1. Procedura controllo accessi

Procedura controllo accessi

La presente procedura definisce le modalità operative per la gestione e il controllo degli accessi fisici e logici presso GMK SISTEMI S.R.L., in coerenza con i requisiti di sicurezza informatica previsti dalla norma ISO/IEC 27001 (clausole 9.1, 9.2, 10.1) e con l'obiettivo di garantire la qualità e la riservatezza delle informazioni, in linea con la ISO 9001 (clausole 7.1.3, 8.5.1). L'accesso controllato è fondamentale per tutelare le risorse aziendali, i dati sensibili e assicurare la continuità operativa nei processi di commercio all'ingrosso e sviluppo software.

1. Ambito e campo di applicazione

La procedura si applica a tutti i dipendenti, collaboratori esterni, fornitori e visitatori che necessitano di accedere alle sedi operative di GMK SISTEMI S.R.L. e ai sistemi informatici aziendali. Include il controllo degli accessi agli ambienti fisici (uffici, sale server) e agli accessi logici (sistemi informativi, software gestionali, rete aziendale).

2. Responsabilità

Ruolo |

Responsabilità |

Responsabile IT |

Gestione delle credenziali di accesso logico, monitoraggio degli accessi, aggiornamento delle autorizzazioni, gestione incidenti di sicurezza. |

Responsabile Amministrativo |

Gestione degli accessi fisici, registrazione degli ingressi e uscite di personale e visitatori, coordinamento con la sicurezza sul luogo di lavoro. |

Tutti i dipendenti |

Rispetto delle procedure di accesso, segnalazione di anomalie o accessi non autorizzati. |

3. Modalità operative per il controllo accessi

L'accesso fisico agli ambienti aziendali è regolato mediante sistemi di identificazione personale (badge, chiavi elettroniche) e registrazione manuale o automatica degli ingressi. L'assegnazione delle credenziali è subordinata a una valutazione preventiva delle necessità operative e autorizzata dal Responsabile Amministrativo.

Per gli accessi logici, il Responsabile IT assegna account individuali con privilegi commisurati al ruolo e alle responsabilità, applicando il principio del minimo privilegio. Le password devono rispettare criteri di complessità e scadenza periodica, e l'accesso ai sistemi è protetto da autenticazione multifattoriale ove possibile.

4. Gestione delle modifiche e revoca degli accessi

Ogni variazione di ruolo, cessazione del rapporto di lavoro o modifica delle necessità operative comporta la revisione tempestiva delle autorizzazioni di accesso. Il Responsabile IT e il Responsabile Amministrativo collaborano per revocare o aggiornare le credenziali entro 24 ore dalla comunicazione ufficiale, garantendo la tempestività nel mitigare rischi di accesso non autorizzato.

5. Monitoraggio, verifica e indicatori di efficacia

Il monitoraggio degli accessi è effettuato tramite log di sistema e registri fisici, con verifiche periodiche programmate almeno trimestralmente. Gli indicatori di efficacia includono il numero di accessi non autorizzati rilevati, tempi medi di revoca delle credenziali e conformità alle politiche di sicurezza. Eventuali anomalie sono oggetto di analisi e azioni correttive documentate.

6. Registrazioni e documentazione di supporto

Sono mantenuti aggiornati e archiviati i seguenti documenti, che costituiscono evidenza di conformità e supporto alle attività di audit interno ed esterno:

• Registro degli accessi fisici (ingressi/uscite di personale e visitatori);

• Elenco aggiornato delle autorizzazioni di accesso logico e fisico;

• Log di accesso ai sistemi informatici;

• Report periodici di monitoraggio e verifica degli accessi;

• Registro delle modifiche e revoche delle credenziali.

7. Interfacce con altri processi aziendali

La procedura di controllo accessi interagisce con i processi di gestione risorse umane (per la comunicazione tempestiva di variazioni di personale), gestione della sicurezza sul lavoro (per la sicurezza fisica degli ambienti) e gestione della sicurezza delle informazioni (per la protezione dei dati e la continuità operativa). Tali interfacce sono formalizzate e monitorate per garantire coerenza e tempestività nelle azioni.

[Placeholder per diagramma di flusso del processo di controllo accessi, che evidenzia le fasi di richiesta, autorizzazione, assegnazione, monitoraggio e revoca degli accessi.]

8. Audit e miglioramento continuo

Le attività di audit interno includono la verifica della corretta applicazione della procedura di controllo accessi, la completezza e l'accuratezza delle registrazioni e la conformità ai requisiti ISO 9001 e ISO/IEC 27001. Le non conformità rilevate sono gestite secondo la procedura dedicata, con azioni correttive e preventive documentate e monitorate per garantirne l'efficacia.

L'analisi dei dati di monitoraggio e i risultati degli audit costituiscono input fondamentali per il riesame della direzione e per l'aggiornamento continuo delle misure di controllo accessi, in linea con l'evoluzione delle esigenze aziendali e delle minacce alla sicurezza.