Allegato alla Delibera n. 221 del 26/03/2010

# DPS

## Documento Programmatico sulla Sicurezza
## Redatto ai sensi e per gli effetti dell'art. n. 34, c.1, lettera g) del D.Lgs. n.196/2003 e del relativo disciplinare tecnico.

# Azienda Sanitaria Provinciale di Palermo

Via G. Cusmano 24,
90141 Palermo

Aggiornamento 31 marzo 2010

# Indice

pagina

**1. Premessa al Documento Programmatico sulla Sicurezza** 3
1.1 Scopo del documento
1.2 Titolare del trattamento
1.3 Responsabile del Trattamento
1.4 Incaricato del Trattamento
**2. Principali Riferimenti Legislativi** 5

**3. Identificazione delle Risorse da Proteggere** 9
3.1 Luoghi Fisici
3.2 Risorse hardware
3.3 Risorse software
3.4 Risorse dati

**4. Analisi dei Rischi** 11

**5. Definizione ed attuazione della politica di Sicurezza Aziendale** 12

**6. Formazione del personale** 13

**7. Piano di verifica delle Misure Adottate** 14

**8. Allegati** 15

**Allegato "A":** Schede di Trattamento e Rilevazioni dei Rischi
**Allegato "B":** Elenco delle possibili misure adottate

### Premessa al Documento Programmatico sulla Sicurezza

L'ASP di Palermo ha avviato una serie di azioni per migliorare i propri standard in materia di sicurezza ed ha intrapreso un serio ed approfondito percorso per far crescere la formazione del proprio personale sanitario ed amministrativo . Il percorso è iniziato ma non avrà una fine. Il tema della sicurezza di dati personali verrà, infatti, monitorato nel tempo e mantenuto costantemente sotto controllo.
Questa ASP sta producendo uno sforzo progettuale notevole che si è già tradotto nella adozione di un nuovo Regolamento in Materia di trattamento, comunicazione e diffusione dei dati personali sensibili e giudiziari e nella nuova redazione del DPS dell'Azienda.

## 1.1 Scopo Del Documento

Questo documento adempie agli obblighi previsti dagli artt. 33, 34 e regola 19 Allegato B (Disciplinare tecnico in materia di misure di sicurezza) del D.Lgs. 30 giugno 2003 n.196.
Esso è redatto in ottemperanza alle prescrizioni del suddetto D.Lgs. n.196/2003 ("Codice della Privacy") ed individua le linee guida generali, le azioni e le misure per il trattamento dei dati personali, sensibili e giudiziari 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.
La stesura del presente documento è aderente alle seguenti linee guida:
1. analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle figure soggettive coinvolte nel trattamento; l'identificazione, l'inventario e l'analisi dell'hardware, del software e delle banche dati;
2. l'individuazione e la valutazione del rischio;
3. l'individuazione delle misure preventive e correttive;
4. l'individuazione di istruzioni agli incaricati e la previsione di un programma formativo.

## 1.2 Titolare del Trattamento

**L'AZIENDA SANITARIA PROVINCIALE DI PALERMO E' TITOLARE DEL TRATTAMENTO DEI DATI**

Ai sensi dell' art. 4 del D.Lgs 196/03 il **Titolare** è " la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"

## 1.3 Responsabile del Trattamento

I Responsabili del trattamento dei dati di cui l'Azienda è Titolare sono stati individuati
nelle figure istituzionali dei Direttori delle strutture organizzative complesse Aziendali e nei Responsabili delle strutture semplici in staff alla Direzione Aziendale, secondo le modalità indicate nel proprio regolamento interno approvato con delibera n°.1132 del 27.09.2006.
Sono inoltre individuati quali Responsabili del trattamento i soggetti terzi all'amministrazione (persone fisiche e giuridiche) che per conto di questa e sulla base di atti contrattuali, trattano i dati personali acquisiti dall'Azienda e di cui questa è Titolare nell'ambito delle proprie attività istituzionali. L'individuazione del Responsabile del trattamento avviene all'atto della stipula della convenzione o

con atto successivo. Nessun trattamento di soggetti terzi in assenza di tale individuazione è da ritenersi legittimo.

## 1.4 Incaricato del Trattamento

L'Incaricato è la persona fisica alla quale, nell'ambito delle proprie attività, il Titolare o il Responsabile affidano il trattamento dei dati personali. L'Incaricato è dunque colui che operativamente effettua i trattamenti attenendosi alle istruzioni del Titolare o del Responsabile. L'ASP di Palermo ha affidato ai Responsabili il compito di nominare Incaricati le persone fisiche in relazione alle attività svolte nell'ambito della struttura aziendale di appartenenza, impartendo loro adeguate istruzioni, secondo le modalità indicate nel regolamento interno approvato con delibera n° 1132 del 27.09.2006.
Ciascun Responsabile può procedere, inoltre alla nomina di un **preposto alla custodia delle parole chiavi (password)** il quale deve:

1. mantenere un apposito Registro con l'elenco dei codici identificativi e delle parole chiavi assegnati/revocati ed in generale utilizzati dagli Incaricati, allo scopo di assicurare la disponibilità dei dati e/o degli strumenti elettronici nei casi di assenza o impedimento degli Incaricati stessi per esclusive necessità di operatività e di sicurezza del sistema;

2. adottare adeguate misure di sicurezza al fine di garantire la segretezza delle informazioni contenute nel Registro e di informare tempestivamente l'Incaricato di ogni intervento eventualmente effettuato;

3. comunicare al Custode Password ogni variazione apportata sulle parole chiavi;

## 2. Principali Riferimenti Legislativi

- D.Lgs. 30 giugno 2003 n.196, relativo al "Codice in materia di protezione dei dati personali e rapporto di lavoro".

## Definizioni - art. 4 D.Lgs 196/2003

1. Ai fini del presente DPS si applicano le definizioni elencate nel decreto, che per facilità di consultazione, qui si riportano:

   a) **"*trattamento*"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

   b) **"*dato personale*"**, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

   c) **"*dati identificativi*"**, i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"*dati sensibili*"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"*dati giudiziari*"**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"*Titolare*"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) **"*Responsabile*"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"*Incaricati*"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"*Interessato*"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **"*comunicazione*"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) **"*diffusione*"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"*dato anonimo*"**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) **"*blocco*"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) **"*banca di dati*"**, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"*Garante*"**, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del citato Decreto si intende, inoltre, per:

a) **"*comunicazione elettronica*"**, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) **"*chiamata*"**, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) **"*reti di comunicazione elettronica*"**, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito ed a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata;

d) **"*rete pubblica di comunicazioni*"**, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) **"*servizio di comunicazione elettronica*"**, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) **"*abbonato*"**, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) **"*utente*"**, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) **"*dati relativi al traffico*"**, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) **"*dati relativi all'ubicazione*"**, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) **"*servizio a valore aggiunto*"**, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) **"*posta elettronica*"**, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del Decreto si intende, altresì, per:

a) **"*misure minime*"**, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) **"*strumenti elettronici*"**, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) **"*autenticazione informatica*"**, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) **"*credenziali di autenticazione*"**, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

e) **"*parola chiave*"**, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) **"*profilo di autorizzazione*"**, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) **"*sistema di autorizzazione*"**, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del Decreto si intende per:

a) **"*scopi storici*"**, le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) **"*scopi statistici*"**, le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) **"*scopi scientifici*"**, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore

## 3. Identificazione delle Risorse da Proteggere

Sono state identificate le risorse da proteggere con riferimento a quelle che hanno impatto sulla sicurezza dei dati. Particolare importanza è stata data agli strumenti elettronici che sono alla base dei trattamenti automatizzati.

Le risorse coinvolte nel trattamento dei dati personali sono divise in alcune categorie:

- **Luoghi fisici:** sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati o si trovano i sistemi d'elaborazione o i luoghi ove si conservano i dati.

- **Risorse *hardware*:** sono state analizzate le apparecchiature elettroniche coinvolte nelle operazioni di trattamento. Tra queste, particolare rilievo assumono i *server* delle reti locali, ove sono conservati i dati in formato elettronico, ed i *personal computer* da cui sono eseguiti i programmi che elaborano i trattamenti.

- **Risorse *software*:** sono stati analizzati i software applicativi mediante i quali sono effettuati i trattamenti automatizzati.

- **Risorse dati:** sono stati rilevati tutti gli archivi contenenti dati personali trattati siano essi in formato elettronico che in formato cartaceo, oltre ai materiali biologici umani.

## 3.1 Luoghi Fisici

Abbiamo identificato i luoghi fisici in tutte le sedi in cui sono svolte le attività operative e il trattamento dei dati dell'ASP di Palermo .
**L' ASP di Palermo** ha una struttura organizzativa complessa suddivisa in Organi di Direzione e Staff, Dipartimenti, Presidi Ospedalieri, Distretti Sanitari e Unità Operative così come definite nel Documento di Organizzazione Aziendale, approvato con Delibera n° 2878 del 20.12.2005.
**Le strutture dell'ASP sono distribuite in tutti i Comuni del territorio della Provincia di Palermo e nelle isole di Lampedusa, Linosa ed Ustica.**

## 3.2 Risorse Hardware

Fanno parte di questa categoria i Server di rete e i *PC client*, i *Notebook* o *PC* portatili, i *modem*, i *router*.
L' ASP di Palermo dispone di numerosi *Server*; dislocati nell'amministrazione centrale e nelle sedi periferiche.
L'Azienda dispone di sistemi e programmi *antivirus* e dispositivi antiintrusione (Firewall) per la tutela dei dati presenti nel sistema *hardware*. I server sono protetti da gruppi di continuità per impedire che improvvise cadute di tensione danneggino i dati.

## 3.3 Risorse Software

L'utilizzazione di qualunque applicazione, attraverso qualunque risorsa, è possibile solamente se tale applicazione è regolarmente acquisita dal legittimo titolare del software e/o dell'applicazione ai sensi e per gli effetti di cui alla Legge n. 633/41 sul c.d. diritto d'autore.

## 3.4 Risorse Dati

L' ASP di Palermo necessita di trattare dati personali per lo svolgimento della propria attività e detiene al proprio interno liste di dati che sono state individuate in fase di censimento delle banche dati, come da tabelle allegate al Regolamento Aziendale Privacy.
I dati sono trattati sia con strumenti elettronici che in formato cartaceo.
Sono praticate le misure di *back-up*. I Responsabili e gli Incaricati trattano i dati nel rispetto delle norme di Legge e di quanto stabilito dal Regolamento.
In relazione alla natura dei dati e all'analisi dei rischi sono praticate le misure minime descritte nelle tabelle allegate, relative ad ogni struttura.

# 4. Analisi dei Rischi

Questo capitolo identifica, valuta ed analizza le modalità che possono contrastare i rischi indicati dalla legge, in particolare il rischio di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.
Le categorie di rischio individuate sono in relazione alle:

- **Risorse fisiche**,
- **Risorse *hardware***,
- **Risorse *software***,

Dopo essere state identificate le risorse coinvolte a vario titolo nelle operazioni di trattamento, è stata realizzata l'Analisi dei Rischi. Per Analisi dei Rischi s'intende lo studio delle minacce e delle vulnerabilità cui sono soggette le risorse. Gli indici di rischio sono fissati mediante una scala semiqualitativa a tre valori che di seguito si riporta.
Descrizione della soglia di rischio individuata:

- **Basso**: con questa soglia è individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
- **Medio**: con questa soglia è individuato un rischio superiore al precedente ed identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
- **Alto**: con queste soglie sono individuati dei rischi che è sicuramente rischioso pensare di correre. Pertanto si dovranno probabilmente attivare un insieme di contromisure (di natura fisica, logica, ecc..) per abbattere il rischio e contenerlo su livelli accettabili.

## 5. Definizione ed Attuazione della Politica di Sicurezza Aziendale

L'ASP di Palermo ha individuato le contromisure fisiche, logiche ed organizzative. Queste sono state individuate in relazione alle categorie di rischio associate.
Il D.lgs 196/2003, agli artt. 33, 34 e 35 definisce le misure minime di sicurezza per il trattamento dei dati personali.
Il Decreto prevede inoltre, all'art. 31, tutte le ulteriori cautele (Misure idonee) che devono essere adottate per ridurre al minimo, o per escludere, il pericolo del verificarsi dei rischi previsti nel medesimo art. 31. Esse costituiscono un obiettivo a cui l'ASP deve tendere in materia di sicurezza.
Per questi motivi l'obiettivo cui tutti devono tendere non è limitato all'applicazione delle sole misure minime quanto all'individuazione e applicazione delle misure idonee e necessarie a tutelare con efficacia i dati oggetto del trattamento.
Le contromisure che di seguito sono state individuate sono la risposta ad un determinato rischio. Queste si possono anche dividere in:

1. **Fisiche:** sistemi di rilevazione di intrusione, sistemi di vigilanza audiovisivi o tramite personale addetto, sistemi di protezione e sbarramento agli accessi, controllo degli accessi, registrazione degli accessi, predisposizione di armadi non accessibili da personale privo di autorizzazione, custodia di dati o copie in armadi blindati e/o ignifughi, utilizzo della cassaforte, utilizzo di contenitori con serratura, presenza di dispositivi antincendio, continuità dell'alimentazione elettrica, verifica dei supporti magnetici per le copie.

2. **Logiche:** nomina dei responsabili del trattamento, nomina ed indicazione dei compiti in forma scritta agli incaricati, predisposizione dell'utilizzo delle parole chiave ai sensi del D.lgs 196/2003 e del collegato Allegato B, controllo elaboratori con *antivirus*, crittografia dei dati trasmessi, controllo degli accessi su ogni singolo elaboratore.

3. **Organizzative:** divulgazione dei contenuti del Documento Programmatico sulla Sicurezza a tutte le funzioni aziendali, per le parti di specifica competenza, formazione degli incaricati, verifica e controllo delle misure adottate, distruzione dei supporti magnetici che non devono essere riutilizzati.

   Le misure fisiche e logiche adottate dall' ASP di Palermo sono descritte nelle tabelle dei rischi allegate, relative ad ogni struttura.
   I dati sensibili e giudiziari sono oggetto di ulteriori cautele (art. 22 D. Lgs 196/03) che si possono esemplificare nell' adozione di tecniche di cifratura o utilizzazione di codici identificativi o, comunque, nell'adozione di altre soluzioni che rendano i dati temporaneamente inintelligibili. I dati che riguardano la salute o la vita sessuale sono conservati separatamente dagli altri dati e trattati con le modalità di cui sopra anche nel caso in cui sono contenuti in registri, elenchi o banche di dati senza l'ausilio di strumenti elettronici.

## 6. Formazione del Personale

Il personale è informato sugli obblighi che deve rispettare, sui rischi individuati e sui modi per prevenire i danni ai sensi degli artt. 33, 34, 35 e della regola 19.6 Allegato B del Decreto.
Coerentemente con l'evoluzione degli strumenti tecnici adottati dall'ASP di Palermo e l'insorgere di

nuove disposizioni legislative in materia, la nostra Azienda attua i piani di formazione congrui allo sviluppo del proprio personale.
Nella programmazione della formazione teniamo altresì conto delle caratteristiche del personale addetto al trattamento dei dati.
All'interno della nostra Azienda esiste un Piano della Formazione che è redatto annualmente; questo si inserisce all'interno della regolare attività di lavoro ed ha l'obiettivo di seguire anche il progresso tecnologico nel campo di sicurezza delle informazioni.
Il personale interno, concordemente con quanto previsto nel Piano della Formazione, è regolarmente informato sulle normative vigenti in materia ed istruito sui comportamenti più idonei alla sicurezza nel trattamento dei dati personali; ciò avviene principalmente durante la formazione c.d. 'continua' organizzata periodicamente al fine di migliorare l'efficacia nell'utilizzo dei sistemi informatici.
Nell'ambito della formazione si inserisce il corso destinato ai Responsabili delle strutture complesse che ha avuto luogo in data 29 giugno 2006.

## 7. Verifica delle Misure Adottate

L'efficacia e l'efficienza delle misure adottate è periodicamente verificata da parte dei Responsabili Privacy di ogni struttura e del Titolare in tempo utile a consentire all'ASP di Palermo l'aggiornamento del DPS, che deve avvenire entro il 31 Marzo di ogni anno secondo quanto previsto dal D.Lgs 196/2003.
Sulla base delle verifiche effettuate, i Responsabili provvedono direttamente ad adottare le misure minime di sicurezza di cui sia rilevata la mancanza o il cattivo funzionamento e quelle ulteriori previste per i dati sensibili e giudiziari. L'obiettivo ultimo a cui i Responsabili devono tendere è l'adozione di misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Il Titolare verifica periodicamente l'attività dei Responsabili.
Durante le operazioni di verifica è data particolare importanza a:

1. qualità delle misure di antintrusione adottate;
2. corretto utilizzo delle parole chiave e dei profili di accesso degli Incaricati e prevedere la disattivazione dei codici di accesso non utilizzati per più di sei mesi;
3. aggiornamento dei dispositivi antivirus;
4. aggiornamento dei programmi software che trattano i dati personali;
5. integrità dei dati e delle loro copie di back-up;
6. tipo di conservazione dei documenti cartacei;
7. accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati;
8. accertamento del livello di formazione degli Incaricati con la previsione di sessioni d'aggiornamento anche in relazione all'evoluzione tecnologica.

## 8. Allegati

**Allegato "A":** Schede di Trattamento e Rilevazione dei Rischi per singola struttura

**Allegato "B":** Elenco delle possibili misure adottate

**Scheda di trattamento ed analisi dei rischi (strumenti elettronici e cartacei)** Allegato "A"/_____

N.B.: Scheda-tipo, gli originali compilati dalle singole strutture sono disponibili solo in formato cartaceo

| | |
|---|---|
| | **Macrostruttura: _____ U.O. _____** |
| 1 | Denominazione del trattamento dei dati: _____<br>N.B. : Le denominazioni vanno tratte dall'apposito elenco allegato al Regolamento Aziendale Privacy indicando i soli numeri corrispondenti |
| 2 | Categorie ( indicare una o più ) cui si riferiscono i dati trattati: paz. ric. □ ; paz. amb. □ ; utenti □ ; personale □ ; fornitori □ ; altro □ , specificare _____ |
| | |
| 3 | Strumento utilizzato per il trattamento : PC □ ; Terminale □ ; Server □ ; Cartaceo □ ; Altro □ |
| 4 | Nome dei programmi applicativi con cui vengono trattati i dati e/o del database in cui sono contenuti i dati e/o della directory in cui sono conservati ( per dati trattati come files singoli tipo word o excel ) : usare un rigo per ciascun tipo di dati<br>1)<br>2)<br>3)<br>4) |
| 5 | Luogo in cui sono trattati i dati (indirizzo) _____ |

| | |
|---|---|
| | **Solo per i dati trattati in forma elettronica** |
| 6 | 1) luogo in cui sono custodite le copie di back-up (per i dati elettronici) _____<br>2) frequenza con cui viene effettuato il back-up: _____<br>3) dispositivo di accesso : PC □ ; Terminale □ ; Server □<br>4) sistema operativo : Windows 95 □ ; 98 □ ; NT □; 2000 □ ; XP □ ; Altro □ , specificare_____<br>5) il PC o Terminale o server è connesso con : Rete locale, via cavo □ ; Rete locale wireless □ ; Rete aziendale □ ; Altra rete □ , specificare _____<br>6) il Pc è isolato ( stand alone ) □<br>7) Il Pc è connesso con Internet : SI via telefonica □ ; SI via HDSL aziendale □ ; SI altro □ , specificare |
| 7 | Trattamenti ( segnare uno o più ) : Archiviazione dati □ ; Gestione dati on line □ ; Elaborazione dati □ ; Altro □ , spec. _____ |
| 8 | Compiti ( segnare uno o più ) Acquisizione dati □ ; Interrogazione dati □ ; elaborazione dati □ ; trasmissione dati su supporto mobile □ ; trasmissione dati via rete □ ; trasmissione dati via e-mail □ ; salvataggio dati ( back-up ) □ ; ripristino dati |

| 9 | **Rischi relativi agli strumenti** | **si** | **no** | **probabilità** | **conseguenze** | **misure da adottare** |
|---|---|---|---|---|---|---|
| | ingresso di virus | | | | | |
| | spamming | | | | | |
| | malfunzionamento | | | | | |
| | accessi esterni | | | | | |
| | intercettazione | | | | | |
| | altro | | | | | |

N.B.probabilità: indicare se alta media o bassa in relazione alla dotazione di antivirus, firewall, collegamento in rete, tipo di collegamneto, password generali, e di utenza, login etc.

N.B. conseguenze: indicare uno o più dei seguenti: errore nei dati, cancellazione dati, perdita parziale dati, sottrazione dei dati, alterazione dei dati, rallentamento delle operazioni, daneggiamento hardware, altro ( specificare )

**Per i dati trattati in forma elettronica e cartacea**

| 10 | **Rischi relativi al personale** | **si** | **no** | **probabilità** | **conseguenze** | **misure da adottare** |
|---|---|---|---|---|---|---|
| | sottrazioni credenziali | | | | | |
| | incuria | | | | | |
| | comportamenti fraudolenti | | | | | |
| | errore materiale | | | | | |
| | altro | | | | | |

N.B. probabilità: indicare se alta, media,bassa in base a formazione, autonomia e responsabilità del personale, rilevanza clinica sociale ed economica dei dati

N.B. conseguenze: indicare uno o più dei seguenti: errore nei dati, cancellazione dati, perdita parziale dati, sottrazione dei dati, alterazione dei dati, rallentamento delle operazioni, daneggiamento hardware, altro ( specificare )

| 11 | **Rischi relativi al contesto** | **si** | **no** | **probabilità** | **conseguenze** | **misure da adottare** |
|---|---|---|---|---|---|---|
| | Accesso non autorizzato ai locali | | | | | |
| | Sottrazione strumenti | | | | | |
| | Eventi distruttivi | | | | | |
| | Guasti ai sistemi complementari | | | | | |
| | Errori umani | | | | | |
| | Altro | | | | | |

N.B. probabilità: indicare se alta, media,bassa in base ai seguenti criteri: locali incustoditi,porte o finestre facilmente forzabili, presenza di personale di vigilanza/portineria, presenza di sistemi di allarme, gruppi di continuità, sistemi antiince

N.B. conseguenze: indicare uno o più dei seguenti: errore nei dati, cancellazione dati, perdita parziale dati, sottrazione dei dati, alterazione dei dati, rallentamento delle operazioni, daneggiamento hardware, altro ( specificare )

| | |
|---|---|
| 12 | Altre informazioni: |

Data_____

Firma del Responsabile _____

# Misure da adottare per la protezione dei dati personali in relazione all’intensità del rischio:

(da utilizzare per la compilazione dell’allegato “A” inserendo uno o più numeri nel rigo predisposto)

## Trattamenti elettronici

1. Controllo delle consegne sw (test esaustivi prima della messa in esercizio)
2. Formazione professionale agli utenti del sistema
3. Manutenzione preventiva
4. Installazione antivirus
5. UPS (gruppi di continuità)
6. Aggiornamento sw antivirus
7. Sistema di controllo accessi logici
8. Aggiornamenti periodici patch di sicurezza
9. Procedure di backup
10. Sistema di profilazione utenti
11. Divieto di uso di dispositivi personali (modem, PC…)
12. Controllo centralizzato
13. Crittografia delle comunicazioni sensibili
14. Sicurezza perimetrale
15. Sistemi di network scanning
16. Sistema di autenticazione
17. Sistema di autorizzazione
18. Procedure per attività di manutenzione delle apparecchiature. UPS, gruppi di continuità Test delle procedure primadell'installazione
19. Sicurezza fisica dei locali che ospitano gli apparati

## Trattamenti cartacei

20. Impianto antincendio - armadi ignifughi
21. Policy di archiviazione/reperimento documenti
22. Armadi chiusi a chiave
23. Razionalizzazione dei criteri di archiviazione
24. Controllo accessi fisici
25. Archivi cartacei chiusi a chiave