



Documento unico

composto da numero ____ di pagine

Si richiede l'apposizione del
timbro postale per la data certa.

Data _____

Firma del Presidente

**PROCEDURA PER IL TRATTAMENTO DEI DATI PERSONALI
E
DOCUMENTO PROGRAMMATICO DI SICUREZZA**

AVIS COMUNALE DI _____





DOCUMENTO PROGRAMMATICO SULLA SICUREZZA



INDICE

PREMESSA

DEFINIZIONI

ASPETTI SANZIONATORI

☞

1) IL TRATTAMENTO DEI DATI: le caratteristiche

- 1.1. tipologia dei dati
- 1.2. tipologia dei trattamenti
- 1.3. supporto di memorizzazione e trattamento dei dati
 - 1.3.a. supporto cartaceo
 - 1.3.b. supporto informatico
- 1.4. luoghi di conservazione dei dati
- 1.5. soggetti che attuano il trattamento

2) IL TRATTAMENTO DEI DATI – gli adempimenti e le procedure

- 2.1. Gli adempimenti formali:
 - 2.1.a. Informativa
 - 2.1.b. Nomina di Responsabili e incaricati
- 2.2. Valutazione dei rischi
- 2.3. Misure di sicurezza
 - 2.3.a. fisiche per la protezione delle aree e dei locali e dei contenitori
 - 2.3.b. elettroniche per la protezione dei sistemi informatici
 - 2.3.c. organizzative
- 2.4. La pianificazione degli interventi formativi
- 2.5. La pianificazione delle verifiche e revisioni periodiche



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Premessa

Il presente documento contiene le linee guida per la conservazione e la messa in sicurezza dei dati contenuti nei supporti informatici e/o cartacei, utilizzati da AVIS COMUNALE DI _____, di qui in poi denominata anche Titolare nello svolgimento della propria attività assistenziale.

Ferme le procedure e le norme individuate nella presente procedura, ogni incaricato nello svolgimento delle proprie mansioni e nella gestione di casi particolari non espressamente disciplinati, dovrà attenersi alle linee guida, curando comunque che, in ogni caso, siano rispettati i diritti dei soggetti interessati al trattamento ed evitare che il medesimo possa determinare conseguenze dannose per l'associazione e/o i terzi.

La normativa italiana in materia di privacy, alla data di pubblicazione della presente procedura, è raccolta ed accorpata nel D. Lgs. 196/2003 meglio conosciuto come Codice della Privacy, disponibile in allegato cartaceo o mediante il link [..CODICE PRIVACY.pdf](#)

Per ogni approfondimento è disponibile il sito del Garante al seguente indirizzo www.garanteprivacy.it

Il presente documento costituisce altresì Documento Programmatico di sicurezza in adempimento di quanto previsto dall'art. 34 del D.Lgs. e all'All. B – art. 19.

Definizioni

Al fine di agevolare la lettura e la comprensione del significato normativo delle disposizioni del presente documento, si riportano di seguito le definizioni, fornite dal Garante, dei termini utilizzati nel Codice.

"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;

"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;

"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;

"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;

"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;

"incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ASPETTI SANZIONATORI

L'inosservanza delle norme del Codice della Privacy comporta l'applicabilità di sanzioni amministrative e penali a seconda delle fattispecie.

Di seguito vengono riportate le principali sanzioni.

SANZIONI PENALI

Trattamento dei dati in violazione delle disposizioni di cui agli art. 18,19,23,123,126,130 ovvero in dell'art. 129	Reclusione da 6 a 18 mesi elevati a 24 mesi se il fatto consiste nella diffusione o comunicazione dei dati illecitamente trattati
Trattamento dei dati in violazione delle disposizioni di cui agli art. 17,20,21,22,25,26,27 e 45	Reclusione da 1 a tre anni
Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da sei mesi a 3 anni
Omessa adozione di misure di sicurezza	Arresto sino a due anni o ammenda da € 10.000,00 a € 50.000,00
Inosservanza dei provvedimenti del Garante	Reclusione da 3 mesi a due anni

SANZIONI AMMINISTRATIVE

Cessione di dati in violazione di disposizioni in materia di trattamento di dati personali	Sanzione amministrativa pecuniaria da € 5.000,00 a € 30.000,00
Omessa informazione o esibizione al Garante di documenti richiesti	Sanzione amministrativa pecuniaria da € 4.000,00 a € 24.000,00
Omessa o incompleta notificazione al Garante	Sanzione amministrativa pecuniaria da €10.000,00 a € 60.000,00

RESPONSABILITÀ CIVILE.

La responsabilità civile prevista dal Codice della Privacy è quella tipica prevista per l'esercizio delle attività pericolose ([art. 2050 cod. civ.](#)).

Il danneggiato dovrà pertanto provare il danno e il nesso di causalità, mentre sul danneggiante (responsabile e incaricato del trattamento) incomberà l'onere di provare di aver adottato tutte le misure idonee ad evitare il danno.

In considerazione delle conseguenze sanzionatorie previste dalla legge (penali, civili, amministrative) non potranno essere tollerate condotte contrarie alla norma e alla presente procedura.

Le condotte illegittime dovranno essere immediatamente contestate e, nei casi di accertata violazione, dovranno essere sanzionate disciplinarmente in ragione della loro gravità, salve le conseguenze sanzionatorie espressamente previste dalla legge.



IL TRATTAMENTO DEI DATI
Le caratteristiche del sistema

TITOLARE DEL TRATTAMENTO

AVIS COMUNALE DI

SEDE LEGALE

OGGETTO SOCIALE:

Gestione senza scopo di lucro degli ASSOCIATI DONATORI, ASSOCIATI ASPIRANTI DONATORI e ASSOCIATI NON DONATORI per le finalità statutarie principalmente connesse alla donazione di sangue ed emocomponenti; attività di promozione della donazione e della solidarietà in generale rivolta alla popolazione in generale.

RAPPRESENTANTE LEGALE

Presidente

1.1) Tipologia dei dati personali trattati

L'attività Associativa rende necessario il trattamento di dati personali sia per le finalità proprie che per quelle amministrative e contabili.

In particolare, si possono delineare le seguenti tipologie generali di dati:

- ASSOCIATI DONATORI

Dati comuni Dati sensibili Persone fisiche

- ASSOCIATI ASPIRANTI DONATORI

Dati comuni Dati sensibili Persone fisiche

- ASSOCIATI EX DONATORI

Dati comuni Dati sensibili Persone fisiche

- UTILIZZATORI

Dati comuni Dati sensibili
 Enti Ospedalieri pubblici Persone Fisiche Ditte individuali
 Società Altro (specificare)



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

- FORNITORI

- | | |
|--|--|
| <input type="checkbox"/> Dati comuni | <input type="checkbox"/> Dati sensibili |
| <input type="checkbox"/> Società | <input type="checkbox"/> Ditte individuali |
| <input type="checkbox"/> Persone Fisiche | |

- ALTRO, SPECIFICARE

.....

- | | |
|--------------------------------------|---|
| <input type="checkbox"/> Dati comuni | <input type="checkbox"/> Dati sensibili |
|--------------------------------------|---|
-

1.2) Tipologia dei trattamenti

Con i dati personali sopra individuati (punto 1.1), l'**AVIS COMUNALE DI**
attua le seguenti tipologie di trattamento:

cod. 01) Trattamento dei dati personali, sia sensibili che comuni, degli ASSOCIATI DONATORI e degli ASSOCIATI ASPIRANTI DONATORI per la gestione della donazione di sangue e plasma con riferimento al controllo dell'idoneità (di pertinenza esclusiva dei Centri Trasfusionali) e alla reperibilità del donatore, per la gestione delle chiamate e l'invio di materiale dell'Associazione;

cod. 02) Trattamento dei dati personali, sia sensibili che comuni, degli ASSOCIATI NON DONATORI per la conservazione per l'invio di materiale dell'Associazione e per la loro reperibilità;

cod. 03) Trattamento dei dati personali dei fornitori, clienti, banche, concernenti la reperibilità e la corrispondenza con gli stessi, nonché i dati necessari ai fini fiscali o i dati di natura bancaria per le operazioni di pagamento;

cod. 04) Trattamento dei dati personali di cittadini e associazioni, ricavati da elenchi e/o albi accessibili al pubblico, al fine di svolgere la propria attività associativa di promozione del dono del sangue e della solidarietà in generale.

Per ogni tipologia di trattamento è stata realizzata una scheda descrittiva, che riporta sinteticamente: le strutture di riferimento, la natura dei dati, l'ubicazione fisica, i supporti di trattamento, la tipologia dei dispositivi di accesso, l'eventuale tipologia di interconnessione, gli eventuali incaricati al trattamento, le misure di sicurezza adottate. Le schede sono allegate al presente Documento .

1.3) Supporti di memorizzazione e trattamento dei dati

1.3.a Supporto cartaceo

La documentazione cartacea contenente dati personali, viene conservata in armadi

- | | |
|--|------------------------------------|
| <input type="checkbox"/> chiusi a chiave | <input type="checkbox"/> ignifughi |
|--|------------------------------------|

In particolare, vengono conservati

- i moduli di adesione, con relativa autorizzazione al trattamento dei dati dei donatori, ex donatori e aspiranti donatori;
- i faldoni cartacei contenenti i documenti relativi ai trattamenti dei dati personali di cui ai codici (cfr. punto 1.2)



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Ogni incaricato è tenuto a curare la custodia dei documenti cartacei contenenti dati personali, all'interno degli armadi chiusi.

Le chiavi di accesso ai locali sono in possesso, oltre che del titolare, anche di:

Cognome Nome		
_____	<input type="checkbox"/> Responsabile	<input type="checkbox"/> Incaricato
_____	<input type="checkbox"/> Responsabile	<input type="checkbox"/> Incaricato
_____	<input type="checkbox"/> Responsabile	<input type="checkbox"/> Incaricato
_____	<input type="checkbox"/> Responsabile	<input type="checkbox"/> Incaricato
_____	<input type="checkbox"/> Responsabile	<input type="checkbox"/> Incaricato

1.3.b Informatico

Per quanto riguarda il trattamento di dati su supporto informatico, l'Associazione utilizza:

Hardware (fisso e/o portatile)

Denominazione PC	Supporti di memorizzazione	Connessione Rete Locale/INTRANET	Connessione Internet
	<input type="checkbox"/> Hard- disk interno <input type="checkbox"/> keymemory /Usb <input type="checkbox"/> Unità Lettore Cd/Dvd <input type="checkbox"/> Registratore di Cassette <input type="checkbox"/> Unità Floppy Disk	<input type="checkbox"/> SI <input type="checkbox"/> No	<input type="checkbox"/> SI <input type="checkbox"/> No
	<input type="checkbox"/> Hard- disk interno <input type="checkbox"/> keymemory /Usb <input type="checkbox"/> Unità Lettore Cd/Dvd <input type="checkbox"/> Registratore di Cassette <input type="checkbox"/> Unità Floppy Disk	<input type="checkbox"/> SI <input type="checkbox"/> No	<input type="checkbox"/> SI <input type="checkbox"/> No

- N° _____ Telefoni cellulari
- N° _____ Palmari
- N° _____ Router
- N° _____ Stampanti
- N° _____ Fax
- N° _____ Firewall

Software

- Microsoft Word
- Microsoft Excel
- Software gestionale dedicato denominato Assoavis.
- _____ (altro)

Tipologie di interconnessione

- Rete locale
- Intranet
- Internet
- (altro)



1.4) I luoghi di conservazione dei dati

Gli armadi/contenitori nei quali sono custoditi i supporti cartacei sono ubicati presso

Gli elaboratori elettronici sono collocati presso

1.5) I soggetti che attuano il trattamento

Ai sensi del Codice, si è proceduto alla formalizzazione

- della nomina a **Responsabile** al trattamento di dati personali

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

- degli **Incarichi** al trattamento, nei confronti di

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

Sig.

Trattamenti: codice.....

IL TRATTAMENTO DEI DATI

Gli adempimenti, le procedure, le misure di sicurezza

PREMESSE

Il Codice della Privacy prevede che, per effettuare legittimamente il trattamento dei dati personali, si attuino una serie di incombenti formali (informativa, raccolta del consenso, formalizzazione delle nomine responsabile e incarico al trattamento) e si adottino le misure di sicurezza idonee a garantire il controllo dell'accesso ai dati, della loro trasmissione e della loro conservazione, per evitare la loro accidentale distruzione e/o la loro illecita trasmissione.

2.1) Gli incombenti formali

Preliminarmente, sono state conferite le nomine ai responsabili e agli incaricati, mediante comunicazione scritta.

Il Titolare cura che, all'assunzione o al cambiamento di mansioni, vengano formalizzate anche le funzioni relative

Prima della raccolta dei dati, viene fornita una specifica informativa all'interessato, circa le finalità del trattamento, la sua obbligatorietà e/o necessità, i mezzi utilizzati, il Titolare al trattamento, i diritti dell'interessato, etc.

E' altresì raccolto il consenso al trattamento da parte dell'interessato, laddove richiesto per il trattamento. In particolare, nell'ambito dell'Azienda è stata creata una modulistica standard da utilizzare nell'ambito nelle procedure stabilite per le singole banche dati e riportate nelle relative schede.

Elenco modulistica

- **Informativa del trattamento e raccolta del consenso** – che dovrà essere visionata e sottoscritta per ricevuta ed espressione del consenso dall'interessato al trattamento stesso:
Modello informativa per Aspiranti Donatori;
Modello informativa per fornitori;
Modello informativa dipendenti;
Modelli informativa ai collaboratori dell'Associazione non retribuiti;
- **Nomina del responsabile** – che dovrà essere sottoscritta dal titolare, visionata e sottoscritta per ricevuta ed espressione dell'accettazione dal nominato.
Modello nomina responsabile interno alla struttura;
Modello e nomina responsabile esterno alla struttura
- **Incarico al trattamento** che dovrà essere visionato e sottoscritto per ricevuta ed espressione dell'accettazione dall'incaricato.
Modello e incarico al trattamento per i dipendenti e collaboratori dell'Associazione;

I moduli standard, in versione cartacea e/o informatica, devono essere conservati unitamente al presente documento e resi disponibili per i responsabili.

I moduli di nomina e di incarico, sottoscritti dai destinatari, sono conservati in apposita cartellina archiviata nello stesso faldone in cui viene archiviato il presente documento identificato esternamente dalla dicitura "PRIVACY".

Ogni incaricato deve accertare e garantire la regolarità formale degli adempimenti necessari in relazione alle operazioni di trattamento dei dati dal medesimo compiute, secondo le istruzioni ricevute e con l'utilizzo della modulistica disponibile.

2.2) valutazione dei rischi

In generale

Preliminarmente è stato affrontato lo studio dei rischi che possano arrecare danno alle banche dati in uso presso l'Associazione e si sono evidenziati i seguenti rischi:

<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	rischio di furto
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	rischio incendio;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	rivelazione illegittima di informazioni da parte di soggetti interni o terzi;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	accesso non autorizzato ai dati da parte di soggetti interni non autorizzati o da parte di terzi;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	trattamento non consentito da parte di soggetti non abilitati;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	trattamento eccedente le finalità per le quali i dati sono stati raccolti;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	perdita o distruzione accidentale dei dati.

Rischi specifici:

<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	furto di credenziali di autenticazione;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	incuria, disattenzione, errore materiale degli operatori;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	comportamenti sleali o fraudolenti degli operatori e/o di terzi;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	azioni dannose provocate da virus informatici, spamming, o altre tecniche di sabotaggio;
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	accessi esterni non autorizzati, malfunzionamento o degrado delle strumentazioni elettroniche.
<input type="checkbox"/> Alto	<input type="checkbox"/> Medio	<input type="checkbox"/> Basso	guasto ai sistemi complementari (impianto elettrico, idraulico, di climatizzazione)

2.3) Le misure di sicurezza

Fisiche

- a) sistema elettronico antifurto (*descrizione sintetica delle caratteristiche tecniche e dei periodi di attivazione*)
- b) sistema elettronico antincendio (*descrizione sintetica delle caratteristiche tecniche e dei periodi di attivazione*)
- c) Porta blindata (*descrizione sintetica delle caratteristiche tecniche e della procedura di possesso delle chiavi*)
- d) Sbarre alle finestre
- e) Estintori a norma



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

- f) Armadi con serratura (*descrizione sintetica delle caratteristiche tecniche e della procedura di possesso delle chiavi*)
- g) distruggi –documenti
- h) gruppo di continuità

Responsabile del controllo periodico efficienza:

Informatiche

i) Sistema operativo

E' necessario premettere che è stato appurato che, secondo le migliori tecniche disponibili, non tutti i sistemi operativi di gestione dell'hardware e del software garantiscono la migliore protezione dei dati essendo necessario installare le versioni più recenti.

Tuttavia, versioni precedenti, possono essere utilizzate se riservate esclusivamente alla associazione titolare del presente documento, proteggendo il sistema direttamente all'accensione.

I computer e i server dell'Associazione utilizzano i seguenti sistemi operativi

- Windows Versione
- Mac Versione
- Linux
- Altro

l) Password

L'accesso alle banche dati è selezionato mediante il sistema delle password.

Ad ogni responsabile e ad ogni incaricato vengono assegnati una user-id identificativa ed una password iniziale di almeno otto caratteri per l'accesso alla rete aziendale tramite i terminali individuali.

Unitamente alla password iniziale viene fornita per iscritto la procedura per la sua modifica con la prescrizione di modificarla al primo accesso e successivamente ogni sei mesi, mantenendo ferma la lunghezza di otto caratteri e facendo in modo che la password non sia riconducibile al titolare.

m) Software Antivirus

Il sistema informatico è protetto mediante il seguente antivirus:

Marca.....; Mod..... Vers.

La funzionalità e l'aggiornamento dei sistemi di protezione sono aggiornati con cadenza

n) Software Firewall

Il sistema di connessione alla rete internet è dotato del seguente sistema che permette di monitorare ed inibire gli accessi ai dispositivi informatici:

Marca.....; Mod..... Vers.

p) Software per prevenire vulnerabilità e/o correggere difetti degli strumenti elettronici (ad es. Patch di Windows)

Marca.....; Mod..... Vers.

q) Back-up e ripristino

Per prevenire il rischio di perdita o distruzione dei dati, sono periodicamente effettuate delle procedure c.d. di backup per il salvataggio dei dati su supporti



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il salvataggio è disposto con cadenza;
I supporti di memorizzazione su cd- floppy- keymemory /Usb sono custoditi in (es. armadi ignifughi o blindati, cassette di sicurezza..... presso
Unitamente ai supporti di memorizzazione dei dati, sono conservati i supporti di memorizzazione dei software utilizzati per la gestione dei dati stessi
In caso di necessità il ripristino avviene attraverso la seguente procedura:
(descrizione sintetica delle caratteristiche tecniche e della procedura di ripristino)
.....

Organizzative

Innanzitutto sono stati formalizzati gli incarichi sono stati nominati i responsabili.

Inoltre, sono state impartite, in aggiunta alle procedure gestionale le seguenti misure organizzative specifiche

- E' fatto divieto di lasciare incustoditi sulle scrivanie o su altri ripiani, documenti che contengano dati personali.
E' prescritta l'adozione di screen saver dotati di parola chiave analoga a quella di accesso al sistema, con attivazione automatica quando il computer sia inattivo per un periodo di tempo eccedente i minuti.
E' obbligatorio distruggere i supporti cartacei non utilizzati con mezzi meccanici o manuali
E' vietato divulgare a terzi le password nonchè di conservare le password su supporti cartacei facilmente accessibili da persone non autorizzate.
E' fatto divieto inoltre di affidare a terzi un trattamento di dati senza nessuna autorizzazione .;
E' fatto divieto di memorizzare nelle memorie dei telefoni o delle SIM di proprietà dell'Associazione, numeri diversi da quelli relativi ai trattamenti autorizzati.
Descrivere sinteticamente la procedura per l'apertura della posta e la ricezione dei fax. (Chi apre la posta, chi può accedere ai fax in arrivo)
Altro.....

2.4) la pianificazione degli interventi formativi

Il titolare deve curare che gli incaricati possiedano le nozioni necessarie per il corretto trattamento dei dati nel rispetto della norma.

A tal fine gli incaricati, prima di iniziare il trattamento, devono:

- partecipare ad un corso di apprendimento delle nozioni basilari sulle norme in materia di dati personali avente ad oggetto:

- Conoscenza dei rischi che incombono sui dati;
Misure disponibili di sicurezza fisiche, logiche, informatiche per prevenire eventi dannosi;
Disciplina sulla protezione dei dati personali in rapporto alle relative attività;
Profili di responsabilità in merito al trattamento dei dati.

- prendere visione della presente procedura e dei relativi allegati dichiarando per iscritto di averla visionata e di accettarla per intero;

- ricevere comunicazione degli aggiornamenti della normativa e della presente procedura mediante .

Il titolare deve, inoltre, impartire tutte le disposizioni che si rendono necessarie ad integrare le procedure previste nel presente documento e nei suoi allegati utilizzando, laddove possibile, la forma scritta per la comunicazione agli incaricati.

Il titolare deve inoltre integrare la formazione specifica qualora ciò si renda necessario per il cambiamento di mansioni o per l'introduzione di nuovi strumenti di lavoro.



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

2.5) la pianificazione delle revisioni periodiche

Oggetto revisione	Incaricato revisione	Cadenza	Date
Documento Programmatico Sulla Sicurezza	Titolare	Annuale	
Formalizzazione nomine Responsabili	Titolare	Annuale	
Formalizzazione Incarichi	Responsabile	Annuale	
Credenziali di autenticazione	Responsabile	Annuale	
Efficienza e aggiornamento misure di sicurezza	Responsabili	Annuale	
Verifica attività di formazione degli incaricati	Responsabile	Annuale	

Il presente documento programmatico sulla sicurezza è stato redatto ai sensi dell'art. 34 D. Lgs. 196/2003 e art. 19 all. B codice della Privacy. Si compone di n° 14 pagine ed è valido fino **al 31 marzo 2013. Rimane a disposizione degli organi competenti presso la struttura che lo ha redatto ed ha validità sino al 31 marzo 2013.**

..... , li

Firma del Titolare