INDICE

PREMESSA

Le misure di sicurezza tecniche ed organizzative contrastano i rischi di distruzione, perdita, trattamento non consentito o illecito dei dati personali, nonché la loro modifica, accesso divulgazione non autorizzati.

Le misure di sicurezza, applicate alle risorse tecniche, informatiche devono assicurare la resilienza dei sistemi, ovvero la loro capacità di resistere nel tempo alle minacce.

Inoltre le misure organizzative contrastano le minacce, intenzionali o involontarie, proventi dal comportamento delle persone o dai loro errori.

In particolare i sistemi informatici, telematici e le reti d'informazione sono sottoposti a costanti rischi interni ed esterni. A causa dell'interconnessione e dell'interdipendenza tra sistemi, le falle in materia di sicurezza su un componente del sistema possono propagare i loro effetti fino ad incidere gravemente sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi e arrecare danni ad altri sistemi.

Le misure di sicurezza tengono conto della natura dei dati, delle specifiche caratteristiche del trattamento e delle conoscenze acquisite in base al progresso tecnico.

Ai trattamenti sono applicate le misure di sicurezza anche in riferimento alle normative in materia di tutela contro la criminalità informatica: la loro omissione è punita penalmente, in quanto vi si applica la forma della responsabilità per l'esercizio di attività pericolose.

M01 SISTEMA DI AUTENTICAZIONE INFORMATICA

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, ai sistemi ed applicativi di elaborazione dei dati, alle banche dati.

La procedura di autenticazione permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso dei diritti di accesso ad un determinato strumento e/o banca dati.

L'accesso alle risorse informatiche è consentito ai soli soggetti autorizzati.

Il sistema è attivo, gestito dal Sistema Operativo, sul PC Desktop.

M02 SISTEMA DI AUTORIZZAZIONE

Il sistema di autorizzazione informatica viene adottato al fine di circoscrivere l'acceso alle tipologie di banche dati informatiche ai quali i soggetti autorizzati possono accedere.

Alla data dei redazione del presente documento, stante la struttura organizzativa che vede l'impiego di una unica postazione informatica Personal Computer senza il ricorso ad archivi centralizzati accessibili da più utenze, non sussiste la necessità di definire profili di autorizzazione. Inoltre i dati memorizzati sul PC sonno accessibili in modo paritetico tra gli utenti dotati delle credenziali di autenticazione.

M03 SISTEMI DI PROTEZIONE DI AREE E LOCALI

Gli ingressi all'ufficio sono consentiti previa identificazione dei visitatori.

Il trattamento avviene in locali accessibili al solo personale autorizzato. Le porte sono chiuse con serratura quando i locali non sono presidiati.

M04 SISTEMI DI PROTEZIONE INFORMATICA

Cooperativa Sociale Il talento adotta e mantiene in efficienza sistemi e dispositivi di protezione contro gli accessi abusivi ai sistemi informatici e telematici (art. 615-ter c.p.) e contro i il rischi di intrusione e dell'azione di programmi e sistemi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.). I principali sistemi implementati sono:

SISTEMA	PROTEZIONE
FIREWALL	Firewall di sistema su Sistema Operativo dei Personal Computers , attivi per il controllo e registrazione su file di LOG, di tutte le attività di comunicazione di rete, intervenendo su quelle anomale (tentativi di intrusione o azione di codici e software pericolosi).
ANTIVIRUS / ANTIMALWARE	Antivirus di Sistema del PC Desktop, per il controllo in tempo reale e programmato dei files ricevuti, trasmessi e memorizzati, raffrontandoli con le più note minacce ("firme") e avvisando l'utente sull'azione da compiere e/o disattivando preventivamente la minaccia (cancellazione o, messa in "quarantena"). Il sistema è aggiornato automaticamente con le firme più recenti, rese disponibili dal produttore
AGGIORNAMENTI PERIODICI	prevenzione della la vulnerabilità di strumenti elettronici e correzione dei difetti: • dei Sistemi Operativi dei Personal Computer collegati alla rete informatica, • degli antivirus • degli software di navigazione Internet Gli aggiornamenti di sicurezza sono automatici oppure programmati con cadenza almeno

semestrale

M05 CRITERI E MODALITÀ DI RIPRISTINO DEI DATI

Al fine di garantire la disponibilità e l'integrità dei dati contro i rischi di distruzione o perdita, sono previste procedure di backup per i dati trattati con strumenti elettronici, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema informatico, su idonei dispositivi.

I backup sono effettuati periodicamente, almeno settimanalmente, su dispositivo di memorizzazione di massa USB a cura del presidente.

M06 REIMPIEGO E SMALTIMENTO DI SUPPORTI

Tutti i supporti di memorizzazione riutilizzabili contenenti dati personali devono essere trattati con particolare cautela: in previsione del reimpiego o dello smaltimento dei supporti, oppure al termine del loro ciclo di utilizzo, questi sono consegnati all'Amministratore di Sistema che adotterà le procedure necessarie per cancellare in sicurezza ogni informazione contenuta, prima di autorizzarne il reimpiego o prima di procedere allo smaltimento degli stessi, attraverso procedure di:

- *wiping* o formattazione *low level* in caso di reimpiego
- distruzione dei supporti mediante punzonatura, deformazione, disintegrazione fisica o demagnetizzazione in caso di smaltimento

M07 CIFRATURA DEI DATI

Non sono adottati sistemi di cifratura.

M08 FORMAZIONE

Gli interventi formativi, le istruzioni e gli aggiornamenti sono programmati in modo tale da avere luogo al verificarsi di almeno una delle seguenti circostanze:

- al momento dell'implementazione del Sistema di Gestione Privacy
- in occasione di cambiamenti organizzativi, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali
- in occasione della individuazione di rischi che possano compromettere la sicurezza, l'integrità, la riservatezza e la disponibilità dei dati personali
- necessità di aggiornamento a nuove leggi, regolamenti, linee guida ecc.

La formazione viene eseguita mediante:

- formazione diretta (corsi in aula o eventi formativi)
- consegna di un set informativo con procedure e materiali didattici di auto-formazione

La formazione è integrata con strumenti di divulgazione quali, ad esempio, seminari tematici, e-mail di aggiornamento, circolari e note informative.

M09 DISCIPLINARE UTILIZZO DEGLI STRUMENTI INFORMATICI

Stante l'attuale struttura organizzativa che non prevede personale dipendente o collaboratori cui sono assegnati strumenti informatici da cui possa derivare un controllo sulle attività non si è ritenuto di redigere il Disciplinare utilizzo strumenti informatici.

M10 GESTIONE DEI DOCUMENTI E DEGLI ARCHIVI CARTACEI

I documenti contenenti dati personali di qualsiasi natura sono soggetti a misure di custodia e salvaguardia in accordo a quanto descritto nella procedura di riferimento, ove sono riportate le modalità di protezione, di accesso e di trattamento.

L'accesso e la gestione di documenti contenenti di dati sensibili o dati giudiziari è determinato sulla base delle autorizzazioni assegnate dal Titolare del trattamento ai soggetti autorizzati.

L’autorizzazione all’accesso è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento. Periodicamente è verificata la sussistenza dei criteri di autorizzazione all'accesso ed delle condizioni per la conservazione dei documenti.

DOCUMENTO	8.4PRD_M10	Procedura di gestione dei documenti contenenti dati personali