**PROTOCOLLO OPERATIVO N. 8**

**GESTIONE SISTEMI INFORMATIVI**

**1. Obiettivo e ambito di applicazione.**

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di condotta e di controllo a cui tutto il personale di Segrate Servizi, a qualsiasi titolo coinvolto nel processo di gestione dei sistemi informatici aziendali, deve attenersi.

Il presente documento si applica con particolare riferimento al personale addetto alla gestione dei sistemi informativi, nonché al personale che faccia uso degli stessi nello svolgimento delle proprie attività lavorative e per tali si intendono:

* coloro i quali abbiano avuto assegnati utenze (User id) e password, anche non esclusive, per accedere al sistema informatico aziendale;
* coloro i quali utilizzano software della Pubblica Amministrazione (SSN, INPS, INAIL ecc.);
* coloro i quali si occupano della manutenzione e sviluppo dei sistemi informativi, fornendo attività di assistenza tecnica e funzionale dei server, delle applicazioni, dei client e delle reti di telecomunicazione.

Il presente documento, in particolare è volto a garantire il rispetto dei principi di trasparenza, correttezza, segregazione delle funzioni, verificabilità e tracciabilità delle operazioni.

**2. Riferimenti.**

* D.Lgs. 231/2001;
* Codice di Comportamento Integrativo dei dipendenti del Comune di Segrate;
* Modello di Organizzazione, gestione e controllo ex. D.Lgs. 231/2001 e allegato Codice Etico;
* Protocollo operativo n. 1 "Approvvigionamento di forniture, servizi e lavori".

**3. Funzioni aziendali coinvolte.**

Il processo di gestione in esame prevede il coinvolgimento, secondo le rispettive competenze, delle seguenti funzioni aziendali:

* Amministratore Unico o Presidente della Società;
* Coordinatore della Società;
* Direttori di Farmacia;
* Coordinatore/Direttore dei singoli servizi;
* tutti i soggetti muniti di User Id e password.

**4. Principi generali di condotta.**

Il personale della Società, a qualsiasi titolo coinvolto nel processo in esame, è tenuto ad osservare il presente protocollo, i regolamenti interni aziendali, le previsioni di legge esistenti in materia e le norme comportamentali richiamate nel Codice Etico e nel Modello adottati dalla Società.

Il personale della Società deve garantire il rispetto dei seguenti principi:

* il personale aziendale deve attenersi rigorosamente alle istruzioni dalla Società in materia di gestione dei sistemi informativi facendone un uso appropriato rispetto alle previsioni normative;
* custodire i codici identificativi assegnati, astenendosi dal comunicarli a terzi non autorizzati;
* ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate, che devono essere utilizzate esclusivamente per l'espletamento delle attività lavorative; tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
* astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati della Società e di soggetti terzi (Enti pubblici e fornitori) contenuti nel sistema informatico;
* astenersi da qualsiasi condotta diretta ad aggirare le protezioni del sistema informatico della Società o altrui.

Inoltre:

* ogni dipendente/amministratore del sistema è tenuto a segnalare al Responsabile Sistemi informativi l'eventuale esistenza di "virus" e segnalare eventuali incidenti di sicurezza;
* ogni dipendente/amministratore del sistema deve evitare di utilizzare password di altri utenti della Società, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
* nel caso di attività di gestione dei sistemi informativi e del patrimonio informativo conferite a soggetti terzi/outsourcer, tali soggetti devono impegnarsi per iscritto ad operare nel rispetto della normativa vigente, nonché delle prescrizioni del Codice Etico adottato dalla Società.

In particolare, è fatto divieto:

* modificare e/o cancellare, distruggere, danneggiare, dati o documenti informatici, pubblici o privati;
* accedere abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;
* accede al sistema informatico o telematico, o a parti di esso, ovvero a banche dati, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
* svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
* istallare apparecchiature per l’intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
* svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
* svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
* distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
* installare e/o modificare componenti hardware o utilizzare strumenti software e/o hardware atti a distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l’integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente Pubblico o ad essi pertinenti o comunque di pubblica utilità;
* introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
* detenere, procurarsi, riprodurre, o diffondere abusivamente codici d’accesso o comunque mezzi idonei all’accesso ad un sistema protetto da misure di sicurezza;
* procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l’interruzione o l’alterazione del suo funzionamento;
* alterare, mediante l’utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
* produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
* installare programmi provenienti dall’esterno, salvo espressa autorizzazione ed in particolare:
* software (programmi) non approvati e non correlati con l’attività lavorativa espletata;
* software (c.d. “P2P”, di files sharing o di instant messaging) mediante i quali è possibile scambiare con altri soggetti all’interno della rete internet ogni tipologia di file (quali filmati, documentazioni, canzoni, dati etc.), senza alcuna possibilità di controllo da parte della Società;
* software e/o CD privi delle necessarie autorizzazioni/ licenze o supporti sottoposti a licenza d’uso;
* software aziendali in violazioni delle licenze d’uso.

**5. Modalità operative.**

Le procedure di sicurezza per l’accesso ai sistemi computerizzati della Società sono le seguenti:

Password per accesso ai sistemi computerizzati:

**5.1 Nelle farmacie**

I direttori e vice direttori hanno una password dispositiva con la quale possono accedere a tutte le operazioni: vendita/ variazioni di magazzino carico e scarico.

I magazzinieri hanno una password simile a quella dei direttori.

I farmacisti collaboratori e i commessi per hanno una password operativa con la quale possono accedere solo alle vendite.

Ogni password è conosciuta solo da chi la detiene e dalla Direzione Centrale per eventuali verifiche sulla correttezza dell’operato.

Le password vengono cambiate periodicamente con richiesta alla Software house perché possono essere cambiate solo in questo modo, gli operatori non hanno la possibilità di variarla.

**5.2 Negli Uffici**

Ogni operatore per accedere ha una sua password personale. Le password vengono cambiate periodicamente con richiesta alla Software house perché possono essere cambiate solo in questo modo, gli operatori non hanno la possibilità di variarla.

**5.3 Back up**

Il back up viene effettuato in modo automatico tutti i giorni in tutte le sedi della Società con verifica dei Direttori di Farmacia nelle farmacie e dell’ufficio amministrativo in sede.

**5.4 Sistemi anti-virus**

Viene fornito e aggiornato in modo automatico dalla Software House. Firewall esiste in tutte le sedi.

**5.5 Operazioni effettuate online**

Accesso al SISS da parte delle farmacie è possibile solo con inserimento nel lettore card la carta del direttore che comprende la firma elettronica del direttore stesso.

La sede legale dispone di un lettore e di una card per la firma elettronica da parte dell’Amministratore Unico o del Presidente della Società .

L’ufficio amministrativo dispone di un dispositivo di sicurezza per accedere alle operazioni on-line sul conto corrente bancario principale.

**6. Archiviazione.**

Tutta la documentazione prodotta nell'ambito delle attività regolate nel presente protocollo è conservata a cura di ciascun settore per quanto di competenza e messa a disposizione su richiesta dell'Amministratore Unico o del Presidente della Società, del Collegio Sindacale e dell'organismo di vigilanza.

Detti documenti devo essere conservati per un periodo di almeno 10 anni, salvo diverse previsioni legislative.

**7. Flussi informativi all'Organismo di Vigilanza.**

L'Organismo di Vigilanza istituito ai sensi del D.Lgs. 231/2001 vigila sul funzionamento e sull'aggiornamento del Modello di organizzazione, gestione e controllo adottato dalla Società.

A tal fine l’Organismo di Vigilanza potrà richiedere alle funzioni aziendali, a vario titolo coinvolte, di comunicare periodicamente il rispetto delle regole comportamentali nello svolgimento dei compiti assegnati e la predisposizione di specifici e regolari flussi informativi sulla corretta attuazione dei principi di controllo, sanciti nel presente protocollo, secondo le modalità che verranno comunicate dallo stesso Organismo di Vigilanza.

Le funzioni aziendali coinvolte nelle attività regolate nel presente protocollo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi anomalia o eccezione procedurale.