					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P07					Titolo del documento: **Politica di onboarding e cessazione del personale**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineamento a norme e regolamenti applicabili

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 7.2, Clausola 6	Competenza del personale, integrazione sicura e applicazione delle responsabilità in caso di cessazione o cambiamento del rapporto.
ISO/IEC 27002:2022	Controlli 6.2, 6.5, 5	Controlli relativi a onboarding, accesso e ciclo di vita del personale.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Transizione e cessazione del personale, principio del privilegio minimo, registrazione degli audit, gestione degli accessi durante e dopo i cambiamenti relativi al personale.
GDPR UE	Articoli 5(1)(f), 25, 32; Considerando 39	Limitazione degli accessi, riservatezza, protezione e controlli appropriati per i dati del personale.
NIS2 UE	Articolo 21(2)(b, c, d)	Misure di sicurezza del personale e operative; mitigazione delle minacce interne; processi del ciclo di vita.
DORA UE	Articoli 5, 8, 9	Governance, controllo interno ICT, rischio ICT, gestione degli incidenti durante la transizione del personale.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Risorse umane, gestione della conoscenza, sicurezza e conformità nei processi di onboarding e cessazione.

1. Scopo

1.1 La presente politica stabilisce procedure standardizzate per la gestione dell'onboarding, dei trasferimenti interni e delle cessazioni per tutte le tipologie di utenti.

1.2 Garantisce il provisioning e la revoca degli accessi, sia fisici sia logici, in modo tempestivo e sicuro, assicurando al contempo riservatezza, accountability e restituzione degli asset.

1.3 La presente politica mitiga i rischi associati ad accessi non autorizzati, fuoriuscita di dati e mancata restituzione degli asset, integrando i controlli di onboarding e cessazione nei processi HR, IT e di sicurezza.

1.4 Supporta il Controllo 6 dell'Appendice A della ISO/IEC 27001:2022, garantendo che gli obblighi di sicurezza del personale siano applicati durante e dopo il rapporto di lavoro o di collaborazione.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipendenti, collaboratori esterni, consulenti, fornitori e altre terze parti cui è concesso l'accesso ai sistemi, alle reti, alle strutture o ai dati dell'organizzazione.

2.2 Essa disciplina l'intero ciclo di vita di:

2.2.1 onboarding (assunzione, contrattualizzazione o incarico temporaneo)

2.2.2 trasferimento interno o modifica del ruolo

2.2.3 offboarding (dimissioni, pensionamento, cessazione, scadenza del contratto)

2.3 La politica copre:

2.3.1 accesso logico (sistemi, applicazioni, cloud, VPN)

2.3.2 accesso fisico (badge, chiavi, sistemi di accesso agli edifici)

2.3.3 asset assegnati (laptop, telefoni, token, credenziali)

2.3.4 presa visione delle politiche e obblighi di riservatezza

2.4 Tutte le funzioni aziendali (HR, IT, Gestione delle strutture e degli asset, Sicurezza e Management) sono responsabili dell'esecuzione del proprio ruolo nei workflow di onboarding e offboarding.

3. Obiettivi

3.1 Garantire che a tutto il personale sia concesso l'accesso solo dopo il soddisfacimento dei prerequisiti di sicurezza, formazione e natura contrattuale.

3.2 Revocare i diritti di accesso e recuperare gli asset dell'organizzazione immediatamente in caso di modifica del ruolo o cessazione.

3.3 Preservare la riservatezza, l'integrità e la disponibilità (CIA) degli asset dell'organizzazione durante le transizioni del personale.

3.4 Supportare la tracciabilità ai fini di audit e la difendibilità in sede giudiziaria mediante registrazioni complete degli eventi di onboarding e cessazione.

3.5 Ridurre l'esposizione alle minacce interne mediante validazione e documentazione di tutti gli eventi di accesso correlati al personale.

3.6 Allineare il ciclo di vita del personale dell'organizzazione a pratiche di sicurezza basate sul rischio e agli obblighi normativi.

4. Ruoli e responsabilità

4.1 Direzione esecutiva

4.1.1 Approva la presente politica e assegna autorità e risorse per i processi di onboarding, offboarding e controllo degli accessi.

4.1.2 Garantisce che le transizioni del personale non espongano l'organizzazione a rischi di sicurezza o legali non accettabili.

4.2 Risorse Umane (HR)

4.2.1 Avviano i workflow di onboarding e cessazione per i dipendenti e notificano i cambiamenti alle funzioni interessate.

4.2.2 Garantiscono che le verifiche dei precedenti, i contratti, gli accordi di riservatezza e la presa visione delle politiche siano completati prima della concessione dell'accesso.

4.2.3 Informano IT e Gestione delle strutture e degli asset delle uscite del personale in conformità allo SLA di notifica.

4.2.4 Si coordinano con la Funzione legale e compliance per applicare gli obblighi successivi alla cessazione del rapporto (ad es. clausole di non divulgazione).

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Frequenza di riesame della politica

9.1.1 La presente politica deve essere riesaminata:

9.1.1.1 annualmente, oppure

9.1.1.2 dopo qualsiasi incidente significativo che coinvolga uso improprio degli accessi, perdita di asset o mancato rispetto delle procedure

9.1.1.3 in occasione dell'implementazione di modifiche rilevanti ai sistemi HR o alla piattaforma IAM

9.1.1.4 a seguito di aggiornamenti normativi o legali che incidano sui dati del personale o sui relativi obblighi

9.2 Processo di riesame e titolarità

9.2.1 Il Responsabile del SGSI e il Direttore HR devono coordinare il riesame, con il contributo di Sicurezza IT, Legale e compliance.

9.2.2 Tutte le modifiche devono essere approvate dalla Direzione esecutiva e dal Comitato direttivo del SGSI.

9.2.3 Le versioni aggiornate devono essere ridistribuite alle funzioni aziendali e al personale interessati per una nuova presa visione.

9.3 Controllo documentale e conservazione

9.3.1 La presente politica deve includere:

9.3.2 controllo delle versioni, storico delle versioni e data di entrata in vigore

9.3.3 proprietario del documento e revisore/i

9.3.4 classificazione della politica e registrazione dell'approvazione

9.3.5 Le versioni obsolete devono essere archiviate per un periodo minimo di 3 anni in conformità con la Politica di gestione documentale.

10. Politiche correlate e collegamenti

10.1.1 La presente politica si integra direttamente con:

10.1.2 P1 – Politica per la sicurezza delle informazioni: stabilisce gli obiettivi di sicurezza dell'organizzazione, inclusa la governance degli accessi del personale.

10.1.3 P4 – Politica di controllo degli accessi: definisce i requisiti operativi per l'assegnazione e la revoca dell'accesso ai sistemi e degli accessi fisici sulla base degli eventi di onboarding e cessazione.

10.1.4 P3 – Politica di uso accettabile: richiede la presa visione durante l'onboarding e supporta l'applicazione della politica dopo la cessazione.

10.1.5 P6 – Politica di gestione del rischio: garantisce che i rischi relativi agli accessi utente e alle transizioni siano valutati e mitigati in linea con i principi del SGSI.

10.1.6 P11 – Politica di gestione degli account utente e dei privilegi: disciplina i controlli tecnici per il provisioning e la revoca degli accessi a supporto della presente politica.

10.2 Tali politiche costituiscono un sistema integrato di controlli per gestire gli eventi del ciclo di vita del personale in modo sicuro e tracciabile.

11. Norme e quadri di riferimento

11.1 La presente politica è allineata a quadri di riferimento internazionalmente riconosciuti in materia di sicurezza, privacy e governance IT, per garantire che i processi di onboarding e cessazione siano sicuri, tracciabili e conformi ai requisiti legali e organizzativi.

11.2 ISO/IEC 27001:

11.2.1 Clausola 7.2 – Competenza e Clausola 6.2 – Obiettivi per la sicurezza delle informazioni: la presente politica supporta l'istituzione della competenza del personale e l'integrazione sicura delle persone nei ruoli che influenzano gli obiettivi del SGSI.

11.2.2 Appendice A, Controllo 6.5 – Responsabilità dopo la cessazione o il cambiamento del rapporto di lavoro: la presente politica applica pienamente i controlli sui diritti di accesso residui, sulla custodia dei dati e sugli obblighi contrattuali al momento dell'uscita.

11.2.3 Appendice A, Controllo 5.9 – Screening e 6.2 – Termini e condizioni di impiego: le procedure di onboarding incorporano meccanismi di verifica dei precedenti e di presa visione della politica coerenti con tali clausole.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personnel Termination) e PS-5 (Personnel Transfer): la presente politica impone la rimozione o modifica strutturata dei diritti di accesso, dei badge fisici e degli asset.

11.3.2 AC-2 (Account Management) e AC-6 (Least Privilege): le disposizioni garantiscono che l'accesso sia allineato al ruolo e prontamente revocato quando non più necessario.

11.3.3 IA-4 (Identifier Management) e IA-5 (Authenticator Management): supporta la gestione sicura delle credenziali durante e dopo i cambiamenti del personale.

11.3.4 CM-5 (Access Restrictions for Change): previene modifiche non autorizzate successive alla cessazione attraverso la revoca dei diritti di accesso elevati.

11.3.5 AU-2 e AU-6: la registrazione e la tracciabilità degli eventi di accesso sono rafforzate tramite integrazione con IAM e pista di audit.

11.4 GDPR UE (2016/679):

11.4.1 Articolo 5(1)(f): protegge i dati personali da accessi non autorizzati, qui applicato tramite la revoca degli accessi utente durante l'offboarding.

11.4.2 Articolo 32: richiede controlli tecnici e organizzativi appropriati per proteggere i dati personali durante il ciclo di vita del rapporto di lavoro.

11.4.3 Articolo 25 – Protezione dei dati fin dalla progettazione: garantisce che onboarding e cessazione integrino minimizzazione dei dati, conservazione e controlli di accesso leciti.

11.4.4 Considerando 39: enfatizza la limitazione degli accessi e la riservatezza, supportate dalla struttura della presente politica.

11.5 Direttiva NIS2 UE (2022/2555):

11.5.1 Articolo 21(2)(b, c, d): richiede misure di sicurezza del personale e operative per affrontare il controllo degli accessi, la mitigazione delle minacce interne e i processi del ciclo di vita, tutti aspetti riflessi nella presente politica.

11.6 DORA UE (2022/2554):

11.6.1 Articolo 5 – Governance e controllo interno: la presente politica supporta la governance interna ICT relativa al rischio umano e alla gestione degli accessi.

11.6.2 Articolo 8 – Gestione del rischio ICT: applica controlli alle transizioni del personale che potrebbero esporre asset critici o ambienti regolamentati.

11.6.3 Articolo 9 – Classificazione e gestione degli incidenti: garantisce che le violazioni correlate alla cessazione siano segnalabili e mitigate tramite adeguata revoca degli accessi e gestione degli asset.

11.7 COBIT 2019:

11.7.1 APO07 – Gestire le risorse umane: definisce ruoli, responsabilità e azioni del ciclo di vita per onboarding e cessazione allineati agli obiettivi di governance.

11.7.2 BAI08 – Gestione della conoscenza: rafforza la documentazione delle procedure, la conservazione della conoscenza e il trasferimento dei controlli al termine del rapporto.

11.7.3 DSS05 – Gestire i servizi di sicurezza: applica disattivazione degli utenti, controllo degli asset e accountability durante le transizioni di ruolo.

11.7.4 MEA03 – Monitorare, valutare e verificare la conformità: garantisce che i controlli di onboarding e offboarding siano valutati durante audit interni ed esterni.