

## DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dal **Comune di Chiuduno con sede in Largo Europa, 3 - 24060 CHIUDUNO (BG) – Codice fiscale 00278290168** (nel seguito del documento indicato come Titolare).

=====

Il presente documento è redatto e firmato in calce dal responsabile per la sicurezza, i cui dati sono i seguenti:

- Moscato Giovanna, con la qualifica di Segretario Comunale.

=====

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al Dlgs 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
  - la individuazione dei tipi di dati personali trattati
  - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
  - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento
3. l'analisi dei rischi che incombono sui dati
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
7. le procedure da seguire per il controllo sullo stato della sicurezza
8. dichiarazioni d'impegno e firma.

## Indice:

1	L'elenco dei trattamenti dei dati personali	Pag. 3
	1 Tipologie di dati trattati	
	2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti	
	3 La mappa dei trattamenti effettuati	
2	Mansionario privacy ed interventi formativi degli incaricati	Pag. 11
3	Analisi dei rischi che incombono sui dati	Pag. 14
4	Misure atte a garantire l'integrità e la disponibilità dei dati	Pag. 17
	1 La protezione di aree e locali	
	2 La custodia e l'archiviazione di atti, documenti e supporti	
	3 Le misure logiche di sicurezza	
5	Criteri e modalità di ripristino dei dati	Pag. 25
6	L'affidamento di dati personali all'esterno	Pag. 26
7	Controllo generale sullo stato della sicurezza	Pag. 28
8	Dichiarazioni d'impegno e firma	Pag. 29

## **1. L'elenco dei trattamenti dei dati personali**

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si è proceduto come segue:

- Si individuano i tipi di dati personali trattati, in base alla loro natura, alla categoria di soggetti cui essi si riferiscono e alla finalità.
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

### **1.1 Tipologie di dati trattati**

In dettaglio i trattamenti effettuati dal titolare riguardano:

- Dati relativi allo Stato civile, anagrafe e liste elettorali dei cittadini
- Dati relativi all'esercizio dell'elettorato attivo e passivo e per il trattamento economico degli amministratori.
- Dati comuni e sensibili per la gestione dei contratti di lavoro dei dipendenti del Titolare per: assunzione; licenziamento; trattamento economico; ferie, permessi, aspettative, previdenza, assicurazioni, procedimenti disciplinari, valutazione attività) e gestione sostituto di imposta;
- Dati comuni e sensibili rilevanti per la gestione dei tributi locali.
- Dati comuni e sensibili per l'accertamento delle violazioni amministrative.
- Dati comuni e sensibili relativi all'assolvimento dell'obbligo scolastico e della gestione mense scolastiche. I dati relativi alla salute e alle confessioni religiose sono necessari per la gestione delle mense e anche dei calendari scolastici, nonché delle attività educative
- Dati comuni e sensibili relativi all'erogazione di contributi a persone giuridiche e fisiche; sussidi diretti ed indiretti a bisognosi per condizioni economiche e stato di salute.
- Dati comuni e sensibili per l'assolvimento della funzione di autorità sanitaria locale da parte del Sindaco.
- Dati comuni e sensibili per la gestione dei sussidi diretti ed indiretti a favore dei Portatori di handicap e per interventi per superamento barriere architettoniche
- Dati comuni e sensibili per la gestione obiettori impiegati nell'ente (come per il personale)
- Dati comuni e sensibili per la gestione autorizzazioni commercio fisso e ambulante, concessione suolo pubblico, pubblici esercizi; gestione edifici di edilizia residenziale pubblica (i dati relativi alla salute sono rilevanti al fine della gestione degli alloggi riservati ai portatori di handicap).
- Dati comuni relativi all'abitabilità; tutela territorio; concessioni ad edificare; gestione piani urbanistici attuativi; nulla osta attività produttive; agibilità; tutela dell'atmosfera; tutela acque e sottosuolo;
- Dati comuni e sensibili per la gestione di Gare di appalto (come per i contratti). I dati relativi ai carichi pendenti e al certificato generale del casellario giudiziale sono necessari per la stipulazione dei contratti
- Dati comuni e sensibili per l'erogazione del servizio di prestito dei libri.
- Dati relativi alla Gestione impianti sportivi; appartamenti in affitto; gestione strutture comunali.

Al fine della stesura della mappa dei trattamenti effettuati e della redazione del mansionario i dati trattati dal Titolare si riassumono in modo esaustivo come segue:

Dati comuni relativi a clienti /cittadini / dipendenti.

Dati comuni relativi a fornitori.

Dati comuni relativi ad altri soggetti.

Dati di natura giudiziaria relativi a clienti, fornitori, cittadini, dipendenti e ad altri soggetti.

Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile.

Dati di natura sensibile relativi a clienti / fornitori / utenti / cittadini.

Dati idonei a rivelare lo stato di salute e/o la vita sessuale dei cittadini.

Dati idonei a rivelare l'affezione da virus HIV.

**Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti.\***

**Dati biometrici relativi al personale e ad altri soggetti. \***

**\*Attualmente non è installato alcun sistema elettronico in grado di acquisire questi dati, ma con molta probabilità potrebbe essere installato nel prossimo futuro. In vista dei prossimi aggiornamenti annuali del documento le tabelle di analisi prevedono già questi tipi di dati anche se attualmente non trattati.**

Si allega la tabella riepilogativa di tutti i trattamenti frutto dell'analisi interna dal Titolare dalla quale si è partiti per identificare le tipologie di dati di questo paragrafo.

## 1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali avviene nei **seguenti edifici**:

### **Palazzina del Municipio**

E' situata in Largo Europa, 3 in zona centrale del comune di Chiuduno (BG). La palazzina si sviluppa su tre piani più un sottotetto. Al piano terra si trovano tre aree di trattamento ben distinte che corrispondono a tre uffici ognuno con un'entrata propria direttamente accessibile dall'esterno e un altro accesso dove troviamo la porta blindata dell'entrata principale che permette l'accesso ai piani superiori.

Le aree di trattamento e archiviazione dati sono identificate e sono state classificate come segue perché isolabili dalle altre e provviste di porte chiudibili a chiave. Tali zone sono riassunte in questa lista:

#### **Piano Terra:**

- Ufficio Segreteria / Tributi
- Ufficio Polizia Locale
- Ufficio Servizi alla persona

#### **Primo piano:**

- Sala Giunta
- Ufficio Sindaco
- Ufficio Economico / Contabile
- Ufficio Segretario Comunale
- Ufficio Amministrativo (Anagrafe, Stato civile, Commercio)\*
- Archivio / Magazzino 1 piano
- Sala Server / Teleassistenza

#### **Secondo piano:**

- Sala Consiliare
- Ufficio Tecnico 1 e 1 a\*
- Ufficio Tecnico 2
- Archivio / Magazzino 2 piano

#### **Sottotetto:**

- Archivio sottotetto

**\* le due aree comunicano tramite una scala a chiocciola e non possono essere isolabili l'una d'altra.**

### **Biblioteca**

E' situata in via C. Battisti, in zona centrale del comune di Chiuduno (BG). I locali sono localizzati al secondo piano interrato all'interno di un palazzina. L'area di trattamento è accessibile dalle parti comuni dello stabile (rampa delle

scale e porta principale) ed è protetta da n. 1 cancello in ferro chiudibile a chiave e n. 1 porta di accesso, chiudibile a chiave.

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

#### **A – Schedari ed altri supporti cartacei**

I supporti cartacei, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- Ogni area di trattamento è dotata di armadi dotati di chiusura a chiave da destinare a quelle banche dati di cui sono incaricate che contengono dati personali (sensibili e giudiziari). Solo nel caso che la banca dati contenga esclusivamente dati (comuni) vengono utilizzati eventuali parti di armadi non chiudibili a chiave.
- Sono presenti inoltre tre aree destinate ad archivio rispettivamente al primo piano, al secondo e nel sottotetto dove sono contenuti in scaffali i dati degli anni precedenti.

#### **B – Elaboratori non in rete**

Il titolare dispone di un PC stand-alone con funzioni di postazione multimediale dislocato nella biblioteca.

#### **C – Elaboratori in rete privata**

Il titolare non dispone di pc in rete privata. Tutti i pc in rete condividono l'accesso alla rete pubblica internet reso disponibile da un router ADSL, un pc nella biblioteca anche se non in rete dispone di una connessione tramite un modem ISDN.

#### **D – Elaboratori in rete pubblica**

##### **PALAZZINA MUNICIPIO**

Numero 21 postazioni fisse, così suddivise e dislocate come segue:

- 01 Elaboratore con funzioni di Server al primo piano nella palazzina Municipio, nell'area classificata come Sala Server / Teleassistenza
- 01 Elaboratore con funzioni di posto lavoro e video conferenza al primo piano nella palazzina Municipio nell'area classificata come Sala Server / Teleassistenza
- 01 Elaboratore con funzioni di firewall al primo piano nella palazzina Municipio nell'area classificata come Sala Server / Teleassistenza
- 03 Elaboratori con funzioni di postazione lavoro al piano terra nella palazzina Municipio nell'area classificata come Ufficio Segreteria / Tributi
- 03 Elaboratori con funzioni di postazione lavoro al piano terra nella palazzina Municipio nell'area classificata come Ufficio Polizia Locale.
- 01 Elaboratore con funzioni di postazione lavoro al piano terra nella palazzina Municipio nell'area classificata come Servizi alla Persona.

- 01 Elaboratore con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Sala Giunta.
- 01 Elaboratore con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio Economico / Contabile
- 01 Elaboratori con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio Segretario comunale
- 04 Elaboratori con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio Amministrativo (Anagrafe, Stato civile, Commercio).
- 01 Elaboratore con funzioni di postazione lavoro al secondo piano nella palazzina Municipio nell'area classificata come Ufficio Tecnico 1 a
- 02 Elaboratori con funzioni di postazione lavoro al primo piano nella palazzina Municipio nell'area classificata come Ufficio Tecnico 1 e 2
- 01 Elaboratore stand-alone (non collegato in rete con altri pc del Comune) con funzione di postazione di lavoro dislocato **nella Biblioteca**, ma collegato alla rete pubblica internet tramite un modem.

Il titolare non dispone di nessun computer portatili o altra periferica simile mobile.

Numero 18 stampanti, dislocate come segue:

- Stampanti dislocate nei vari uffici per le relative esigenze lavorative delle strutture organizzative.

Numero 1 fotocopiatore, dislocate come segue:

- 01 Fotocopiatore dislocato nell'area Segreteria / Tributi .
- 01 Fotocopiatore dislocato nell'area Tecnico 2
- 01 Fotocopiatore dislocato nell'area Amministrativo
- 01 Fotocopiatore dislocato presso la Biblioteca Comunale.

Numero 03 scanner, così suddivise e dislocate come segue:

- Scanner dislocato nell'ufficio dislocati nell'area classificata come Segreteria / Tributi.
- Scanner dislocato nell'ufficio dislocati nell'area classificata come Biblioteca.
- Scanner dislocato nell'ufficio dislocati nell'area classificata come Settore Amministrativo (Anagrafe, Stato civile, Commercio).

Altri strumenti elettronici quali router, switches, dispositivi di backup etc. dislocati nell'area classificata come Sala Server / Teleassistenza.

**E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti**  
Attualmente non sono installati dispositivi.

**F – Altri strumenti (es. basati su dati biometrici, )**

Attualmente non è installato alcun dispositivo.

Dall'analisi di quanto descritto precedentemente otteniamo questa tabella dove la **X** significa che un determinato strumento di trattamento / archiviazione è presente e SI/NO se il trattamento dati è effettuato in tale area.

AREE	TRATTAMENTO DATI	TIPI DI STRUMENTI																
		A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F			
Ufficio Segreteria / Tributi	SI	X	X											X				
Ufficio Polizia Locale	SI	X	X											X				
Ufficio Servizi alla persona	SI	X	X											X				
<b>Sala Giunta</b>	<b>NO</b>	X	X											X				
<b>Ufficio Sindaco</b>	<b>NO</b>	X	X															
Ufficio Economico / Contabile	SI	X	X											X				
Ufficio Segretario Comunale	SI	X	X											X				
Ufficio Amministrativo (Anagrafe, Stato civile, Commercio)*	SI	X	X											X				
Archivio / Magazzino 1 piano	SI		X															
Sala Server / Teleassistenza	SI	X	X											X				
<b>Sala Consiliare</b>	<b>NO</b>																	
Ufficio Tecnico 1 e 2	SI	X	X											X				
Ufficio Tecnico 1a*	SI	X	X											X				
Archivio / Magazzino 2 piano	SI		X															
Archivio sottotetto	SI		X															
Biblioteca	SI	X	X		X									X				
<b>in grassetto le aree dove non si effettuano trattamenti</b>																		
<b>* le aree sono su piani diversi ma collegate da una scala interna.</b>																		

Legenda degli strumenti utilizzati per il trattamento:

**A** – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadio/locale chiuso a chiave
- **A3** quelli custoditi in un'area ad accesso controllato

**B** – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **B3** quelli portatili o altri dispositivi mobili

**C** – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

**D** – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato

- **D2** quelli localizzati in un'area ad accesso controllato
- **D3** quelli portatili o altri dispositivi mobili

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

F – Altri strumenti (es. basati su dati biometrici).

### 1.3 La mappa dei trattamenti effettuati

Incrociando le coordinate di cui ai due paragrafi precedenti e la tabella riepilogativa di tutti i trattamenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare. Il simbolo **X** apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti. Nella tabella di incrocio, si appone un simbolo identificativo di ciascun trattamento, che sta tra l'altro a significare che determinati tipi di dati sono trattati con determinati strumenti.

TIPI DI TRATTAMENTI														
Dati comuni relativi a clienti /cittadini / dipendenti.	X											X		
Dati comuni relativi a fornitori.	X											X		
Dati comuni relativi ad altri soggetti.	X											X		
<b>Dati biometrici relativi al personale e ad altri soggetti.*</b>														
<b>Dati idonei a rilevare la posizione di persone ed oggetti.*</b>														
Dati di natura giudiziaria relativi a clienti, fornitori, cittadini..	X											X		
Dati sensibili al personale, nonché ai candidati per diventarlo	X											X		
Dati di natura sensibile relativi a clienti/fornitori/cittadini.	X											X		
Dati idonei a rivelare lo stato di salute e/o la vita sessuale.	X											X		
Dati idonei a rivelare l'affezione da virus HIV.	X											X		
* attualmente non trattati														
	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F
	TIPI DI STRUMENTI													

Legenda degli strumenti utilizzati per il trattamento:

**A** – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadio/locale chiuso a chiave
- **A3** quelli custoditi in un'area ad accesso controllato

**B** – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **B3** quelli portatili o altri dispositivi mobili

**C** – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

**D** – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato
- **D2** quelli localizzati in un'area ad accesso controllato

- **D3** quelli portatili o altri dispositivi mobili

**E** – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

**F** – Altri strumenti (es. basati su dati biometrici).

Da una prima lettura della mappa, si evince che:

- Tutti i dati indifferentemente dalla natura vengono trattati e/o archiviati in aree che durante l'orario di lavoro non sono ad accesso controllato. Nessuna delle aree di trattamento è considerata in questa sede ad accesso controllato in quanto non esiste nessun dispositivo elettronico che durante l'orario di lavoro possa identificare esattamente l'identità, e memorizzare l'orario di accesso e di uscita di chi accede ad una determinata area. In ogni caso si precisa che le aree di trattamento e relativi archivi **sono da considerarsi aree ad accesso ristretto** in quanto nel mansionario facente parte di questo documento sono fornite agli incaricati dei trattamenti tutte le indicazioni per una corretta gestione dei dati trattati e della loro custodia , nonché per la vigilanza e il controllo delle aree di trattamento in cui direttamente operano.
- Tutti i dati sensibili e giudiziari vengono archiviati in armadi chiusi a chiave.
- Tutti i dati indifferentemente dalla natura vengono trattati e/o archiviati sia con strumenti diversi da quelli elettronici (sostanzialmente archivi cartacei) che con quelli elettronici.
- La totalità dei dati è trattata per quanto riguarda gli strumenti elettronici è trattata con pc in rete pubblica.
- Non sono utilizzati computer portatili o simili soluzioni mobili.
- I dati relativi allo stato di salute / la vita sessuale di cittadini vengono trattati e archiviati in una zona senza accesso controllato (comunque isolabile e chiudibile a chiave) in armadi chiusi a chiave e con strumenti elettronici collegati in rete pubblica.

## 2. Mansionario privacy ed interventi formativi degli incaricati

Per il trattamento dei dati personali, il Titolare:

- **ha nominato i seguenti responsabili**, attribuendo loro incarichi di ordine organizzativo e direttivo, come segue.
  - responsabile per la sicurezza, il cui compito è di progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 Dlgs 196/2003, nella persona di **MOSCATO D.SSA GIOVANNA, incarico Segretario Comunale.**
  - amministratore del sistema informativo, cui è conferito il compito di sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione, nella persona di **SOGGETTI LIVIO, incarico Responsabile del Servizio Segreteria – Affari Generali – Cat. D2;**

Il trattamento dei dati personali viene effettuato solo da **sogetti che hanno ricevuto un formale incarico**, mediante documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati

- modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (**mansionario privacy**), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni. La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nella seguente matrice si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- sull'asse verticale si riportano i dati oggetto di trattamento, quali emergono dall'analisi effettuata nel paragrafo 1. del presente documento
- sull'asse orizzontale si riportano le unità organizzative ("**strutture di riferimento**") in cui si suddivide l'organizzazione del Titolare.
- l'apposizione del simbolo X, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:
- l'apposizione del simbolo **X in grassetto** indica che la primaria responsabilità è dell'unità organizzativa, mentre per le altre unità il trattamento è limitato a talune fasi, strettamente necessarie per lo svolgimento dei propri compiti.

TIPOLOGIA DEI DATI TRATTATI						
Dati comuni relativi a clienti /cittadini / dipendenti.	X	X	X	X	X	X
Dati comuni relativi a fornitori.	X	X	X	X	X	X
Dati comuni relativi ad altri soggetti.	<b>X</b>	X	X	X	<b>X</b>	<b>X</b>
<b>Dati biometrici relativi al personale e ad altri soggetti.*</b>						
<b>Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti.*</b>						
Dati di natura giudiziaria relativi a clienti, fornitori, cittadini, dipendenti e ad altri soggetti.	X			<b>X</b>		
Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile.	<b>X</b>					<b>X</b>
Dati di natura sensibile relativi a clienti/fornitori/cittadini.	<b>X</b>	<b>X</b>	X	X	X	<b>X</b>
Dati idonei a rivelare lo stato di salute e/o la vita sessuale.	<b>X</b>	<b>X</b>		<b>X</b>		
Dati idonei a rivelare l'affezione da virus HIV.		<b>X</b>				
* attualmente non trattati	1	2	3	4	5	6
	<b>Unità organizzative</b>					

La legenda delle unità organizzative ("**strutture di riferimento**") è la seguente:

- 1 – Affari generali
- 2 – Servizi alla persona
- 3 – Amministrativo

4 – Polizia locale

5 – Tecnico 1

6 – Tecnico 2

7 – Economico contabile

Si allegano tabelle indicanti:

1. il responsabile della struttura, i servizi facenti capo alla struttura e il personale assegnato.
2. le banche dati dei trattamenti operati dai vari servizi e relative finalità.

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implicino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia incaricati dal Titolare, che all'esterno, presso soggetti specializzati.

### **3. Analisi dei rischi che incombono sui dati**

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Nella seguente matrice si procede a una stima del grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

<b>GRADO DI INTERESSE PER I TERZI</b>	<b>ELEVATISSIMO</b>				<b>12</b> Dati genetici (non trattati)
	<b>ALTO</b>		<b>6</b> Dati svolgimento di attività economiche		<b>11</b> Dati idonei a rivelare l'affezione da virus HIV
	<b>MEDIO</b>	<b>1</b> Dati comuni clienti /cittadini/dipendenti <b>3</b> Dati comuni altri soggetti		<b>9</b> Dati sensibili clienti/fornitori/cittadini	<b>10</b> Dati stato di salute e/o vita sessuale
	<b>BASSO</b>	<b>2</b> Dati comuni di fornitori	<b>4</b> Dati biometrici personale ed altri soggetti. <b>5</b> Dati idonei a rilevare la posizione	<b>7</b> Dati di natura giudiziaria <b>8</b> Dati sensibili personale	
		<b>BASSO</b>	<b>MEDIO</b>	<b>ALTO</b>	<b>ELEVATISSIMO</b>
<b>PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO</b>					

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati
- quelli che costituiscono una importante risorsa, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
  - al verificarsi di eventi distruttivi (incendi, allagamenti, terremoti...)
  - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)
3. rischio di penetrazione logica nelle reti di comunicazione
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

1	Bianco = molto basso o assente	<b>Legenda:</b>  Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. La scala dei simboli da porre nella casella di intersezione varia secondo la legenda in basso. (per esempio bianco corrisponde un'esposizione al rischio modesta; il rosso significa che l'esposizione al rischio è molto elevata.)
2	Verde = basso	
3	Giallo = medio	
4	Arancione = alto	
5	Rosso = molto alto	

TIPO DI RISCHIO	LIVELLO DI RISCHIO													
Rischio d'area, legato al verificarsi di eventi distruttivi	3	3	3	3	3	2	3	3	2	3	3	2	3	3
Rischio d'area, legato all'accesso non autorizzato nei locali	3	2	1	2	1	3	2	1	3	2	1	3	1	1
Rischio di guasti tecnici di hardware, software e supporti	1	1	1	3	3	4	3	3	4	3	3	4	2	2
Rischio di penetrazione logica nelle reti di comunicazione	1	1	1	1	1	1	1	1	1	4	4	4	1	1
Rischio legato ad atti di sabotaggio e ad errori umani	3	2	2	3	2	2	3	2	2	3	3	3	2	2
	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3	E	F
	<b>TIPI DI STRUMENTI</b>													

Legenda degli strumenti utilizzati per il trattamento:

**A** – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:

- **A1** quelli custoditi in un'area ad accesso non controllato
- **A2** quelli custoditi in un'area ad accesso non controllato in armadi/locali con chiave
- **A3** quelli custoditi in un'area ad accesso controllato

**B** – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:

- **B1** quelli localizzati in un'area ad accesso non controllato
- **B2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

**C** – Elaboratori in rete privata

- **C1** quelli localizzati in un'area ad accesso non controllato
- **C2** quelli localizzati in un'area ad accesso controllato
- **C3** quelli portatili o altri dispositivi mobili

**D** – Elaboratori in rete pubblica

- **D1** quelli localizzati in un'area ad accesso non controllato
- **D2** quelli localizzati in un'area ad accesso controllato
- **D3** quelli portatili o altri dispositivi mobili

**E** – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti.

**F** – Altri strumenti (es. basati su dati biometrici).

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- Il rischio d'area, legato al verificarsi di eventi distruttivi è considerato medio, perché anche se remoto è sempre possibile.

- il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato medio e più basso per le aree ad accesso controllato, rispetto a quanto accade per gli altri luoghi in cui si svolge l'attività, con conseguente diminuzione del rischio.
- il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti obsoleti o comunque meno recenti che hanno parti meccaniche mobili (hard disk, dissipatori ) o elettroniche (alimentatori) che per loro natura sono più soggetti a rotture.
- il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro interconnessi e collegati ad una rete di comunicazione accessibile al pubblico (internet) ed considerata alta in caso di connessione ADSL.
- il rischio legato ad atti di sabotaggio o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati è sempre presente ed è maggiore per quelli che sono collegati in rete pubblica o per le zone non ad accesso controllato o in assenza di un regolamento interno e di una corretta formazione del personale.

Per facilitare la stesura del capitolo successivo si è redatto la seguente tabella che tenuto conto di quanto detto in precedenza rappresenta un'analisi dei principali rischi che gravano sui dati trattati dal Titolare e sulle contromisure da mettere in atto.

FATTORE DI RISCHIO	IMPATTO SUI DATI	CONTROMISURA
<b>Comportamento degli operatori</b>		
- furto di credenziali di autenticazione	Perdita, modifica, furto. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati, sistemi di crittografia dei dati.
- carenza di consapevolezza, disattenzione o incuria	Perdita. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati
- comportamenti sleali o fraudolenti	Perdita, modifica, furto. Trattamenti non consentiti.	Protezione strumenti e locali, formazione del personale, procedure di backup e di ripristino dei dati, sistemi di crittografia dei dati.
- errore materiale	Perdita. Trattamenti non consentiti.	Formazione del personale, procedure di backup e di ripristino dei dati.
<b>Eventi relativi agli strumenti</b>		
- azione di virus informatici o di codici malefici	Perdita e/o temporanea indisponibilità	Utilizzo di software specializzato sempre aggiornato, procedure di backup e di ripristino dei dati, Formazione del personale.
- malfunzionamento, indisponibilità o degrado degli strumenti	Perdita e/o temporanea indisponibilità	Corretta manutenzione e costante aggiornamento, procedure di backup e di ripristino dei dati
- accessi non autorizzati	Perdita, modifica e furto. Trattamenti non consentiti.	Installare Firewall e implementare sistema di autenticazione, procedure di backup e di ripristino dei dati, Formazione del personale, sistemi di crittografia dei dati.
- intercettazione di informazioni in rete	Modifica e furto. Trattamenti non consentiti.	Installare Firewall e implementare sistema di autenticazione, sistemi di crittografia dei dati.
- guasto ai sistemi complementari (impianto elettrico etc..)	Perdita e/o temporanea indisponibilità	Installazione di gruppo di continuità e procedure di backup e di ripristino dei dati.
<b>Eventi relativi al contesto</b>		
- accessi non autorizzati a locali / reparti ad accesso ristretto	Perdita, modifica e furto. Trattamenti non consentiti.	Formazione del personale, antifurto e sistemi di protezione locali., procedure di ripristino dei dati
- asportazione e furto di strumenti contenenti dati	Perdita, modifica e furto. Trattamenti non consentiti.	Formazione del personale, antifurto e sistemi di protezione locali, procedure di ripristino dei dati

- eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti a incuria	Perdita.	Formazione del personale, sistemi di protezione locali, procedure di ripristino dei dati.
- errori umani nella gestione della sicurezza fisica	Perdita e/o temporanea indisponibilità. Trattamenti non consentiti.	Formazione del personale, procedure di ripristino dei dati.

#### **4. Misure atte a garantire l'integrità e la disponibilità dei dati**

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

##### **4.1 La protezione di aree e locali**

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da :

- sono presenti i dispositivi antincendio come previsto del Dlgs 626/94 e successive modifiche.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da :

- I locali al piano terra della palazzina del Municipio presentano accessi con porte blindate.
- Dopo la chiusura degli uffici, le porte di ingresso di tutti gli uffici vengono chiuse.
- Durante l'orario di apertura esiste una continua vigilanza da parte di personale interno.
- Accesso ristretto alle aree in cui si svolgono i trattamenti più critici, mediante:
  - Adozione della regola che i dati più personali (sensibili e giudiziari) sono trattati esclusivamente all'interno dei locali previsti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificamente autorizzati ad accedervi.

Gli impianti ed i sistemi di cui è dotata l'organizzazione:

- appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2006 sono quindi previsti semplicemente interventi di manutenzione o ripristino.

## **4.2 La custodia e l'archiviazione di atti, documenti e supporti**

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole....), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione.

A tale fine, gli incaricati sono stati dotati di :

- cassettiere con serratura
- armadi chiudibili a chiave
- di speciali archivi chiudibili a chiave
- in alcuni casi di cassaforte

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa avviene in luoghi , armadi , casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti

- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede.
- alcuni dipendenti svolgono la mansione di addetti all'archivio.
- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla.

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione dei seguenti accorgimenti :

- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di coloro che hanno richiesto di accedere all'archivio

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari:

- appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2006, sono quindi previsti semplicemente interventi di manutenzione o ripristino.

### **4.3 Le misure logiche di sicurezza**

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si sono adottate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato.
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative.

- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus).
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD....), nei quali siano contenuti dati personali.

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici.

E' impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi:

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

A tale riguardo i computers lavorano in rete operano con un sistema uniforme per l'autenticazione degli utenti basato su un dominio e relativo server Domain Controller. All'accensione ogni computer richiede l'inserimento di credenziali (nome utente e password) che vengono verificate dal server di dominio che concederà un token per utilizzare le risorse di quella macchina secondo quanto profilato nel database SAM del server.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

**Agli incaricati vengono impartite precise istruzioni** in merito ai seguenti punti:

- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:

- immediatamente, non appena viene consegnata loro da chi amministra il sistema
- successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, ....)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che:

- si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione è stato studiato ed impostato per unità organizzativa allegando alla relativa lettera d'incarico, uno schema dei dati trattati dai singoli servizi/uffici facenti parte di quest'ultima. Non viene in genere

studiato per ogni singolo incaricato, ma ogni dipendente del Titolare che sarà assegnato alla unità organizzativa e al relativo servizio, seguirà lo schema di autorizzazione predisposto per tale unità. L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le sue mansioni lavorative.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si è dotati di idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus,

Si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- automatico ogni giorno le nuove impronte virali se disponibili dal sito web del produttore del software antivirus per tutti i pc collegati in rete pubblica.
- Periodicamente le nuove impronte virali installando tramite supporto cd-rom le patches preventivamente scaricate dal sito web del produttore del software antivirus nel caso di strumenti elettronici che non sono in rete .
- Ogni anno alla scadenza di rinnovare l'aggiornamento della versione più aggiornata del software antivirus installato su ogni pc utilizzato all'interno della struttura del Titolare.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idoneo strumento elettronico, comunemente conosciuto come firewall, che il nuovo codice privacy ha reso obbligatorio per i casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo:

- la nostra organizzazione per la protezione degli elaboratori in rete collegati alla rete pubblica internet tramite un router con collegamento ADSL **si è dotata di tale strumento**. La scelta è caduta su una versione software installata su un pc dedicato dotato di 2 schede di rete che garantisce una protezione perimetrale molto efficace e facilmente aggiornabile .

Si è inoltre ritenuto opportuno che tale strumento sarà sottoposto ad aggiornamento, di regola:

- Ogni anno alla scadenza prevista di rinnovare il contratto di aggiornamento del software firewall in modo di ricevere e installare sempre l'ultima versione disponibile considerata la più adatta a fronteggiare le ultime tecniche di intrusione nelle reti informatiche.

Per il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale, si sono adottati particolari accorgimenti, con il fine di:

- rendere temporaneamente inintelligibili tali dati, anche a chi è autorizzato ad accedervi: per l'accesso a tali dati, gli incaricati autorizzati devono inserire una ulteriore parola chiave nel documento in mancanza della quale l'accesso ai dati è impedito.

Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi. A tale riguardo:

1. la nostra organizzazione si è da tempo dotata di una metodologia di comportamento per la protezione da malfunzionamenti degli strumenti elettronici, che prevede che una ditta specializzata su richiesta del responsabile di sistema interno del Titolare effettui visite periodiche con cadenza almeno semestrale per verificare tutti gli strumenti in particolare con i quali si trattano dati sensibili o giudiziari ed effettuare la manutenzione preventiva e d'urgenza dell'hardware installato e dell'aggiornamento dei programmi (firewall, sistema operativo, backup) e della loro corretta configurazione.

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD...), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassette chiuse a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.

- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

Per l'anno 2006, al fine di migliorare ulteriormente l'efficacia di tali misure, sono quindi previsti, oltre agli interventi finalizzati all'aggiornamento, alla manutenzione e al ripristino, investimenti per le finalità indicate nella seguente tabella:

<b>Descrizione dell'investimento</b>
Installazione di un sistema di crittografia al fine di cifrare il contenuto dei file che riguardano lo stato di salute o la vita sessuale e rivelare l'affezione da virus HIV per garantire loro una particolare protezione, in modo che il loro contenuto possa essere letto solo dagli incaricati in possesso di un particolare codice che permetterà l'identificazione degli interessati solo in caso di necessità.

## **5. Criteri e modalità di ripristino dei dati**

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Attualmente **esiste un sistema generalizzato** che crea una copia dei documenti cartacei e degli eventuali altri supporti diversi da quelli elettronici. Attualmente il Titolare è in possesso delle apparecchiature necessarie a scannerizzare i documenti e ha implementato una procedura software previste dal cosiddetto "Protocollo informatico".

I supporti CD-R contenenti le copie verranno:

- archiviati in cassaforte ignifuga.

Per i dati trattati con strumenti elettronici, sono state previste procedure di backup, centralizzate su un server attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Il salvataggio dei dati trattati avviene in tre modi distinti come segue:

- con una frequenza giornaliera da lunedì al sabato.
- con frequenza settimanale.
- Con frequenza annuale.

Si utilizzano supporti differenti, da quelli in cui sono contenuti i dati dei salvataggi eseguiti le volte precedenti e per ciascun salvataggio, si eseguono 2 copie.

Le copie vengono custodite:

- in luoghi protetti nella palazzina del Municipio in cassaforte ignifuga.

Periodicamente, con cadenza almeno semestrale vengono effettuate, sotto la responsabilità dell'amministratore di sistema, delle prove di ripristino, mediante l'esecuzione di appositi test di efficacia delle procedure di salvataggio e di ripristino dei dati adottate.

Attualmente la procedura di backup dei trattamenti effettuati con strumenti elettronici è installata su un server "applicativo" e "dati" che dispone di alcune caratteristiche peculiari richieste da questa tipologia di hardware.

Infatti:

- **dispone di sistemi RAID** (Redundant array of inexpensive disks): si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco, che garantiscono la disponibilità e l'integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema.

Questo server dispone di gruppo di continuità adeguato per garantire il suo funzionamento in caso di brevi interruzioni di corrente.

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari:

- appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2006, sono quindi previsti semplicemente interventi di manutenzione o ripristino.

## 6. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE, se il terzo destinatario non è italiano.

In ogni caso, il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
2. di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
3. di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Qualora il trasferimento dovesse avvenire verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico

Allo stato attuale, il quadro sintetico delle attività trasferite a terzi, che comportano il trattamento di dati personali, è il seguente:

<b>Soggetto esterno</b>	<b>Descrizione sintetica</b>	<b>Dati personali interessati</b>	<b>Data delle verifiche</b>
Comune di Castelli Calepio	Buono mirato per (disabili (18 e-73 anni) ed anziani 74 in su) maggiorenni parzialmente o totalmente non autosufficienti	Idonei a rivelare lo stato di salute Idonei a rilevare lo stato di disabilità Idonei a rivelare malattie mentali Relativi all'utilizzo di particolari ausili protesici Inerenti a caratteristiche o idoneità psichiche	
	Buono mirato per minori e famiglie	Nominativo, indirizzo o altri elementi di identificazione personale	
	Tutela Minori	Codice fiscale o altri dati di identificazione	

ASL	Contributo ex omni	personale	
Tribunali di competenza	Raccolta e inoltro domande e istanze altri enti	Dati relativi alla famiglia e a situazioni personali Lavoro Idonei a rilevare la condizione socio economica Nominativo, indirizzo o altri elementi di identificazione personale Codice fiscale o altri dati di identificazione personale  Beni, proprietà, possessi Nominativo, indirizzo o altri elementi di identificazione personale Codice fiscale o altri dati di identificazione personale	
Ditta che cura accertamenti ICI T&T	Dichiarazioni ICI	Nominativo, indirizzo, codice fiscale, proprietà	
	Avvisi di accertamento e liquidazione ICI recupero insoluti	Nominativo, indirizzo, codice fiscale, proprietà, provvedimento sanzionatorio amministrativo	
Consorzio Nazionale Concessionari	Dichiarazioni ICI	Nominativo, indirizzo, codice fiscale, proprietà	
SIEL	Stampa bollette tributi	Nominativo, indirizzo, codice fiscale, proprietà	
Studio Tecnico Algisi Giosuè	Gestione immobili di proprietà comunale	Nominativo, indirizzo, codice fiscale, proprietà Idonei a rilevare la condizione socio economica	
Azienda Ospedaliera Bolognini – neuropsichiatria infantile	Minori Disabili	Idonei a rivelare lo stato di salute Idonei a rivelare lo stato di disabilità Idonei a rivelare malattie mentali	
CPS – Trescore Balneario	Soggetti Psichiatrici	Idonei a rivelare lo stato di salute Idonei a rivelare lo stato di disabilità Idonei a rivelare malattie mentali Inerenti a caratteristiche o idoneità psichiche	

		Nominativo, indirizzo o altri elementi di identificazione personale Codice fiscale o altri dati di identificazione personale Dati relativi alla famiglia e a situazioni personali	
Provincia di Bergamo – Agenzia per l'integrazione	Soggetti minori stranieri	Nominativo, indirizzo o altri elementi di identificazione personale Codice fiscale o altri dati di identificazione personale Dati relativi alla famiglia e a situazioni personali	
Agenzia delle entrate	Modello 770	Nominativo, indirizzo, codice fiscale, lavoro e attività finanziarie	

Soggetto esterno	Descrizione sintetica	Dati personali interessati	Data delle verifiche
BERGAMO ESATTORIE SPA Via F. Calvi, 9 24122 BERGAMO	Riscossione I.C.I. Recupero insoluti	Dati comuni dei contribuenti	
BANCA POPOLARE DI BERGAMO Filiale di Chiuduno (BG)	Servizio tesoreria e cassa	Dati comuni dei clienti e fornitori - dati sensibili riguardanti le rette ridotte per motivi di reddito	
COLLEGIO REVISORE DEI CONTI - BERGAMO	Servizio di controllo dati contabili e di gestione	Dati di Bilancio – controllo di gestione	
DANSAR AFFISSIONI ENDINE GAIANO (BG)	Accertamento e riscossione tassa pubblicità e diritti pubbliche affissioni	Dati comuni degli utenti	

Soggetto esterno	Descrizione sintetica	Dati personali interessati	Data verifiche
A.s.l.	Dati delle condizioni dell'ospite comunicati all'Asl al fine di stabilire un'adeguata terapia	<b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale. <b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie	
Farmacia Gaio – Chiuduno (BG)	Comunicazione di dati necessari per ottenere la fornitura dei medicinali necessari per le terapie.	<b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Tessera sanitaria, Codice Fiscale ed altri numeri di identificazione personale. <b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie	
Telecom S.P.A.	Accesso ai dati nell'ambito gestione tecnica amministrativa dell'impianto di telefonia fissa messo a disposizione dei dipendenti e degli assistiti .	<b>Dati diversi da quelli sensibili e giudiziari</b> Dati relativi alle telefonate effettuate: numero di telefono, durata chiamata, telefono da cui sono state effettuate.	
Banca Popolare di Bergamo SPA Chiuduno (BG)	Comunicazioni di dati nell'ambito dell'amministrazione dei clienti e fornitori, dei contratti .	<b>Dati diversi da quelli sensibili e giudiziari</b> Dati relativi a controllo dell'affidabilità e della solvibilità.	
Halley Informatica Matelica (MC)	Accesso ai dati nell'ambito della manutenzione relativa al software di gestione della struttura del Titolare.	<b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale. <b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie.	
I.T. Innovazione Snc Montello (BG)	Accesso ai dati nell'ambito della manutenzione relativa al software di gestione della struttura del Titolare.	<b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale. <b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie.	
Halley Informatica Matelica (MC)	Accesso ai dati nell'ambito della manutenzione	<b>Dati diversi da quelli sensibili e giudiziari</b> Dati relativi all'entrata e all'uscita in servizio.	

	dell'impianto elettronico di timbratura dei cartellini dei dipendenti.		
Istituto Comprensivo di Chiuduno	Comunicazioni di dati nell'ambito dell'iscrizione dei bambini a scuola e/o nella gestione delle attività scolastiche	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
Scuola Materna "Lavinia Storti" Chiuduno (BG)	Comunicazioni di dati nell'ambito dell'iscrizione dei bambini a scuola e/o nella gestione delle attività scolastiche	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
Consorzio il So.Co. Città Aperta di Torre Boldone (BG)	A.D.M. (Assistenza domiciliare minori, servizio pre-scuola – progetto giovani – spazio gioco, C.R.E. disabili – assistenza alunni)	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
Cooperativa San Cassiano di Trescore Balneario	Inserimenti lavorativi	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
Cooperativa il Battello di Sarnico	Inserimenti disabili nel mondo del lavoro, centro diurno, attività varie	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
Iris Televita di Gallarate	Gestione Telesoccorso	<p><b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.</p> <p><b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie</p>	
AUSER - Chiuduno	Trasporto persone dializzate presso centri,	Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale.	

	ospedalieri, case di cura etc.	<b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie	
Coop. SERENA di Bergamo (BG)	S.A.D. (Servizio Assistenza Domiciliare)	<b>Dati diversi da quelli sensibili e giudiziari:</b> Nominativo, indirizzo o altri elementi di identificazione personale, Codice Fiscale ed altri numeri di identificazione personale. <b>Dati sensibili</b> dati idonei a rivelare lo stato di salute e a rilevare la gravità o il decorso del quadro clinico di patologie	

## 7. Controllo generale sullo stato della sicurezza

Al responsabile per la sicurezza è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvedono con frequenza settimanale / mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

## 8. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel Marzo 2006 viene firmato in calce da:

- Il sindaco ON. MARTINELLI RAG. PIERGIORGIO, in qualità di rappresentante legale del Titolare.
- Il Segretario Comunale, MOSCATO D.SSA GIOVANNA, in qualità di responsabile per la sicurezza.

Il presente Documento programmatico sulla sicurezza è stato sottoposto per l'approvazione al Consiglio Comunale e successivamente trascritto nel libro che riporta le delibere prese dallo stesso.

L'originale del presente documento viene custodito presso il Municipio del Comune, per essere esibito in caso di controlli.

Una sua copia verrà consegnata.:

- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce:

- la prima redazione del Documento programmatico sulla sicurezza.

*Luogo e data ..... 2006.*

*Firma del rappresentante legale del Titolare.....*

*Firma del responsabile per la sicurezza.....*