					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P04S					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 a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 5	
ISO/IEC 27002:2022	Controlli: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 fino ad AC-5	
GDPR UE	Articolo 32	
NIS2 UE	Articolo 21(2)(b)	
DORA UE	Articolo 9	
COBIT 2019	APO07, DSS01	

1. Finalità

1.1. La presente politica definisce le modalità con cui l'organizzazione gestisce l'accesso a sistemi, dati e strutture, al fine di garantire che solo i soggetti autorizzati possano accedere alle informazioni in base alle esigenze operative.

1.2. Essa stabilisce regole chiare per l'assegnazione, la modifica, il monitoraggio e la revoca degli accessi degli utenti, al fine di ridurre al minimo il rischio di accessi non autorizzati e supportare la conformità alle leggi e alle norme applicabili.

1.3. La politica applica il principio del minimo privilegio, richiedendo che l'accesso sia limitato allo stretto necessario per lo svolgimento delle mansioni lavorative.

2. Ambito di applicazione

2.1. La presente politica si applica a tutte le persone che utilizzano o gestiscono l'accesso ai sistemi IT, alle reti, ai dati o alle strutture dell'organizzazione, inclusi:

2.1.1. Dipendenti

2.1.2. Collaboratori esterni

2.1.3. Lavoratori temporanei

2.1.4. Fornitori esterni di servizi IT

2.2. La politica si applica all'accesso a:

2.2.1. Applicazioni aziendali, condivisioni di file e database

2.2.2. Sistemi di posta elettronica, VPN e accesso remoto

2.2.3. Servizi cloud utilizzati per finalità aziendali

2.2.4. Accesso fisico a strutture sicure, quali uffici o sale server

2.3. La presente politica si applica a tutti i dispositivi (aziendali o BYOD approvato), alle piattaforme e alle sedi.

3. Obiettivi

3.1. Garantire che i diritti di accesso siano concessi solo a seguito di approvazione formale, sulla base del ruolo e di una giustificazione operativa.

3.2. Prevenire accessi non autorizzati o eccessivi a dati sensibili, sistemi o infrastrutture.

3.3. Definire procedure chiare per l'assegnazione, la modifica e la revoca dell'accesso degli utenti.

3.4. Richiedere riesami periodici degli accessi e la registrazione automatica o manuale delle evidenze di audit a supporto delle verifiche.

3.5. Supportare l'attuazione tecnica delle restrizioni di accesso mediante configurazione e monitoraggio.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. Approva la presente politica e garantisce la disponibilità delle risorse necessarie per attuare un controllo degli accessi efficace.

4.1.2. Approva le eccezioni e riesamina annualmente gli esiti degli audit sugli accessi.

4.2. Responsabile IT / Fornitore esterno di supporto IT

4.2.1. Gestisce l'assegnazione, la modifica e la revoca degli account utente.

4.2.2. Mantiene un registro del controllo degli accessi contenente tutte le attività svolte (creazioni, modifiche, rimozioni).

4.2.3. Implementa il controllo degli accessi basato sui ruoli (RBAC) e applica un'autenticazione forte (ad es. MFA).

4.2.4. Riesamina i log di accesso per individuare attività sospette e segnala eventuali anomalie al Direttore generale (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. Riesame annuale della politica

9.1.1. Il Responsabile IT deve riesaminare la presente politica annualmente. Qualsiasi cambiamento del contesto legale, tecnico od organizzativo deve comportare un aggiornamento immediato.

9.2. Fattori che attivano il riesame

9.2.1. La politica deve inoltre essere riesaminata se si verifica una delle seguenti condizioni:

9.2.2. Modifiche rilevanti ai sistemi o migrazioni al cloud

9.2.3. Modifiche ai ruoli o alla struttura organizzativa

9.2.4. Un incidente di sicurezza delle informazioni che coinvolga accessi non autorizzati

9.2.5. Modifiche normative (ad es. aggiornamenti del GDPR, della NIS2 o del DORA)

9.3. Documentazione e comunicazione delle modifiche

9.3.1. Le revisioni devono essere registrate con storico delle versioni, approvazione del Direttore generale (GM) e comunicate a tutto il personale interessato.

9.4. Accessibilità e formazione

9.4.1. La presente politica deve essere resa disponibile a tutto il personale e la formazione pertinente deve essere erogata nell'ambito dell'onboarding e successivamente con cadenza annuale.

10. Politiche correlate e collegamenti

10.1. La presente politica deve essere applicata in coordinamento con le seguenti politiche SME per garantire la piena attuazione di pratiche sicure di accesso:

10.1.1. P3S – Politica di uso accettabile: garantisce che gli utenti comprendano i comportamenti consentiti nell'ambito degli accessi concessi.

10.1.2. P5S – Politica di gestione delle modifiche: garantisce che i diritti di accesso siano allineati alle modifiche di sistema approvate.

10.1.3. P7S – Politica di onboarding e cessazione del personale: definisce i punti di attivazione per l'assegnazione e la revoca degli accessi degli utenti.

10.1.4. P17S – Politica di protezione dei dati e privacy: garantisce che i controlli di accesso siano allineati alle misure di protezione dei dati personali.

10.1.5. P30S – Politica di risposta agli incidenti: definisce come vengono gestiti e investigati gli incidenti relativi agli accessi (ad es. uso improprio o violazioni).

11. Norme e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 5.15 – Richiede politiche e processi formalizzati per il controllo degli accessi.

11.2. ISO/IEC 27002

11.2.1. Controlli 5.15–5.17 – Specificano indicazioni dettagliate su controllo degli accessi basato sui ruoli, gestione del ciclo di vita degli utenti e gestione degli accessi privilegiati.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 fino ad AC-5 – Richiedono politiche strutturate per la gestione degli accessi, inclusi autorizzazione degli account, riesame e monitoraggio.

11.4. GDPR UE

11.4.1. Articolo 32 – Richiede controlli tecnici e organizzativi (quali la gestione degli accessi) per garantire la sicurezza e la riservatezza dei dati.

11.5. Direttiva NIS2 UE

11.5.1. Articolo 21(2)(b) – Impone il controllo operativo degli accessi e sistemi di gestione delle identità per prevenire l'accesso non autorizzato ai sistemi.

11.6. DORA UE

11.6.1. Articolo 9 – Sottolinea la gestione sicura dei rischi ICT, incluso un solido controllo degli accessi per i soggetti finanziari.

11.7. COBIT 2019

11.7.1. APO07 Gestire le risorse umane – Richiede responsabilità di accesso definite e applicate.

11.7.2. DSS01 – Gestire le operazioni: include procedure per la gestione degli accessi logici e il mantenimento di ambienti operativi sicuri.