1. Procedura controllo accessi

Procedura Controllo Accessi

La presente procedura definisce le modalità operative per la gestione e il controllo degli accessi alle sedi e alle infrastrutture informatiche di DNS Informatica SAS, in conformità ai requisiti delle norme ISO 9001 (clausole 7.1.4 e 8.5.1) e ISO/IEC 27001 (clausole 9.1, 9.2 e A.9). L'obiettivo è garantire la tutela della riservatezza, integrità e disponibilità delle informazioni e dei sistemi, minimizzando i rischi di accessi non autorizzati, in linea con il contesto aziendale e le specificità del settore ICT-IT consultancy and solutions.

1. Ambito di Applicazione

La procedura si applica a tutti i dipendenti, collaboratori esterni, fornitori e visitatori che accedono alle sedi operative di DNS Informatica SAS, in particolare presso la sede legale di via Ticino 51, Romentino (NO) e la sede operativa di via Pietro Micca 3, Trecate (NO). Include l'accesso fisico agli ambienti di lavoro e l'accesso logico ai sistemi informatici e alle infrastrutture di rete gestite dall'azienda.

2. Responsabilità

- Responsabile della Sicurezza delle Informazioni (RSI): supervisiona l'applicazione della procedura, verifica la conformità ai requisiti ISO/IEC 27001 e coordina le attività di audit interne relative al controllo accessi.
- Responsabile Risorse Umane gestisce l'assegnazione e la revoca degli accessi in relazione alle variazioni del personale.
- Responsabile IT: implementa e mantiene i sistemi di controllo accessi logici, garantendo la corretta configurazione e monitoraggio.
- Titolare del trattamento e Direzione: approvano le politiche di accesso e le modifiche alla procedura, assicurando l'allineamento con gli obiettivi di qualità e sicurezza.

3. Modalità Operative

L'accesso fisico alle sedi è regolato mediante sistemi di identificazione personale (badge, chiavi elettroniche o codici di accesso) assegnati in base al principio del minimo privilegio, limitando l'ingresso alle sole aree necessarie per lo svolgimento delle attività lavorative. L'assegnazione degli accessi avviene previa autorizzazione formale del Responsabile di funzione e registrazione nel registro accessi.

Per l'accesso logico ai sistemi informatici, DNS Informatica SAS adotta politiche di autenticazione forte, gestione delle credenziali e controllo degli accessi basato sui ruoli (RBAC). Le password devono rispettare criteri di complessità e scadenza periodica, mentre l'accesso remoto è consentito esclusivamente tramite VPN sicure con autenticazione multifattoriale, in linea con le misure di sicurezza previste dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

4. Gestione delle Autorizzazioni e Revoche

Le richieste di accesso, sia fisico sia logico, devono essere formalizzate attraverso il modulo Richiesta Accesso, compilato dal richiedente e approvato dal Responsabile di funzione. La documentazione è archiviata in formato elettronico e cartaceo, garantendo la tracciabilità delle autorizzazioni. In caso di cessazione del rapporto di lavoro o variazione delle mansioni, il Responsabile Risorse Umane comunica tempestivamente al Responsabile IT e RSI la revoca o modifica degli accessi.

5. Monitoraggio e Verifica

Il sistema di controllo accessi è soggetto a monitoraggio continuo mediante log di accesso fisico e log di sistema informatico. Tali registrazioni sono conservate per un periodo minimo di 12 mesi e sono oggetto di analisi periodica per individuare eventuali anomalie o tentativi di accesso non autorizzato. Le attività di controllo sono integrate nei programmi di audit interni previsti dal SGQ e SGSI (ISO 9001 clausola 9.2, ISO/IEC 27001 clausola 9.1).

Eventuali non conformità rilevate durante le verifiche sono gestite secondo la procedura di gestione delle non conformità e azioni correttive, con registrazione delle evidenze e monitoraggio dell'efficacia delle misure adottate.

6. Registri e Documentazione di Riferimento

Documento/Registro |

Descrizione |

Responsabile |

Conservazione |

Registro Accessi Fisici |

Elenco autorizzazioni e accessi alle sedi aziendali |

Responsabile Risorse Umane |

5 anni |

Registro Accessi Logici |

Log di accesso ai sistemi informatici e infrastrutture |

Responsabile IT |

12 mesi |

Modulo Richiesta Accesso |

Modulo per autorizzazione accessi fisici e logici |

Richiedente / Responsabile di funzione |

5 anni |

Report Audit Controllo Accessi |

Relazioni di audit interne e verifiche di conformità |

RSI / Responsabile Qualità |

5 anni |

7. Indicatori di Prestazione

• Percentuale di accessi autorizzati rispetto alle richieste ricevute.

• Numero di tentativi di accesso non autorizzato rilevati e gestiti.

• Tempo medio di revoca degli accessi dopo cessazione o modifica del personale.

• Risultati delle verifiche di conformità e audit interni sul controllo accessi.

8. Interfacce con Altri Processi

La procedura di controllo accessi interagisce con i processi di gestione delle risorse umane (assunzioni, cessazioni, variazioni), gestione della sicurezza delle informazioni, gestione delle infrastrutture IT e gestione delle non conformità. La corretta integrazione assicura la coerenza e tempestività delle autorizzazioni e revoche, nonché la protezione continua delle risorse aziendali.

Placeholder diagramma di processo: Gestione integrata del controllo accessi fisico e logico con interfacce HR, IT e Sicurezza delle Informazioni.

9. Audit e Miglioramento Continuo

Le attività di audit interno includono la verifica dell'efficacia della procedura di controllo accessi, la conformità alle politiche aziendali e ai requisiti normativi, e l'analisi delle registrazioni di accesso. Le evidenze raccolte sono documentate e utilizzate per identificare opportunità di miglioramento, aggiornare le misure di sicurezza e prevenire rischi futuri, in linea con il ciclo PDCA previsto da ISO 9001 e ISO/IEC 27001.

Eventuali modifiche alla procedura sono gestite tramite il sistema di controllo documentale aziendale, con approvazione formale e comunicazione a tutte le parti interessate.