

POLITICA PER LA SICUREZZA

La Casa di Cura Eretenia Spa si impegna a garantire il massimo della riservatezza nel trattamento dei dati personali in applicazione delle misure minime elencate nel regolamento definito nel D.Lgs 196 del 30 giugno 2003.

A questo scopo definisce le seguenti misure per la sicurezza:

1. Attivazione di un sistema di identificazione e autenticazione per gli utenti che hanno accesso alle banche dati informatiche interne tramite password ed account utilizzabile solo in una stazione di lavoro e non utilizzabile da più utenti nemmeno in tempi diversi
2. Gli accessi alle aree classificate come riservate debbono essere autorizzati. Vi potrà accedere solo il personale elencato in apposita circolare interna. Qualsiasi altro accesso dovrà essere autorizzato dalla Direzione e/o dal Responsabile Trattamento dati. Gli accessi interessano anche il personale esterno che effettua operazioni di manutenzione e/o pulizia.
3. L'accesso alle aree protette può essere concesso in via straordinaria senza autorizzazione del responsabile trattamento dati se il personale senza autorizzazione viene accompagnato e rimane sotto la vigilanza dal personale interno incaricato al trattamento dati, personale addestrato sulla politica della sicurezza della presente azienda.
4. Assegnazione di un UserID tramite lettera ufficiale e colloquio individuale alla presenza del rappresentate della Direzione del Responsabile Trattamento dati dopo esecuzione test di verifica apprendimento delle norme sulla sicurezza.
5. Password consegnate agli incaricati al trattamento come al punto precedente e in scadenza ogni sei mesi per i posti di lavoro collegati in rete, ogni anno per i posti di lavoro non collegati in rete. Le password debbono essere composte da minimo 8 caratteri di cui almeno 2 numerici.
6. Le risorse hardware e le aree riservate dovranno essere protette da sistemi di sicurezza attivi e passivi quali password, chiavi di accesso, porte e altri dispositivi tecnici.
7. Il codice sorgente del software sviluppato internamente non potrà essere messo a disposizione di terzi senza l'autorizzazione della Direzione. Ogni personalizzazione effettuata da software house esterne dovrà essere effettuata in presenza dell'Amministratore del Sistema e/o da persona da egli delegata, sotto la loro diretta supervisione.
8. Ogni utente sarà autorizzato all'accesso delle risorse, dati e/o informazioni in base al profilo utente definito dall'amministratore del sistema. Non sono concessi altri accessi al di fuori dell'elenco consegnato.
9. Tutti i file di log potranno essere consultati solo dall'Amministratore di Sistema e dal responsabile trattamento dati che, con periodicità settimanale, provvederanno all'archiviazione di questi file e all'analisi degli eventi procedendo ad eventuale relazione alla Direzione in caso di grave violazione delle regole di sicurezza da parte dell'utenza.
10. Tutti i tentativi di intrusione dovranno essere monitorati ed immediatamente segnalati all'Amministratore di Sistema.
11. Nomina di un Amministratore di Sistema e di un Responsabile trattamento dati che si incaricherà di monitorare e mantenere efficiente il sistema di sicurezza adottato.
12. Adeguata istruzione agli utenti sugli obblighi e sulle regole di sicurezze attivate nella Casa di Cura Eretenia Spa.
13. Attivazione e aggiornamento dei programmi antivirus, spyware e antispamming installati.
14. Aggiornamento periodico dei sistemi operativi alle versioni più recenti al fine di mantenere alto il livello tecnologico e di conseguenza la sicurezza intrinseca del software di sistema.
15. Controllo sull'operato delle software house esterne e dello sviluppo software interno avvalendosi anche della consulenza di terzi.
16. Rilevazione tempestiva di eventuali incidenti di sicurezza.
17. Monitoraggio annuale delle attività di rete e della singola stazione di lavoro.

18. Attivazione di un Audit annuale delle attività dell'utenza per la verifica nel tempo dell'efficacia del sistema di sicurezza adottato.
19. Verifica periodica della sussistenza delle condizioni che hanno portato alla concessione delle autorizzazioni d'accesso agli archivi contenenti dati personali sensibili.
20. Adeguamento dei locali dal punto di vista tecnico ed organizzativo per la protezione delle aree interessate dalle misure di sicurezza
21. Monitoraggio giornaliero delle attività di backup.
22. Attivazione di un sistema di manutenzione ordinaria e straordinaria del sistema informativo per ridurre al minimo i tempi di disservizio.
23. Manutenzione e aggiornamento di un elenco dettagliato delle risorse hardware e software per la definizione del livello di criticità del singolo elemento.
24. Elenco dettagliato delle basi dati gestite e definizione del loro livello di criticità.
25. Definizione di un Piano di Continuità Operativa per garantire nel tempo la continuità del servizio informatico limitando i danni al patrimonio informativo a fronte di una emergenza.
26. Il personale autorizzato all'accesso ad informazioni personali sensibili è stato opportunamente addestrato a rispettare le regole di riservatezza minime: rispetto della dignità dell'interessato; attenzione, nei colloqui o nella raccolta di informazioni per l'anamnesi, evitando di far conoscere a terzi informazioni sullo stato di salute del paziente; far rispettare le distanze di cortesia nel rispetto dei canoni di riservatezza; modalità specifiche di comunicazione a terzi di informazioni riservate; eliminazione dove possibile di tutte le informazioni che possano mettere in correlazione il paziente e l'indicazione della struttura, reparto o esame eseguito; comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico.