					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P07S					Titolo del documento: **Politica di inserimento 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**

Allineata alle norme e ai regolamenti applicabili

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 6.2, 7	Requisiti di sicurezza delle risorse umane e di sensibilizzazione
ISO/IEC 27002:2022	Controlli 6.2, 6.5	Pratiche di sicurezza per l'inserimento e la cessazione del rapporto
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Cessazione del personale; ciclo di vita degli account; pianificazione
Direttiva NIS2 dell'UE	Articolo 21(2)(h)	Sicurezza delle risorse umane e ciclo di vita degli accessi
Regolamento DORA dell'UE	Articolo 12	Controlli degli accessi e revoca degli accessi ai sistemi ICT
COBIT 2019	APO07, DSS01	Sicurezza del personale, controlli degli accessi logici e fisici
GDPR dell'UE	Articolo 32	Sicurezza dei dati personali durante il rapporto di lavoro

1. Scopo

1.1 La presente politica definisce il processo di inserimento di nuovi dipendenti o collaboratori esterni e la rimozione sicura degli accessi quando il rapporto cessa o il ruolo cambia.

1.2 Garantisce che l'assegnazione degli accessi avvenga secondo il principio del privilegio minimo, che tutti gli asset siano censiti e che le azioni critiche, quali la disattivazione dei sistemi e il recupero degli asset, siano completate tempestivamente.

1.3 La presente politica supporta la conformità, l'integrità operativa e la protezione dei dati mediante attività di inserimento e cessazione strutturate e verificabili in sede di audit.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i dipendenti a tempo indeterminato e determinato

2.1.2 Collaboratori esterni, consulenti e tirocinanti

2.1.3 Fornitori di servizi esterni con accesso ai sistemi o accesso fisico

2.2 Comprende:

2.2.1 Inserimento: creazione degli account utente, concessione degli accessi, assegnazione delle dotazioni

2.2.2 Cessazione: rimozione degli accessi, recupero dei beni aziendali e chiusura sicura delle identità digitali

2.2.3 Modifiche di ruolo interne che richiedono la riconfigurazione degli accessi o la riassegnazione degli asset

2.3 Si applica a tutti i dispositivi, le piattaforme e le sedi utilizzati per le attività aziendali ufficiali.

3. Obiettivi

3.1 Assicurare che il nuovo personale riceva accessi e risorse sulla base di ruoli e responsabilità verificati.

3.2 Garantire che gli utenti uscenti siano completamente rimossi da sistemi e strutture entro la fine dell'ultimo giorno lavorativo.

3.3 Prevenire account orfani e asset non restituiti, che costituiscono un rischio per la sicurezza.

3.4 Mantenere registrazioni documentate delle attività di inserimento, trasferimento interno e cessazione.

3.5 Promuovere la responsabilizzazione mediante liste di controllo e coordinamento interfunzionale dei ruoli.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 Approva gli accessi per i ruoli ad alto privilegio e sovrintende al programma di inserimento e cessazione.

4.1.2 Garantisce che le eccezioni siano giustificate e che siano adottate azioni correttive quando i processi non vengono seguiti.

4.2 Responsabile d'ufficio / Risorse Umane (HR)

4.2.1 Avvia l'inserimento dei nuovi assunti e notifica all'IT le cessazioni.

4.2.2 Garantisce il completamento della documentazione legale (ad es. accordo di riservatezza) e delle attestazioni di presa visione delle politiche di sicurezza.

4.2.3 Mantiene le liste di controllo di assunzione e cessazione e monitora la conformità alla politica.

[... 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 Riesame annuale

9.1.1 La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore Generale (GM) e dai referenti HR/IT.

9.2 Trigger di riesame anticipato

9.2.1 Devono essere effettuati aggiornamenti se:

9.2.1.1 Vengono introdotti nuovi sistemi HR o IT

9.2.1.2 Cambia il fornitore esterno di servizi IT o il servizio HR gestito

9.2.1.3 Gli audit di sicurezza rilevano carenze di processo

9.2.1.4 Cambiano gli obblighi normativi (ad es. aggiornamenti del GDPR)

9.2.1.5 Si verifica un guasto critico nel processo di cessazione o una violazione

9.3 Controllo delle versioni e approvazione

9.3.1 Ogni versione della presente politica deve includere:

9.3.1.1 Numero di versione e data

9.3.1.2 Sintesi delle modifiche

9.3.1.3 Approvazione da parte del Direttore Generale (GM)

9.3.1.4 Versioni precedenti archiviate e conservate per almeno tre anni

9.4 Comunicazione e presa visione

9.4.1 Tutto il personale responsabile dell'inserimento o della cessazione deve essere informato di qualsiasi aggiornamento della politica. Sono obbligatori briefing annuali di sensibilizzazione o aggiornamento.

10. Politiche correlate e collegamenti

10.1 La presente politica supporta ed è supportata dalle seguenti:

10.1.1 P2S – Politica sui ruoli e le responsabilità di governance: assicura la responsabilizzazione nei processi di accesso e inserimento

10.1.2 P4S – Politica di controllo degli accessi: definisce l'applicazione tecnica dell'assegnazione degli accessi basata sui ruoli e della disattivazione

10.1.3 P6S – Politica di gestione del rischio: valuta i rischi derivanti dal fallimento dei controlli di inserimento e cessazione

10.1.4 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: applica i requisiti di orientamento del personale durante l'inserimento

10.1.5 P30S – Politica di risposta agli incidenti: tratta come incidenti di sicurezza la mancata revoca degli accessi o il furto di asset

11. Norme e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.2 – Stabilisce i requisiti di sicurezza delle risorse umane

11.1.2 Clausola 7.2 – Richiede la formazione di sensibilizzazione per il nuovo personale

11.2 ISO/IEC 27002

11.2.1 Controlli 6.2 e 6.5 – Descrivono in dettaglio le pratiche di sicurezza per l'inserimento e la cessazione del rapporto di lavoro

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Procedure di cessazione del personale, inclusa la disattivazione degli accessi

11.3.2 AC-2 – Garantisce la gestione del ciclo di vita degli account per l'accesso degli utenti

11.3.3 PL-4 – Richiede la pianificazione delle transizioni del personale

11.4 GDPR dell'UE

11.4.1 Articolo 32 – Garantisce un livello di sicurezza adeguato durante e dopo il rapporto di lavoro, in particolare per l'accesso ai dati personali

11.5 Direttiva NIS2 dell'UE

11.5.1 Articolo 21(2)(h) – Richiede controlli sulla sicurezza delle risorse umane e sul ciclo di vita degli accessi

11.6 Regolamento DORA dell'UE

11.6.1 Articolo 12 – Richiede ai soggetti finanziari regolamentati di controllare l'accesso del personale ai sistemi ICT, incluse le procedure di revoca

11.7 COBIT 2019

11.7.1 APO07 Gestire le risorse umane – Stabilisce i requisiti di sicurezza per il ciclo di vita del personale

11.7.2 DSS01 – Comprende il controllo degli accessi logici e fisici durante le transizioni del personale