					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P04					Titolo del documento: **Politica di controllo degli accessi**							
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, ove applicabile, a standard e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.15, 5.17, 5.18	Gestione degli accessi logici e fisici
ISO/IEC 27002:2022	Controlli 8.2, 8.3	Accesso basato sui ruoli e gestione delle identità
NIST SP 800-53 Rev. 5	AC-1 fino ad AC-20, IA-1 fino a IA-8	Controlli su account e accessi, identità e autenticazione
GDPR UE	Articoli 5(1)(f), 32(1)(b); Considerando 39	Protezione dei dati e minimizzazione
NIS2 UE	Articolo 21(2)(c–e)	Controllo degli accessi, autenticazione degli utenti e protezione degli asset
DORA UE	Articoli 6, 9(2)	Accesso ai sistemi ICT e degli utenti, controlli rafforzati e terze parti
COBIT 2019	APO07 Gestire le risorse umane, BAI03, DSS01, DSS05, MEA03	Onboarding, operazioni, monitoraggio, conformità

1. Scopo

1.1 La presente politica stabilisce i principi, le responsabilità e i requisiti di controllo obbligatori per la gestione degli accessi ai sistemi informativi, alle applicazioni, alle strutture fisiche e agli asset informativi dell'organizzazione.

1.2 Garantisce che gli accessi siano concessi in base alle esigenze aziendali, al ruolo lavorativo e al profilo di rischio, applicando principi quali il privilegio minimo, il need-to-know e la segregazione dei compiti (SoD).

1.3 La politica supporta l'attuazione della clausola 5.15 della ISO/IEC 27001:2022 e dei controlli correlati che disciplinano l'accesso logico e fisico, l'autenticazione degli utenti e la gestione del ciclo di vita degli accessi.

1.4 La presente politica costituisce il fondamento per la protezione delle risorse digitali e fisiche da uso non autorizzato, abuso o compromissione.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti gli utenti, sistemi e strutture inclusi nel campo di applicazione del SGSI, compresi:

2.1.1 dipendenti, collaboratori esterni, fornitori e personale temporaneo

2.1.2 infrastrutture on-premise, sistemi ospitati in cloud e ambienti ibridi

2.1.3 tutti gli asset aziendali, inclusi hardware, software, dati e aree fisiche sicure

2.1.4 accesso logico (ad es. sistemi, reti, applicazioni, API) e accesso fisico (ad es. edifici, data center)

2.2 Essa disciplina l'accesso per l'intero ciclo di vita dell'identità e dell'interazione con le risorse, dall'onboarding e dal provisioning degli accessi fino ai cambi di ruolo e alla cessazione.

2.3 La politica copre inoltre i contesti Bring Your Own Device (BYOD) e di accesso remoto (VPN, gestione dei dispositivi mobili), assicurando che i controlli siano coerenti tra sedi e modelli di proprietà dei dispositivi.

3. Obiettivi

3.1 Attuare controlli di accesso sicuri e basati sui ruoli che supportino l'integrità operativa e la conformità normativa.

3.2 Garantire che i diritti di accesso siano approvati, monitorati e revocati in modo appropriato e tempestivo.

3.3 Prevenire accessi non autorizzati, elevazioni di privilegio o il mantenimento di diritti di accesso non più appropriati.

3.4 Supportare i principi Zero Trust negando per impostazione predefinita l'accesso, salvo approvazione e giustificazione esplicite.

3.5 Fornire assurance ad auditor e parti interessate mediante riesami degli accessi basati su evidenze, anche automatizzati, e mediante l'applicazione della politica.

3.6 Integrare il controllo degli accessi nei processi aziendali, negli eventi del ciclo di vita HR e nelle architetture tecniche.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la politica di controllo degli accessi e assicura risorse economiche e personale adeguati per la sua attuazione.

4.1.2 Riesamina i rischi relativi al controllo degli accessi nell'ambito del riesame della direzione e assegna le responsabilità a livello strategico.

4.2 Chief Information Security Officer (CISO) / Responsabile del SGSI

4.2.1 È responsabile del framework di controllo degli accessi e ne assicura l'allineamento con la ISO/IEC 27001 e gli standard correlati.

4.2.2 Coordina l'attuazione della politica, il test dei controlli, le azioni correttive e la reportistica sulle metriche del controllo degli accessi.

4.2.3 Supervisiona la modellazione degli accessi basata sul rischio e monitora eventuali carenze di controllo di natura sistemica.

[... 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 Trigger e frequenza del riesame

9.1.1 La presente politica deve essere riesaminata:

9.1.1.1 annualmente, oppure

9.1.1.2 a seguito di modifiche rilevanti dell'infrastruttura informatica, dei requisiti normativi o del profilo di rischio

9.1.1.3 dopo incidenti che evidenzino debolezze nei controlli di accesso

9.1.1.4 quando intervengono cambiamenti significativi nelle tecnologie di autenticazione o nelle piattaforme di identità

9.2 Autorità e processo di riesame

9.2.1 Il Chief Information Security Officer (CISO) o il responsabile SGSI designato deve gestire il ciclo di riesame, includendo:

9.2.1.1 risultanze dell'audit interno

9.2.1.2 risultati e metriche del riesame degli accessi

9.2.1.3 aggiornamenti legali e normativi

9.2.1.4 modifiche alle piattaforme tecnologiche

9.2.2 Tutte le revisioni devono essere approvate dalla Direzione aziendale e comunicate a tutte le parti interessate.

9.2.3 Agli utenti interessati può essere richiesto di rinnovare la presa visione della politica in caso di aggiornamenti sostanziali.

9.3 Controllo delle versioni e documentazione

9.3.1 La versione master deve essere conservata nel repository documentale del SGSI con i seguenti metadati:

9.3.1.1 numero di versione e registro delle modifiche

9.3.1.2 data di entrata in vigore e data del riesame successivo

9.3.1.3 titolare e autorità approvativa

9.3.1.4 distribuzione e registrazioni di presa visione

9.3.2 Le versioni superate devono essere archiviate e rese accessibili per almeno 3 anni.

10. Politiche correlate e collegamenti

10.1 La presente politica dipende funzionalmente dalle seguenti politiche e deve essere interpretata congiuntamente ad esse:

10.1.1 P01 – Politica per la sicurezza delle informazioni: definisce l'impegno dell'organizzazione in materia di sicurezza e le aspettative di alto livello sul controllo degli accessi.

10.1.2 P03 – Politica di uso accettabile: definisce le condizioni comportamentali per l'accesso e la responsabilità degli utenti per l'uso corretto dei sistemi.

10.1.3 P05 – Politica di gestione delle modifiche: disciplina le modalità con cui le modifiche alle configurazioni di accesso, ai ruoli o alle strutture di gruppo devono essere attuate e sottoposte a test in sicurezza.

10.1.4 P07 – Politica di onboarding e cessazione del personale: regola l'avvio e la revoca degli accessi in conformità agli eventi del ciclo di vita dell'utente.

10.1.5 P11 – Politica di gestione degli account utente e dei privilegi: rende operativi i controlli a livello di account e integra la presente politica con linee guida tecniche per l'applicazione del controllo degli accessi.

10.2 Nel loro insieme, tali politiche forniscono un framework di governance degli accessi coerente e applicabile in tutte le unità aziendali e nelle diverse tecnologie.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:2022:

11.1.1 Clausola 5.15 – Controllo degli accessi: la presente politica soddisfa il requisito di controllare l'accesso alle informazioni e agli altri asset associati, sulla base delle esigenze aziendali e dei requisiti di sicurezza delle informazioni.

11.1.2 Clausola 5.17 – Gestione delle identità e clausola 5.18 – Informazioni di autenticazione: tali requisiti sono resi operativi attraverso il provisioning delle identità, i meccanismi di autenticazione e l'assegnazione dei privilegi.

11.1.3 Controlli dell'Allegato A 8.2 (Access rights) e 8.3 (Information access restriction): costituiscono il fondamento degli obiettivi di controllo della presente politica, inclusi l'accesso basato sui ruoli, l'integrazione del ciclo di vita dell'identità e la protezione degli accessi privilegiati.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Famiglia AC (da AC-1 ad AC-20): la presente politica supporta i requisiti NIST in materia di controllo degli accessi per sistemi sia fisici sia logici, inclusi definizione della policy (AC-1), gestione degli account (AC-2) e segregazione dei compiti (AC-5).

11.2.2 Famiglia IA (da IA-1 a IA-8): fornisce indicazioni per l'autenticazione dell'identità, la protezione delle credenziali e l'MFA.

11.2.3 AU-2, AU-12: i requisiti di logging e audit applicati ai sensi della presente politica supportano l'accountability degli utenti e le indagini sugli incidenti.

11.2.4 PE-2 fino a PE-6: riguardano le restrizioni di accesso fisico, che la presente politica applica in parte mediante badge di accesso agli edifici e relative autorizzazioni.

11.3 GDPR UE (2016/679):

11.3.1 Articolo 5(1)(f): i dati personali devono essere protetti dall'accesso non autorizzato. La presente politica assicura l'applicazione tecnica e procedurale di tale principio.

11.3.2 Articolo 32(1)(b): richiede l'attuazione di controlli di accesso, pseudonimizzazione e cifratura per prevenire il trattamento non autorizzato dei dati personali.

11.3.3 Considerando 39: impone la minimizzazione dell'accesso ai dati personali, applicata nella presente politica attraverso il principio del privilegio minimo e i requisiti di giustificazione dell'accesso.

11.4 Direttiva NIS2 UE (2022/2555):

11.4.1 Articolo 21(2)(c–e): la presente politica consente l'adozione di misure tecniche e organizzative per il controllo degli accessi, l'autenticazione degli utenti e la protezione degli asset presso soggetti essenziali e importanti.

11.5 DORA UE (2022/2554):

11.5.1 Articolo 6: richiede politiche di gestione del rischio ICT che includano espressamente la gestione degli accessi degli utenti e i controlli sul ciclo di vita dell'identità. La presente politica soddisfa tale requisito per i settori finanziario e dei servizi ICT.

11.5.2 Articolo 9(2): la presente politica supporta l'applicazione di controlli di accesso robusti nell'ambito della gestione dei servizi ICT di terze parti e infragruppo.

11.6 COBIT 2019:

11.6.1 APO07 Gestire le risorse umane: applica controlli di onboarding e offboarding a supporto della governance degli accessi.

11.6.2 BAI03 – Gestione dell'identificazione e dello sviluppo delle soluzioni: integra i requisiti di controllo degli accessi nella progettazione dei sistemi e nei processi di cambiamento.

11.6.3 DSS01 – Managed Operations e DSS05 – Managed Security Services: disciplinano l'applicazione delle restrizioni di accesso logico e il monitoraggio delle violazioni.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: supporta i meccanismi di audit e assurance per la convalida dell'efficacia del controllo degli accessi.