					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P11					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**

Allineamento a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 6.1.3, Clausola 8	-
ISO/IEC 27002:2022	Controlli 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR UE	Articoli 5(1)(f), 32; Considerando 39	-
NIS2 UE	Articoli 21(2)(a, d), 21(3)	-
DORA UE	Articoli 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Finalità

1 La presente politica stabilisce controlli obbligatori per la gestione degli account utente e dei privilegi in tutti i sistemi e servizi informativi. Garantisce che l'accesso alle risorse dell'organizzazione sia concesso sulla base di un'identità validata, della necessità connessa al ruolo, del principio del privilegio minimo e della segregazione dei compiti (SoD).

1.1 Supporta l'impegno dell'organizzazione per la sicurezza delle informazioni mediante l'applicazione di processi strutturati e verificabili per il provisioning degli accessi, l'assegnazione dei privilegi, il monitoraggio dell'utilizzo e la revoca degli accessi.

1.2 La presente politica è essenziale per ridurre il rischio di accessi non autorizzati, uso improprio dei privilegi, minacce interne e mancata conformità ai quadri normativi e regolamentari applicabili.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i dipendenti, collaboratori esterni, fornitori di servizi terzi, consulenti e altri soggetti ai quali sia concesso l'accesso alle risorse IT, alle applicazioni o ai dati dell'organizzazione.

2.2 Essa disciplina tutti i sistemi e gli ambienti nei quali sono applicati meccanismi di autenticazione degli utenti e controllo degli accessi, inclusi, a titolo esemplificativo e non esaustivo:

2.2.1 Applicazioni aziendali e basi di dati

2.2.2 Piattaforme cloud e ambienti SaaS

2.2.3 Sistemi operativi e console amministrative

2.2.4 Strumenti di accesso remoto (VPN, gestione dei dispositivi mobili)

2.2.5 Sistemi di gestione delle identità e degli accessi

2.3 La politica comprende sia gli account utente standard sia gli account privilegiati e include controlli su:

2.3.1 Creazione, modifica e disattivazione degli account

2.3.2 Elevazione dei privilegi e delega

2.3.3 Controllo e monitoraggio delle sessioni

2.3.4 Metodi di autenticazione e gestione delle credenziali

3. Obiettivi

3.1 Garantire che tutti gli account utente siano univocamente identificabili, correttamente autorizzati e assegnati solo a seguito di una validazione formale della necessità.

3.2 Attuare il principio del privilegio minimo e prevenire accessi non necessari o eccessivi mediante l'applicazione di controlli rigorosi sull'assegnazione e sull'utilizzo degli account privilegiati.

3.3 Richiedere aggiornamenti tempestivi dello stato degli account in funzione dei cambiamenti occupazionali o di ruolo, inclusa la disattivazione immediata alla cessazione del rapporto.

3.4 Consentire il rilevamento proattivo e le azioni di rimedio su account inattivi, utilizzati impropriamente o non autorizzati mediante log, riesami e automazione.

3.5 Mantenere l'allineamento con ISO/IEC 27001:2022 e gli standard correlati, nonché soddisfare gli obblighi previsti dai pertinenti quadri giuridici e regolamentari quali GDPR, NIS2, DORA e COBIT 2019.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il proprietario della politica e ne garantisce l'applicazione in tutta l'organizzazione.

4.1.2 Riesamina e approva eventuali eccezioni formali o casi di accesso di emergenza.

4.1.3 Riporta le risultanze degli audit relative agli account ed effettua l'escalation dei rischi alla Direzione esecutiva.

4.2 Responsabile del controllo degli accessi / Amministratore IT

4.2.1 Mantiene e gestisce i controlli tecnici per la gestione del ciclo di vita degli account utente.

4.2.2 Esegue le attività di provisioning degli accessi, revoca degli accessi e gestione dei privilegi a fronte di richieste approvate.

4.2.3 Mantiene un registro autorevole di tutti gli account utente, del loro stato e del relativo livello di privilegio.

4.2.4 Supporta gli audit e i riesami di conformità mediante log e report delle attività.

[... 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 o in caso di cambiamenti significativi relativi a:

9.1.1 Struttura organizzativa o processi aziendali

9.1.2 Sistemi IT, piattaforme di identità o modalità di accesso

9.1.3 Requisiti normativi o contrattuali relativi alla gestione delle identità e degli accessi

9.2 Il Responsabile della sicurezza delle informazioni (CISO), congiuntamente al Responsabile del controllo degli accessi, è responsabile dell'avvio del processo di riesame e del coordinamento dei feedback delle parti interessate.

9.3 Riesami intermedi possono essere attivati da:

9.3.1 Incidenti di sicurezza correlati all'uso improprio degli account

9.3.2 Risultanze degli audit che evidenzino carenze nella gestione del ciclo di vita degli account

9.3.3 Implementazione di nuovi strumenti per la gestione delle identità o degli accessi privilegiati

9.4 Gli aggiornamenti alla presente politica devono essere:

9.4.1 Sottoposti a controllo delle versioni e registrati nella libreria documentale del SGSI

9.4.2 Comunicati a tutte le parti interessate rilevanti, inclusi responsabili di funzione, operation IT e HR

9.4.3 Supportati da materiali formativi e guide procedurali aggiornati

9.5 Tutte le modifiche devono essere approvate dalla Direzione esecutiva o dal Comitato di indirizzo per la sicurezza delle informazioni e registrate ai fini di audit.

10. Politiche correlate e collegamenti

10.1 La presente politica è collegata operativamente ed è supportata dalle seguenti politiche correlate nell'ambito del SGSI:

10.1.1 P4 Politica di controllo degli accessi: stabilisce i principi e i meccanismi generali di controllo degli accessi, inclusi i controlli basati su regole e quelli basati sui ruoli.

10.1.2 P7 Politica di onboarding e cessazione del personale: fornisce i passaggi procedurali per l'attivazione e la cessazione dell'accesso utente in allineamento con le azioni HR.

10.1.3 P8 Politica di consapevolezza e formazione sulla sicurezza delle informazioni: rafforza le responsabilità degli utenti in materia di sicurezza degli account e protezione delle credenziali.

10.1.4 P13 Politica di classificazione ed etichettatura dei dati: guida i livelli di accesso in base alla classificazione dei dati, assicurando che i limiti dei privilegi siano coerenti con i livelli di sensibilità.

10.1.5 P22 Politica di registrazione e monitoraggio: garantisce che le tracce di audit siano raccolte per tutte le attività relative agli account e riesaminate per rilevare anomalie o utilizzi non autorizzati.

10.1.6 P30 Politica di risposta agli incidenti (P30): disciplina escalation, contenimento e azioni successive all'incidente nei casi di uso improprio dei privilegi o attività non autorizzata sugli account.

10.2 Ciascuna di queste politiche opera congiuntamente per applicare un quadro coerente e basato sul rischio per la gestione delle identità e degli accessi in tutta l'organizzazione.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata a standard di cibersicurezza e quadri normativi riconosciuti a livello globale che richiedono una gestione sicura di identità, accessi e privilegi quale componente fondamentale della sicurezza delle informazioni dell'organizzazione.

11.2 ISO/IEC 27001:

11.2.1 Clausola 6.1.3 - richiede alle organizzazioni di determinare, valutare e trattare i rischi per la sicurezza delle informazioni, rendendo la gestione degli accessi e dei privilegi un controllo formale basato sul rischio integrato nel processo di pianificazione del SGSI.

11.2.2 Clausola 8.1 - Pianificazione e controllo operativi: rafforza l'attuazione di misure di sicurezza tecniche e procedurali che disciplinano l'accesso degli utenti e l'accesso privilegiato.

11.3 ISO/IEC 27002:2022 - Controlli 5.15 a 5:

11.3.1 Controllo 5.15 - Gestione degli accessi degli utenti: supporta processi formali per il provisioning degli accessi, l'autorizzazione degli accessi e il riesame periodico dei diritti di accesso.

11.3.2 Controllo 5.16 - Gestione delle identità: stabilisce l'unicità dell'identità, i controlli sul ciclo di vita e l'applicazione di un'autenticazione sicura.

11.3.3 Controllo 5.17 - Informazioni di autenticazione: garantisce che l'assegnazione e l'uso delle informazioni di autenticazione siano rigorosamente controllati, tracciabili e allineati al principio del privilegio minimo lungo tutto il ciclo di vita dell'account utente.

11.3.4 Controllo 5.18 - Diritti di accesso: pienamente trattato tramite assegnazione dei privilegi basata sui ruoli, audit e requisiti di approvazione per l'accesso elevato.

11.4 Tali controlli guidano l'attuazione strutturata della registrazione e cancellazione degli account, della separazione dei privilegi e dell'uso delle informazioni di autenticazione. La politica applica la governance del ciclo di vita dell'identità, l'accesso just-in-time e il monitoraggio delle sessioni elevate per prevenire usi non autorizzati dei sistemi.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politica di controllo degli accessi) e AC-2 (Gestione degli account): recepiti attraverso obblighi di politica relativi alle approvazioni di accesso, alla mappatura dei ruoli e all'audit degli account utente.

11.5.2 AC-5 (Segregazione dei compiti) e AC-6 (Privilegio minimo): soddisfatti tramite restrizione dei privilegi, allineamento ai ruoli lavorativi e doppia approvazione per attività ad alto rischio.

11.5.3 IA-2 a IA-5 (Identificazione e autenticazione): applicati tramite meccanismi di autenticazione forte, regole sul ciclo di vita delle credenziali e requisiti MFA.

11.5.4 AU-2, AU-12 (Registrazione e analisi di audit): affrontati mediante registrazione delle sessioni e monitoraggio delle attività privilegiate negli ambienti sensibili.

11.6 GDPR UE (2016/679):

11.6.1 Articolo 32 - Sicurezza del trattamento: richiede controlli di accesso e meccanismi di verifica dell'identità per proteggere i dati personali. È soddisfatto imponendo approvazioni degli account, riesami dei privilegi e misure di autenticazione forte.

11.6.2 Articolo 5(1)(f) - Integrità e riservatezza: garantisce che i dati personali siano accessibili solo a utenti autorizzati con ruoli legittimi, rafforzato dall'applicazione della gestione degli account.

11.6.3 Considerando 39: richiede una chiara limitazione degli accessi e accountability; la presente politica supporta la piena tracciabilità delle identità utente e delle assegnazioni di privilegi.

11.7 Direttiva UE NIS2 (2022/2555):

11.7.1 Articolo 21(2)(a, d): richiede alle entità di applicare politiche di gestione degli accessi e una gestione sicura delle credenziali e delle sessioni privilegiate, supportata dai controlli di provisioning, monitoraggio ed eccezione previsti dalla presente politica.

11.7.2 Articolo 21(3): promuove la disciplina degli accessi e una forte garanzia dell'identità nei settori critici, soddisfatta mediante l'uso di ID univoci, RBAC e accessi elevati limitati nel tempo.

11.8 DORA UE (2022/2554):

11.8.1 Articolo 5 - Governance e controllo ICT: impone processi formalizzati per la gestione degli utenti ICT, coperti tramite provisioning documentato, disattivazione e gestione delle eccezioni.

11.8.2 Articolo 9 - Gestione del rischio ICT: impone alle organizzazioni di proteggere i sistemi tramite restrizioni di accesso e monitoraggio, affrontato mediante MFA, registrazione nei log degli accessi privilegiati e riesami centralizzati.

11.9 COBIT 2019:

11.9.1 DSS01 - Managed Operations: promuove l'applicazione di controlli operativi standardizzati, inclusi la gestione del ciclo di vita degli account utente e la documentazione degli accessi.

11.9.2 DSS05 - Managed Security Services: riflette l'amministrazione sicura dei privilegi utente e di sistema, supportando la mitigazione del rischio tramite privilegio minimo e validazione della traccia di audit.

11.9.3 APO13 - Managed Security: richiede la governance degli accessi sugli asset digitali, soddisfatta tramite prassi formalizzate di autorizzazione degli account e dei ruoli con obblighi di riesame periodico.