERBALE DI USCITA	CHE COSA SCRIVERE	CONTENUTO
Persona e ruolo	nome, ruolo, tipo di rapporto	
Data di uscita e di comunicazione	da qui decorrono le 24 ore	
Accessi revocati	sistema per sistema, con data e ora	
Segreti ruotati	elenco per nome, mai i valori; data	
Dispositivi e supporti	restituiti o cancellati; come si è verificato	
Promemoria della riservatezza	consegnato il	
Anomalie	accessi trovati attivi oltre le 24 ore, con il motivo e la correzione	
Firma	Responsabile della sicurezza, data	

7 Evidenze e registri

- Fascicolo del personale: impegno di riservatezza, designazione con istruzioni, esito della verifica dei precedenti.
- Registro della formazione (documento 43), con data, contenuti e partecipanti di ogni sessione.
- Elenco degli accessi autorizzati e revisioni trimestrali (documento 44).
- Verbali di uscita; inventario dei segreti con la data dell'ultima rotazione (documento 23).
- CloudTrail e i registri di accesso delle console, per ricostruire creazione e revoca degli accessi.

8 Riferimenti

GDPR, artt. 29 e 32, par. 4, e art. 10; Codice privacy (D.Lgs. 196/2003), art. 2-quaterdecies; L. 20 maggio 1970, n. 300, art. 8; DORA, art. 9, par. 4, lett. c), art. 13, par. 6, e art. 30, par. 2, lett. i); Reg. del. (UE) 2024/1774, artt. 19-21 (identità unica e autenticazione forte del personale); AI Act (Reg. (UE) 2024/1689), art. 4; ISO/IEC 27001:2022, controlli 5.18 (diritti di accesso), 6.1 (screening), 6.2 (termini e condizioni d'impiego), 6.3 (consapevolezza e formazione), 6.5 (responsabilità dopo la cessazione) e 6.6 (accordi di riservatezza).

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 21 del pacchetto di conformità Trailgun, versione 2.0, stato al 01/12/2026. Attua la politica P13 (sicurezza del personale e formazione) e la politica P03 (controllo degli accessi). Documento riservato, destinato al Cliente e alle sue autorità di vigilanza.