

Documento Programmatico sulla sicurezza

Redatto ai sensi dell'articolo 34, comma 1, lettera g)
e Allegato B - Disciplinare Tecnico, Regola 19
del Decreto legislativo 30 Giugno 2003 n.196
"Codice in materia di protezione dei dati personali"

Firma del Titolare del trattamento dei dati:

Firma del Responsabile del trattamento dei dati:

Data redazione documento _____

Scopo del documento

Scopo di questo documento è delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche adottate e da adottare per il trattamento dei dati personali effettuato dal titolare e dal responsabile dei dati (se nominato)

Premessa

Il presente documento, in ottemperanza alle prescrizioni del D.Lgs. n. 196/2003 ("Codice della Privacy"), individua le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema informatico descritto nel presente documento deve ritenersi sicuro in quanto strutturato secondo quanto previsto e richiesto dalla normativa per garantire la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

Conformemente a quanto prescrive il punto 19. del Disciplinare Tecnico, allegato sub b) al D.Lgs. 196/2003, la stesura del presente documento è aderente alle seguenti linee guida:

1. l'elenco dei trattamenti di dati personali effettuato;
2. l'analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento;
3. l'individuazione e la valutazione dei rischi che incombono sui dati;
4. l'individuazione delle misure preventive e correttive, già adottate o da adottare, per garantire l'integrità e la disponibilità dei dati nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei dati o degli strumenti elettronici,
6. l'individuazione di istruzioni agli incaricati e la previsione di un programma formativo;
7. i criteri da adottare per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
8. i criteri di cifratura o separazione dei dati

ANAGRAFICA

Titolare del trattamento dei dati

Domicilio Fiscale

Indirizzo: _____

Sede professionale dove avviene il trattamento dei dati

Indirizzo: _____

Codice fiscale: _____

Partita IVA : _____

Tipo di attività professionale esercitata

Medico di medicina generale

Dati ASL

ASL riferimento _____

Tipologia organizzativa

Studio singolo ☐

Studio associato ☐

Medicina in rete ☐

Medicina in Gruppo ☐

Responsabile del trattamento dei dati

(se diverso dal titolare)

Cognome e nome

Data nomina per iscritto

Collaboratori/dipendenti

Nome

Ruolo

Tratta i dati

☐ si

☐ No

Nome

Ruolo

Tratta i dati

☐ si

☐ No

Tipologia del trattamento dei dati

Schedario cartaceo

☐

Solo strumenti elettronici

☐

INFORMAZIONI SUL SISTEMA INFORMATIVO BACKUP E RIPRISTINO DEI DATI

Numero di computer utilizzati

Di cui collegati ad Internet N°:

Copie di sicurezza

Le copie di sicurezza dei dati sono effettuate su:
tutti i Pc

☐ sì☐ no

solo sul server

☐

Le copie di sicurezza dei dati sono effettuate con periodicità:

Giornaliera

☐

Settimanale

☐

Mensile

☐

Altro

☐

Il sistema operativo dei PC è aggiornato periodicamente con le patch fornite dal produttore?

☐ sì☐ no

Ripristino dei dati

Periodicità delle prove di ripristino dei dati:

Settimanale

☐

Mensile

☐

Altro

☐

TIPOLOGIA DEI DATI TRATTATI

Elenco dei trattamenti

Titolare

☐ personali☐ identificativi☐ sensibili

1° Dipendente

☐ personali☐ identificativi☐ sensibili

2° Dipendente

☐ personali☐ identificativi☐ sensibili

SICUREZZA ALL'ACCESSO DEI DATI (Obbligatoria)

Accesso dei dati al computer principale

L'accesso ai dati custoditi sul computer principale è coperto da chiavi personali

USERID ☐ sì
☐ no

Password ☐ sì
☐ no

Accesso dei dati agli altri computer

E' necessario fornire USERID e PASSWORD su tutti i PC ☐ sì
☐ no

Modifica delle password

Giornaliera ☐
Settimanale ☐
Mensile ☐
Altro ☐

Tipologia delle password

Diverse per ogni operatore/collaboratore ☐ sì
☐ no

La password è lunga almeno 8 caratteri ☐ sì
☐ no

Antivirus

Il PC principale dispone di un software antivirus ☐ sì
☐ no

Gli altri PC dispongono di un software antivirus ☐ sì
☐ no

Il sistema antivirus è aggiornato con le patch fornite dal produttore

Giornaliera ☐
Settimanale ☐
Mensile ☐
Altro ☐

Sistemi firewall

I sistemi sono protetti da firewall? ☐ sì
☐ no

Posta elettronica

- | | |
|-------------------------------|-----------------------------|
| Utilizzo la posta elettronica | <input type="checkbox"/> si |
| | <input type="checkbox"/> no |
| su tutti i Pc | <input type="checkbox"/> si |
| | <input type="checkbox"/> no |
| solo sul Pc principale | <input type="checkbox"/> |

SICUREZZA FISICA DEI LOCALI (Facoltativi)

I locali sono dotati di :

- | | |
|---------------------|-----------------------------|
| Porta blindata | <input type="checkbox"/> si |
| | <input type="checkbox"/> no |
| Tapparelle blindate | <input type="checkbox"/> si |
| | <input type="checkbox"/> no |

Gli armadi / cassetti

- Gli armadi ed i cassetti dove sono custoditi i dati su supporto cartaceo sono dotati di serratura
- | |
|-----------------------------|
| <input type="checkbox"/> si |
| <input type="checkbox"/> no |

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (Facoltativi)

Analisi dei rischi

- | Tipologia | Livello Rischio |
|--|---|
| RISCHI AMBIENTALI
(incendio, terremoto, inondazione) | <input type="checkbox"/> basso
<input type="checkbox"/> medio
<input type="checkbox"/> alto |
| RISCHI ORGANIZZATIVI
(furto, uso illegittimo dei dati) | <input type="checkbox"/> basso
<input type="checkbox"/> medio
<input type="checkbox"/> alto |
| RISCHI FISICI
(danneggiamento volontario, involontario, guasti interruzione d'uso) | <input type="checkbox"/> basso
<input type="checkbox"/> medio
<input type="checkbox"/> alto |
| RISCHI LOGICI
(accesso esterni non autorizzati, azione virus, cancellazione dati, invio e-mail a indirizzi sbagliati) | <input type="checkbox"/> basso
<input type="checkbox"/> medio
<input type="checkbox"/> alto |