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 NUBYS S.R.L., 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 protezione delle risorse aziendali, la sicurezza delle informazioni e la continuità operativa, minimizzando i rischi di accessi non autorizzati e garantendo la tracciabilità degli ingressi.

1. Ambito e Applicazione

La procedura si applica a tutti i dipendenti, collaboratori esterni, fornitori e visitatori che necessitano di accedere alle sedi operative di NUBYS S.R.L., in particolare presso l'unità locale di Via Ticino 51, Romentino (NO), e alla rete informatica aziendale. Sono inclusi gli accessi agli ambienti fisici, ai sistemi informativi, alle applicazioni software e alle infrastrutture di rete gestite dall'azienda.

2. Responsabilità

• Responsabile Sicurezza delle Informazioni (RSI): supervisiona l'implementazione della procedura, verifica la conformità e coordina le attività di audit interne relative al controllo accessi.

• Responsabile IT: gestisce le credenziali di accesso ai sistemi informatici, assicura l'aggiornamento delle autorizzazioni e monitora i log di accesso.

• Responsabile Amministrativo: autorizza gli accessi fisici e mantiene il registro degli ingressi e delle uscite di personale e visitatori.

• Tutti i dipendenti e collaboratori: sono tenuti a rispettare le regole di accesso e a segnalare tempestivamente eventuali anomalie o violazioni.

3. Modalità di Controllo Accessi Fisici

L'accesso agli ambienti aziendali è regolamentato mediante sistemi di identificazione personale (badge, chiavi elettroniche o codici di accesso) assegnati individualmente. L'assegnazione e la revoca delle credenziali sono gestite dal Responsabile Amministrativo, in base alle esigenze operative e alle autorizzazioni definite. Ogni accesso è registrato in un apposito registro cartaceo o digitale, contenente data, ora, nominativo e motivo dell'accesso, garantendo la tracciabilità e la verifica periodica (ISO 9001, clausola 8.5.1).

L'accesso ai locali è consentito esclusivamente al personale autorizzato e ai visitatori accompagnati previa registrazione e autorizzazione preventiva. In caso di accessi straordinari o emergenziali, è obbligatorio informare tempestivamente il Responsabile Sicurezza delle Informazioni e documentare l'evento.

4. Controllo Accessi Logici e Sistemi Informativi

L'accesso ai sistemi informativi e alle applicazioni software è regolato da credenziali personali e sistemi di autenticazione robusta, conformemente alle misure di sicurezza previste dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Le autorizzazioni sono assegnate in base al principio del minimo privilegio, limitando l'accesso alle risorse strettamente necessarie per lo svolgimento delle attività lavorative (ISO/IEC 27001, clausola A.9.1).

Il ResponsabileIT mantiene un inventario aggiornato degli utenti e delle relative autorizzazioni, esegue regolari revisioni e revoche tempestive in caso di cessazionedel rapporto di lavoro o variazioni di ruolo. I log di accesso sono monitorati e analizzati per individuare eventuali anomalieo tentativi di accesso non autorizzato, con evidenze documentate e azioni correttive pianificate in caso di non conformità (ISO/IEC 27001, clausola 9.1).

5. Gestione delle Chiavi e Dispositivi di Accesso

Le chiavi fisiche e i dispositivi elettronici per l'accesso sono custoditi in modosicuro e assegnati a personale autorizzato. È prevista una procedura di registrazione e riconsegna, con aggiornamento tempestivo del registro chiavi. In caso di smarrimentoo furto, il ResponsabileAmministrativo deve essere immediatamenteinformato per adottare le misure di sicurezza necessarie, quali la sostituzione delle serrature o la disabilitazione delle credenziali elettroniche.

6. Formazione e Consapevolezza

Tutti i dipendenti e collaboratori ricevono formazione periodica sulle politiche di controllo accessi, sulle procedure operative e sulle responsabilità individuali in materia di sicurezza fisica e informatica. La formazione include l'illustrazione delle conseguenzedi accessi non autorizzati e delle modalitàdi segnalazione di eventi sospetti, in linea con i requisiti di ISO 9001 (clausola 7.2) e ISO/IEC 27001 (clausola 7.3).

7. Monitoraggio, Verifica e Audit

Il sistema di controllo accessi è oggetto di monitoraggiocontinuo e di audit interni programmati,con verifica della conformità alle procedure e alle autorizzazioni. Gli indicatori di performance includono il numerodi accessi autorizzati, le anomalieriscontrate, i tempi di risposta alle segnalazioni e le azioni correttive implementate.Le evidenze raccolte durante gli audit costituiscono documentazionedi supporto per la direzione e per eventuali verifiche esterne.

Eventuali non conformità rilevate sono gestite tramite il processo di gestione delle non conformità e miglioramentocontinuo previsto dal Sistema di Gestione Integrato, con analisi delle cause, definizione di azioni correttive e verifica dell'efficacia.

8. Registri e Documentazione di Controllo Accessi

Registro/Documento |

Descrizione |

Responsabile |

Conservazione |

Periodo di Conservazione |

Registro Accessi Fisici |

Annotazione ingressi e uscite di personale e visitatori |

Responsabile Amministrativo |

Archivio digitale e cartaceo |

5 anni |

Registro Assegnazione Chiavi e Badge |

Gestione e tracciabilità dispositivi di accesso |

Responsabile Amministrativo |

Archivio digitale |

5 anni |

Log Accessi Sistemi Informativi |

Registrazione automatica degli accessi ai sistemi IT |

Responsabile IT |

Archivio digitale protetto |

1 anno |

Report Audit Controllo Accessi |

Verifica periodica conformità e anomalie |

Responsabile Sicurezza delle Informazioni |

Archivio digitale |

5 anni |

9. Interfacce e Integrazione con Altri Processi

La procedura di controllo accessi interagisce con i processi di gestione del personale, sicurezza sul lavoro, gestione incidenti e continuità operativa. In particolare, la tempestiva comunicazione tra il Responsabile Amministrativo, il Responsabile IT e il RSI è fondamentale per garantire la coerenza delle autorizzazioni e la gestione dei rischi associati agli accessi. La procedura supporta inoltre le attività di valutazione del rischio e di miglioramento continuo del Sistema di Gestione Integrato.

[Placeholder per diagramma di flusso del processo di controllo accessi: assegnazione credenziali, registrazione accessi, monitoraggio, audit e gestione non conformità.]