					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P11S					Titolo del documento: **Politica di gestione degli account utente e dei privilegi**							
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 a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clausole 5.3, 8	Ruoli, responsabilità e pianificazione/controllo operativi per la gestione degli accessi degli utenti
ISO/IEC 27002:2022	Controllo 8	Controlli per l'assegnazione, il riesame e la rimozione dei privilegi elevati
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Creazione degli account, monitoraggio, principio del privilegio minimo e segregazione dei compiti
EU NIS2	Articolo 21(2)(d)	Gestione degli accessi degli utenti per i soggetti essenziali e importanti
EU DORA	Articolo 9(2)(b)	Controllo degli accessi privilegiati nei soggetti finanziari
COBIT 2019	DSS05.03, DSS05.04	Provisioning degli accessi, revoca degli accessi e riesame periodico degli accessi degli utenti
EU GDPR	Articolo 32	Controlli di accesso appropriati per la protezione dei dati personali

1. Finalità

1.1 La presente politica stabilisce le regole per la gestione degli account utente e dei diritti di accesso in modo sicuro, coerente e tracciabile. Garantisce che solo gli utenti autorizzati abbiano accesso ai sistemi e ai dati e che tale accesso sia appropriato al loro ruolo e alle loro responsabilità.

1.2 Una gestione efficace degli account e dei privilegi è essenziale per prevenire accessi non autorizzati, ridurre al minimo le minacce interne e assicurare la conformità alla ISO/IEC 27001, al GDPR e agli altri requisiti normativi applicabili.

1.3 La presente politica consente all'organizzazione di assegnare titolarità e responsabilità per l'utilizzo degli account, monitorare e sottoporre ad audit le elevazioni di privilegio e disabilitare o revocare gli accessi in modo sicuro quando non sono più necessari.

1.4 Tutela inoltre le operazioni aziendali da errori operativi o usi impropri causati da accessi eccessivi o non monitorati e contribuisce a ridurre il rischio di perdita accidentale di dati, uso improprio dei privilegi o mancata conformità normativa.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i dipendenti, i tirocinanti, i collaboratori esterni e gli utenti terzi che accedono ai sistemi IT dell'organizzazione;

2.1.2 tutti i sistemi, dispositivi, servizi e piattaforme gestiti dall'organizzazione o per suo conto, comprese le piattaforme cloud, l'infrastruttura on-premise e gli strumenti di terze parti.

2.2 Essa copre tutte le tipologie di account utente, inclusi:

2.2.1 account utente nominativi (ad es. account e-mail, accessi ai sistemi);

2.2.2 account amministrativi e account di sistema;

2.2.3 credenziali di accesso temporanee, guest o di terze parti;

2.2.4 account di servizio utilizzati da applicazioni o sistemi di automazione.

2.3 La politica si applica all'intero ciclo di vita dell'account, dalla creazione e approvazione fino alla modifica, al monitoraggio e alla disattivazione. Ciò include il provisioning iniziale degli accessi durante l'onboarding, il riesame degli accessi in caso di modifica del ruolo e la revoca degli accessi durante l'offboarding.

3. Obiettivi

3.1 Assegnare identità utente univoche e tracciabili a tutti gli utenti dei sistemi, garantendo l'accountability ed eliminando il ricorso a credenziali condivise.

3.2 Applicare il principio del privilegio minimo, assicurando che agli utenti sia concesso esclusivamente il livello minimo di accesso necessario per svolgere le proprie mansioni.

3.3 Prevenire accessi non autorizzati a sistemi o dati sensibili mediante processi di approvazione e riesame chiaramente documentati.

3.4 Garantire la disattivazione tempestiva degli account utente quando non sono più necessari, ad esempio in caso di cessazione del rapporto, completamento del contratto o modifica del ruolo.

3.5 Mantenere un ambiente sicuro e verificabile in sede di audit, documentando tutte le modifiche agli account, le approvazioni e i riesami periodici.

3.6 Garantire che l'elevazione dei privilegi sia rigorosamente controllata, approvata in modo indipendente e registrata e che gli accessi elevati siano revocati tempestivamente quando non sono più necessari.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 Ha la responsabilità complessiva dell'applicazione della presente politica.

4.1.2 Garantisce che le pratiche di gestione degli account siano allineate ai requisiti di certificazione ISO/IEC 27001 e agli obblighi legali pertinenti, tra cui il GDPR.

4.1.3 Deve essere informato immediatamente di qualsiasi accesso non autorizzato, incidente di sicurezza delle informazioni o violazione della politica relativa agli account utente.

4.1.4 Sovrintende ai riesami della politica, agli audit e alle azioni conseguenti.

4.2 Responsabile IT o fornitore esterno di servizi di supporto IT

4.2.1 È responsabile dell'attuazione tecnica dei controlli su account e privilegi nei sistemi utilizzati dall'organizzazione.

4.2.2 Deve effettuare il provisioning degli accessi, modificare e disattivare gli account utente esclusivamente sulla base di approvazioni documentate.

4.2.3 Deve applicare i requisiti di complessità delle password, il blocco automatico dello schermo, l'autenticazione a più fattori (MFA), ove disponibile, e la registrazione dei log di audit dei sistemi.

4.2.4 Deve mantenere registrazioni sicure di tutte le approvazioni di accesso, della titolarità degli account, delle elevazioni di privilegio e delle revoche degli accessi.

4.2.5 Deve monitorare la presenza di account non autorizzati o orfani e segnalare eventuali discrepanze al GM.

[... 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 La presente politica deve essere riesaminata almeno annualmente dal GM e dal Responsabile IT per garantire la conformità a:

9.1.1 controlli e linee guida vigenti della ISO/IEC 27001:2022;

9.1.2 aggiornamenti normativi, ad esempio GDPR, DORA e NIS2;

9.1.3 cambiamenti nei sistemi, nei servizi o nella struttura aziendale.

9.2 I riesami devono essere effettuati anche a seguito di:

9.2.1 incidenti di sicurezza significativi o risultanze di audit;

9.2.2 modifiche rilevanti ai sistemi IT o all'architettura degli account;

9.2.3 introduzione di nuove piattaforme che richiedano l'integrazione del controllo degli accessi.

9.3 Tutte le modifiche devono essere approvate dal GM e comunicate chiaramente al personale interessato.

10. Politiche correlate e collegamenti

10.1 P2S – Politica sui ruoli e sulle responsabilità di governance: stabilisce responsabilità e autorità decisionale per le approvazioni degli accessi e la supervisione.

10.2 P4S – Politica di controllo degli accessi: disciplina l'applicazione del controllo degli accessi a livello di sistema e i metodi di autenticazione.

10.3 P7S – Politica di onboarding e cessazione del personale: garantisce che la creazione e la rimozione degli account siano integrate nelle variazioni del personale gestite dalle Risorse Umane (HR).

10.4 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: forma gli utenti sulle pratiche sicure di gestione degli account e sulle aspettative di utilizzo.

10.5 P30S – Politica di risposta agli incidenti (P30): definisce le azioni da intraprendere se l'uso improprio di un account determina una violazione della sicurezza o una divulgazione non autorizzata.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 5.3: richiede che ruoli e responsabilità per la sicurezza delle informazioni siano chiaramente assegnati e applicati.

11.1.2 Clausola 8.1: la pianificazione e il controllo operativi devono includere la gestione degli accessi degli utenti.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.2: descrive controlli tecnici e procedurali per l'assegnazione, il riesame e la rimozione dei privilegi elevati.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: richiede la creazione, il monitoraggio e la revoca degli account sulla base di ruoli e processi definiti.

11.3.2 AC-5: disciplina la segregazione dei compiti per prevenire conflitti o abusi di privilegio.

11.3.3 AC-6: prescrive l'applicazione del principio del privilegio minimo a tutti i diritti di accesso.

11.4 EU GDPR

11.4.1 Articolo 32: richiede controlli di accesso appropriati per proteggere i dati personali da accessi non autorizzati o alterazioni.

11.5 EU NIS

11.5.1 Articolo 21(2)(d): impone la gestione degli accessi degli utenti come parte dei controlli di sicurezza fondamentali per i soggetti essenziali e importanti.

11.6 EU DORA

11.6.1 Articolo 9(2)(b): richiede ai soggetti finanziari di implementare controlli di accesso che limitino e monitorino i diritti privilegiati.

11.7 COBIT 2019

11.7.1 DSS05.03: specifica il provisioning degli accessi e la revoca degli accessi degli utenti nell'ambito della governance IT.

11.7.2 DSS05.04: richiede il riesame continuo e l'allineamento degli accessi degli utenti con i ruoli organizzativi.