DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(Art. 6 D.P.R. n. 318/1999)

(Approvato dal Consiglio di Amministrazione in data __/__/____)

1. SCOPO

Il presente **Documento Programmatico Sulla Sicurezza** è adottato, ai sensi dell'art. 6 del D.P.R. n. 318/1999, per definire le politiche di sicurezza in materia di trattamento di dati personali, ed i criteri organizzativi per la loro attuazione.
In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:
a) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

2. CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza, in raccordo con il Regolamento di attuazione delle norme sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, adottato dall'Ente (da ora innanzi indicato come Regolamento), e del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza deve essere conosciuto ed applicato da tutti gli Uffici dell'Ente e dai relativi dipendenti.

3. RIFERIMENTI NORMATIVI

- L. n. 675/1996
- D. Lgs n. 123/1997
- D. Lgs n. 547/1993
- D. Lgs n. 255/1997
- D. Lgs n. 135/1998
- D. Lgs n. 171/1998
- D. Lgs n. 389/1998
- D. Lgs n. 51/1999
- D. Lgs n. 135/1999
- D. Lgs n. 281/1999
- D. Lgs n. 282/1999
- D.P.R. n. 318/1999
- L. n. 325 del 3/11/2000

4. I COMPITI DELLE SINGOLE FIGURE PREVISTE DALLA NORMATIVA A PROTEZIONE DEI DATI PERSONALI NELSETTORE DELLA SICUREZZA

4.1. IL TITOLARE DEL TRATTAMENTO

E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi dell'art. 15, commi 1 e 2, della legge 675/1996.
Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

4.2. IL RESPONSABILE DEL TRATTAMENTO

In relazione all'attività del Titolare del trattamento, è prevista la nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.
Il Titolare del trattamento affida ai singoli Responsabili del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento.
Il Responsabile del trattamento dei dati ha il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati;
- Attribuire, con l'ausilio degli Amministratori di sistema, ad ogni Utente (USER) o incaricato un Codice identificativo personale (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale;

- Autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili e giudiziari, qualora si utilizzino elaboratori accessibili in rete; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- Verificare, con l'ausilio degli amministratori di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure indicate al successivo paragrafo 12;
- Garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'Ente siano applicate all'interno dell'Ente ed eventualmente al di fuori della stessa, qualora siano cedute a soggetti terzi quali Responsabili del trattamento tutte o parte delle attività di trattamento;
- Informare il Titolare nella eventualità che si siano rilevati dei rischi.

4.3. CUSTODE DELLE PASSWORD

E' compito del Custode delle password gestire e custodire le password per l'accesso ai dati da parte degli Incaricati.
Il Custode delle password deve predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato lo USER-ID utilizzato: all'interno della busta,secondo il modello fornito, deve essere indicata la password usata per accedere al sistema.
Le buste con le password debbono essere conservate in luogo chiuso e protetto.
Il Custode delle password deve revocare tutte le password non utilizzate per un periodo superiore a 6 (sei) mesi.

4.4. AMMINISTRATORE DI SISTEMA

E' compito degli Amministratori di sistema:
- Individuare, nominare e incaricare per iscritto un Custode delle password, qualora vi siano più incaricati del trattamento effettuato con mezzi informatici;
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- Fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (USER-ID) per oltre 6 mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

5. NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato nel Regolamento, delle responsabilità che gli sono affidate in relazione a

quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal DPR 318/1999.
A ciascun Responsabile del trattamento il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Responsabile del trattamento è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

6. NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Ai Responsabili del trattamento è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati.
La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli incaricati deve essere assegnata una parola chiave, e, nei casi di cui all'art. 4 del D.P.R. 318/1999, un codice identificativo personale.
La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa e deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

7. NOMINA DEL CUSTODE DELLE PASSWORD

L'Amministratore di sistema nomina uno o più Custodi delle password a cui è conferito il compito di custodire le parole chiave o password per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
La nomina di ciascun Custode delle password deve essere effettuata con una lettera di incarico.
La nomina del Custode delle password deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura dell'Amministratore di sistema in luogo sicuro.
L'Amministratore di sistema deve informare ciascun Custode delle password della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal DPR 318/1999.
A ciascun Custode delle password l'Amministratore di sistema deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Custode delle password è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Custode delle password può essere revocata in qualsiasi momento dall'Amministratore di sistema senza preavviso, ed essere affidata ad altro soggetto.

8. NOMINA DEGLI AMMINISTRATORI DI SISTEMA

L'Amministratore di sistema, così come individuato nel Regolamento, sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di banche dati.
Il Titolare del trattamento dei dati può nominare ulteriori Amministratori di sistema, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere, informandolo delle responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D.P.R. 318/1999.
La lettera di incarico deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Titolare del trattamento dei dati in luogo sicuro.
Agli Amministratori di sistema il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

9. DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO IN OUT-SOURCING

9.1 TRATTAMENTO DEI DATI IN OUT-SOURCING

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in out-sourcing, nominandoli Responsabili del trattamento.
In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.
Nel caso in cui questi non vengano espressamente nominati, i Responsabili del trattamento in outsourcing ai sensi dell'art. 8 della legge 657/96 devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.
Il Titolare del trattamento o uno dei Responsabili del trattamento, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di Responsabile del trattamento, con particolare attenzione a quei soggetti terzi in outsourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato.
Per l'inventario dei soggetti terzi, in outsourcing, deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento in luogo sicuro.

9.2 CRITERI PEE LA SCELTA DEGLI ENTI TERZI A CUI AFFIDARE IL TRATTAMENTO DEI DATI IN OUT-SOURCING

Il Titolare del trattamento può nominare Responsabile del trattamento in outsourcing quei soggetti terzi che abbiano i requisiti individuati all'art. 8 della legge 675/96 (esperienza, capacità, affidabilità).
Il Responsabile del trattamento dei dati in outsourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal D.P.R. n. 318 del 28 Luglio 1999.

9.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING

Per ogni trattamento affidato ad un soggetto esterno nominato Responsabile del trattamento in out-sourcing, il Titolare del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Il Titolare del trattamento deve informare il responsabile del trattamento dei dati in out-sourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D.P.R. n. 318/1999.
Il Responsabile del trattamento dei dati in outsourcing deve accettare la nomina, utilizzando apposito modulo.
La nomina del Responsabile del trattamento dei dati in outsourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

10. INVENTARI E METODOLOGIE OPERATIVE DI TRATTAMENTO DEI DATI

10.1 INDIVIDUAZIONE DELLE BANCHE DI DATI OGGETTO DEL TRATTAMENTO

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di:

- Dati personali comuni
- Dati personali sensibili
- Dati personali giudiziari
- Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

10.2 INVENTARIO DELLE SEDI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.
Per redigere l'inventario delle sedi in cui vengono trattati i dati deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

10.3 INVENTARIO DEGLI UFFICI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati.
In particolare, per ogni ufficio deve essere indicata la sede, e se l'accesso è controllato.
Per l'inventario degli uffici deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del trattamento della sicurezza dei dati in luogo sicuro.

10.4 INVENTARIO DEI SISTEMI DI ELABORAZIONE

Al Responsabile del trattamento dei dati, in collaborazione con l'Amministratore di sistema, se è diverso dallo stesso, è affidato il compito di redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.
Per ogni sistema debbono essere descritte le caratteristiche e se si tratta di sistema di elaborazione:

- Non accessibile da altri elaboratori (stand-alone)
- In rete non accessibile al pubblico
- In rete accessibile al pubblico

Per ogni sistema deve essere specificato il nome dell'Incaricato o degli Incaricati che lo utilizzano nonché del Custode delle password.
Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

11 MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

11.1 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

- Il tipo di supporto da utilizzare per le copie di back-up
- Il numero di copie di back-up effettuate ogni volta
- Se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità
- Se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate
- Le modalità di controllo delle copie di back-up
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di

back-up

- Le istruzioni e i comandi necessari per effettuare le copie di back-up.

Per redigere il Documento con le istruzioni di copia deve essere utilizzato per ogni banca di dati apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata a:

- Amministratore di sistema di competenza
- Incaricati del trattamento di competenza

11.2 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Responsabile del trattamento dei dati stabilisce inoltre la periodicità, almeno ogni sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattati.
I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare, per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato
- La periodicità di aggiornamenti

Per ogni sistema deve essere predisposto apposito modulo di Rilevazione di virus informatico, sul quale debbono essere annotati eventuali virus rilevati, e se possibile la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.
I moduli compilati ed aggiornati dagli Incaricati del trattamento debbono essere conservati a cura del Responsabile del trattamento dei dati in luogo sicuro e debbono essere trasmessi in copia controllata all'Amministratore di sistema di competenza.

11.3 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'Amministratore di sistema deve provvedere a:

- Isolare il sistema
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.
- L'amministratore di sistema deve inoltre compilare apposito modulo di "Report dei contagi da virus informatici".
- I moduli compilati devono essere conservati a cura del responsabile del trattamento dei dati in luogo sicuro.

11.4. CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI

L'Amministratore di sistema è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati.
Per ogni banca dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up dei dati.
Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni ed atti vandalici
- Incendio
- Allargamento
- Furto

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati a:

- Responsabile del trattamento della sicurezza dei dati
- Eventuale Responsabile del trattamento di competenza
- Incaricato del trattamento di competenza
- Amministratore di sistema di competenza

11.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

Se l'Amministratore di sistema decide che i supporti magnetici utilizzati per le copie di back-up delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.
E' compito dell'Amministratore di sistema assicurarsi che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

11.6 PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le operazioni di back-up delle banche di dati trattate.
Per ogni incaricato del trattamento il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, utilizzando apposito modulo che deve essere trasmesso in copia controllata al Titolare del trattamento.

12 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

12.1 NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto dal D.P.R. 318/1999, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento dei dati di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

12.2 PROCEDURE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere a di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, nominando un apposito Incaricato, con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
Il Responsabile del trattamento dei dati deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
Il Responsabile del trattamento dei dati deve informare con una comunicazione scritta l'Incaricato dell'ufficio dei compiti che gli sono stati affidati utilizzando apposito modulo.

12.3. PROCEDURE DI ASSEGNAZIONE DEGLI USER-ID

Il Responsabile del trattamento dei dati, in accordo con l'Amministratore di sistema, deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.
Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei codici identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un Incaricato del trattamento deve essere annullato se l'Incaricato del trattamento ha dato le dimissioni.

12.4 PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD

Il Responsabile del trattamento dei dati deve definire in accordo con l'Amministratore di sistema le modalità di assegnazione delle password.

La definizione dei criteri di assegnazione delle password è descritta in apposito modulo.
In relazione al tipo di banca di dati trattata, l'Amministratore del sistema può decidere che ogni utente Incaricato del trattamento possa modificare autonomamente la propria password di accesso.
In questo caso la modifica equivale alla comunicazione al Custode della password.

12.5 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica.
Per ogni sistema deve essere specificato l'Incaricato del trattamento, l'Amministratore del sistema e il Custode della password.
Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro, e deve essere trasmesso in copia controllata all'Amministratore di sistema di competenza.

12.6 CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni
- Le misure applicate per evitare contagi da virus informatici

13 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

13.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo USER-ID assegnato.
In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione al Custode delle password e all'Amministratore di sistema di competenza che provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Per redigere l'elenco degli Incaricati del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata a:

- Amministratore di sistema di competenza
- Custode delle password di competenza

13.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

All'Amministratore di sistema è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata a :

- Amministratore di sistema di competenza
- Custode della password di competenza

13.3 DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO AI DATI

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione la tabella dei Permessi di accesso che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.
In particolare per ogni Incaricato del trattamento e per ogni banca di dati debbono essere indicati i privilegi assegnati tra i seguenti:

- Inserimento di dati
- Lettura e stampa di dati
- Variazione di dati
- Cancellazione di dati

La tabella dei Permessi di accesso deve essere redatta utilizzando l'apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata a:

- Amministratore di sistema di competenza
- Custode delle password di competenza

13.4 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DEI PERMESSI DI ACCESSO AI DATI

All'Amministratore di sistema è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli

utenti autorizzati, utilizzando apposito modulo che deve essere conservato in luogo sicuro e deve essere trasmesso in copia controllata a:

- Amministratore di sistema di competenza

- Custode delle password di competenza

13.5 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale Incaricato del trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati. Per ogni utente il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione, utilizzando apposito modulo che deve essere trasmesso in copia controllata al Titolare del trattamento.

14 MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

14.1 MANUTENZIONE DI SISTEMI DI ELABORAZIONE DEI DATI

All'Amministratore di sistema è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.
La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito

tenendo conto anche dell'evoluzione tecnologica.
L'Amministratore di sistema deve compilare apposito modulo di "evidenziazione dei rischi hardware".
Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

14.2 MANUTENZIONE DEI SISTEMI OPERATIVI

All'Amministratore di sistema, è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito

tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti

- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposito modulo di "evidenziazione dei rischi sui Sistemi Operativi".

Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme di in vigore.

14.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE.

All'Amministratore di sistema è affidato il compito di verificare ogni anno, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito.

tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposito modulo di "Evidenziazione dei rischi nelle applicazioni".

Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

15 MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI

15.1 NOMINA E ISTRUZIONI AGLI INCARICATI

Per ogni archivio i Responsabili del trattamento dei dati debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano dati sensibili e giudiziari (art. 22 e 24 L. 675/96) gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

15.2 COPIE DEGLI ATTI DEI DOCUMENTI

Quanto indicato nel punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

16 REVISIONI

Il presente Documento Programmatico Sulla Sicurezza (**DPSS**), redatto nel mese di Dicembre 2003, verrà revisionato annualmente ed eventualmente sottoposto a modifiche.