CODICE DELLA PRIVACY
D.LGS. 30 GIUGNO 2003 N. 196

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA
(ALLEGATO B. MISURE MINIME DI SICUREZZA)

In riferimento al nuovo Codice della Privacy approvato con D.Lgs. 30 giugno 2003 n. 196, in vigore dal 1° gennaio 2004, abrogativo di tutte le disposizioni normative e regolamentari precedentemente in vigore;

Richiamato l'Allegato B del Decreto succitato;

Si provvede a redigere il presente documento programmatico per la sicurezza anche tenuto conto e sulla scorta di quanto già adottato con delibera della Giunta Comunale n. 18/2000 e n. 65 del 28/6/2000.

Il presente documento di pianificazione della sicurezza dei dati in questo ente, viene redatto confermando sostanzialmente che i dati oggetto di trattamento sono quelli già elencati nell'allegato alla delibera della Giunta Comunale del 28 giugno 2000 n. 65 *(Documento per le attività di interesse pubblico. Ulteriori misure di salvaguardia. Orientamenti. Banche Dati. Determinazioni*), con il quale venivano individuate le attività che perseguono finalità di interesse pubblico e le relative banche dati, nonché i vari responsabili del trattamento e della gestione dei dati, e quelli legati alle novità introdotte dalle leggi in materia demografica (DPR 396/2000, Prestazioni Sociali ecc.) ed al nuovo Codice della Privacy.

Il presente documento programmatico per la sicurezza viene redatto dopo una attenta valutazione dei rischi a cui possono essere sottoposti i dati trattati, adottando nel contempo un piano per la misurazione ed eventualmente riduzione degli stessi. Nel quadro generale di tale valutazione si inseriscono a pieno titolo sia gli interventi formativi degli incaricati del trattamento, volti ad evidenziare i rischi che incombono sui dati, sensibilizzando il personale sulla necessità informativa circa l'aggiornamento delle misure minime da adottare, sia tutta una serie di misure protettive dei sistemi informatici, comprensivi di antivirus, costantemente attualizzati, che di backup settimanali.

In questo contesto si evidenzia il distinguo tra sistema di trattamento con strumenti informatici e gestione dati non informatizzati e si specifica che il sistema informatico, per i dati da tutelare, è concepito, nel suo complesso, con garanzie tecniche di assoluta inaccessibilità esterna.

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

19.1 – Elenco dei trattamenti di dati personali.

I trattamenti dei dati personali sono indicati nella deliberazione della Giunta Comunale n. 65 del 28/6/2000. Tra questi riguardano:

- Dati sensibili

  - il trattamento dei dati sul personale ai fini della elaborazione delle buste paga (dati relativi alle opinioni sindacali)(attività svolte all'esterno dalla ditta incaricata ALMA o altre);
  - il trattamento dei dati relativi alle malattie del personale dipendente, limitatamente al ricevimento e conservazione del certificato medico (dati inerenti la salute)(attività svolta senza l'ausilio di elaboratori elettronici);
  - trattamento dei dati relativi alla concessione del contrassegno invalidi da parte dell'ufficio di polizia municipale (dati relativi la salute)(attività svolta senza l'ausilio di elaboratori elettronici);
  - trattamento dei dati relativi alle origini etniche nella gestione dei servizi demografici (origine etnica)(dati trattati con elaboratori elettronici);
  - trattamento di dati per comunicazioni delle cause di decesso a soggetti pubblici esterni (ASL)(dati inerenti la salute);

- Dati giudiziari

  - raccolta e consultazione dei certificati del casellario giudiziario e dei carichi pendenti ai fini del rilascio delle licenze di polizia amministrativa e simili e della verifica dei requisiti della capacità a contrattare con la pubblica amministrazione (trattamento effettuato con e senza l'ausilio di elaboratori elettronici);
  - raccolta e consultazione dei certificati del casellario giudiziario ai fini della verifica dei requisiti della capacità elettorale (trattamento effettuato con e senza l'ausilio di elaboratori elettronici);
  - notificazione di atti per conto della Procura della Repubblica o per conto della polizia giudiziaria (trattamento effettuato con e senza l'ausilio di elaboratori elettronici);

19.2 – Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati personali deriva dalla deliberazione della Giunta Comunale n. 65 del 28/06/2000 e aggiornamenti, che individua gli incaricati del trattamento con le integrazioni e gli aggiornamenti successivi per determinazione di individuazione dei responsabili di procedimento e di affidamento a ditte esterne la manutenzione dell'hardware e del software in dotazione agli uffici; inoltre si richiamano i provvedimenti di individuazione amministratori di sistema o, comunque, di preposti alla gestione degli elaboratori elettronici.

19.3 – Analisi dei rischi che incombono sui dati.

Al fine di individuare ed applicare adeguate misure volte a garantire la sicurezza del sistema informativo, è compito dei Responsabili valutare dinamicamente e costantemente:

- la vulnerabilità sia degli elementi costitutivi l'architettura del sistema informativo, sia dei dati che in esso sono collocati
- i rischi cui i dati sono soggetti.

A tale scopo si rilevano le seguenti minacce:

- distruzione materiale dei supporti cu sui sono registrati i dati;
- danneggiamento dei supporti con conseguente inintelligibilità dei dati;
- cancellazione dei dati;
- accesso abusivo ai dati;
- trattamento dei dati eccedente alle finalità per cui vengono trattati;
- alterazione logica dei dati;
- trattamento abusivo tramite procedure o programmi per elaboratore autorizzati;
- danneggiamento o manomissione, fisica o logica, delle apparecchiature e dei dispositivi per l'elaborazione e/o la trasmissione dei dati.

19.4 – Le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.

Per i dati trattati con elaboratori elettronici

- creazione di password di accesso sia al sistema che ai software (autenticazione informatica e utilizzazione di un sistema di autorizzazione) e misure organizzative atte a garantire l'accesso per gruppi di incaricati, il tutto come dalla deliberazione della Giunta Comunale citata e per quanto disposto già in essere;

- procedure di conservazione delle password mediante sigillatura in busta chiusa e conservazione nella cassaforte (adozione di procedure di gestione delle credenziali di autenticazione)
- salvataggi dei lavori periodici e gruppo di continuità (adozione di procedure per la custodia di copie di sicurezza, ripristino della disponibilità dei dati e dei sistemi)
- utilizzazione di un sistema antivirus con aggiornamento delle definizioni dei nuovi virus automatica ad ogni accesso ad internet (protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici)
- disaster recovery: misure operative per scongiurare gravi eventi dannosi

Per gli archivi cartacei

- sistemazione del materiale cartaceo riferibile ai servizi demografici in armadi metallici chiusi a chiave, accessibili dagli addetti all'ufficio (previsione di procedure per la conservazione di determinati atti in archivi ad accesso e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati);
- misure organizzative dirette alla corretta conservazione dei documenti realizzate da ciascun responsabile,
- misure dirette a consentire che i dati sensibili da trattare oralmente da parte degli uffici demografici siano trattati in appositi locali chiusi.

Misure da adottare

Per gli elaboratori elettronici ciascun responsabile cura che gli incaricati del trattamento cambino con frequenza semestrale o minore ove richiesto per legge, le password di accesso al sistema ed ai singoli software e provvedano ad attuare quanto previsto dall'art. 34 D.Lgs. 196/2003 segnatamente a:

a) autenticazione informatica – ciascun soggetto incaricato del trattamento dei dati provvede personalmente a cambiare periodicamente la propria password di accesso al sistema e ai singoli software
b) adozione di procedure di gestione delle credenziali di autenticazione, gestite secondo le norme del D.Lgs. 196/2003. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata, conosciuta solamente dal medesimo. Ad ogni incaricato sono assegnate individualmente una o più credenziali per l'autenticazione. E' prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di

caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi o minore frequenza ove richiesto per legge, ove il sistema informatico ne consenta la gestione diretta da parte dell'interessato. Gli applicativi possono essere interessati da cambi di password con frequenza minore, o non interessati dai cambi in condizioni ordinarie, se al personal computer si può accedere solamente con password. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Il responsabile del trattamento impartisce istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

c) Utilizzazione di un sistema di autorizzazione. Il sistema di autorizzazione consente che gli incaricati siano individuati per profili di autorizzazione di ambito diverso. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. Il sistema di autorizzazione sopra descritto verrà attuato quando si realizzerà la prevista messa in rete dei software, con conseguenti profili di accesso differenziati per incaricati, alcuni profili di mera lettura, altri profili di intervento sul software. Per l'anno in corso vengono mantenuti i profili come in essere, salvo modifiche necessarie per la funzionalità del sistema.

d) Aggiornamento periodico ove occorra dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici. Nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione, a cura dei responsabili del trattamento. L'aggiornamento avviene ove occorrente per mutamenti gestionali o funzionali.

e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici. Ciascun incaricato provvede alla protezione dei personal contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del c.p. mediante l'attivazione di idonei

strumenti elettronici (antivirus) da aggiornare con cadenza almeno semestrale, precisando che quelli in uso sono aggiornabili automaticamente ad ogni accesso ad internet. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (antivirus) e a correggerne difetti sono effettuati almeno annualmente, mediante acquisto degli appositi rinnovi a cura del responsabile della posizione organizzativa ed installazione a cura di ciascun incaricato. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

19.5 – La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al punto 23 – allegato B – D.Lgs. 196/2003.

Devono essere svolte con la periodicità indicata dalla ditta fornitrice del software a cura degli incaricati le copie di back up dei dati relativi all'anagrafe, all'elettorale, allo stato civile, al protocollo, ai tributi e alle liste di carico del servizio idrico integrato, della banca dati ICI, della contabilità. In caso di distruzione o danneggiamento dei dati, sono previsti gli interventi delle società venditrici del software ed incaricati della manutenzione, in tempi brevissimi.
Il backup viene effettuato nell'ambito del server e non a livello di singole postazioni, di norma.

19.6 – La previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Gli interventi formativi sono svolti, compatibilmente con le ridotte dimensioni organizzative di questo Ente, a cura dei fornitori di software nei confronti degli incaricati, per quanto riguarda gli aspetti di dettaglio di gestione dei singoli software, mentre le informazioni di carattere giuridico erano state fornite dal Segretario Comunale nel documento sulle misure minime di sicurezza allegato alla deliberazione della Giunta Comunale n. 65 del 28/6/2000, che con il presente documento si richiama integralmente. Continuano ad essere fornite indicazioni verbali ogni qual volta viene sollevato un problema interpretativo da parte dei responsabili o degli incaricati. La formazione del personale è programmata anche al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. Il presente documento è inoltre reso disponibile agli incaricati e costituisce intervento formativo e istruzione per il trattamento.

19.7 – La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

Il responsabile dei dati relativi al personale per l'elaborazione degli stipendi cura che le comunicazioni alla ditta esterna vengano effettuate con le cautele fisiche (buste chiuse ecc.) idonee ad evitare abusivi accessi da parte di terzi. Analoghe cautele per le comunicazioni nei confronti del concessionario della riscossione e del tesoriere.

Per il futuro dovranno essere adottati ulteriori accorgimenti, come la doppia busta e la stampigliatura sulla busta contenente dati sensibili di una apposita dicitura.

19.8 – Dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 D.Lgs. 196/2003. Individuazione dei criteri da adottare per la cifratura o la separazione di tali dati dagli altri dati personali dell'interessato.

Il presente punto non risulta riferibile soggettivamente al comune.

Si rileva che sono già adottate misure di sicurezza come esposte. Unitamente al presente programma si assumono le misure minime di sicurezza che si allegano.

Si richiamano inoltre i regolamenti relativi al trattamento di dati attualmente adottati presso il Comune di Revello.

Revello, 17 marzo 2010

IL SINDACO – rappresentante del titolare del trattamento
Geom. Ugo Motta

Ai dipendenti comunali
in qualità di incaricati del
Trattamento dati personali

Oggetto: misure di sicurezza dei dati personali - direttiva

Si dispongono, richiamando l'attenzione dei dipendenti incaricati del trattamento dei dati personali, le seguenti misure di sicurezza da adottare in seguito all'entrata in vigore del decreto legislativo n. 196/2003, aggiuntive rispetto a quelle indicate nelle deliberazioni della Giunta Comunale n.18/2000 e n 65/2000 .

In particolare, si richiamano gli articoli da 31 a 36 e l'allegato b oltre alle norme di cui agli articoli 18 e seguenti e 59 e seguenti.

In via immediata è necessario che i singoli incaricati del trattamento adottino alcune misure di sicurezza in aggiunta a quanto già realizzato:

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati **dotati di credenziali di autenticazione** (password) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in **un codice per l'identificazione dell'incaricato** associato a una **parola chiave** riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Per il rispetto di quanto indicato al precedente punto 2 si raccomanda che ogni parola chiave sia conosciuta esclusivamente dall'incaricato, con possibilità di conoscenza da parte di altri incaricati, in caso di flessibilità organizzativa, che prevede ciò come ordinaria la sostituzione degli addetti agli uffici in caso di assenza dell'incaricato principale, ad esempio per il protocollo, e i servizi demografici.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Costantemente sono formulate e concordate specifiche direttive circa le cautele finalizzate alla segretezza della password e il divieto di accesso ai computer da parte di personale estraneo agli uffici

5. La parola chiave, quando è prevista dal sistema di autenticazione, **è composta da almeno otto caratteri** oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Si raccomanda la puntuale osservanza delle misure indicate dal precedente punto 5. Ogni incaricato dovrà procedere con cadenza semestrale o trimestrale come sopra, alla modifica sia della password di accesso al sistema, che delle singole password di accesso ai singoli software, password che dovranno avere le caratteristiche ivi prescritte.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Per la particolare organizzazione degli uffici comunale è indispensabile, per una funzionalità degli stessi, che gli addetti agli uffici si possano sostituire in caso di assenza e pertanto è prevista in linea di principio la non utilizzabilità della parola chiave da parte di altri incaricati, fatta eccezione per quelli chiamati a sostituire gli assenti secondo un criterio di normalità, per cui può configurarsi un incarico congiunto (es. protocollo e servizi demografici).

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Gli incaricati non debbono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Alle istruzioni di cui al punto 9 provvede l'incaricato per gestione attività informatica; si raccomanda, comunque, già fin d'ora, lo spegnimento del computer alla fine di ogni turno di lavoro e il divieto di far accedere ai computer soggetti estranei all'amministrazione.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Coerentemente con il flessibile assetto organizzativo di questo Ente e con la necessità che la gestione dei servizi (soprattutto demografici e protocollo) non può essere interrotta in caso di

assenza dell'incaricato principale, è previsto che le password vengano conservate con modalità e procedure idonee (es.in busta chiusa e sigillata)a cura di ciascun incaricato, che le consegnerà ad altro dipendente il quale conserverà le buste chiuse nella cassaforte.
Ogni sei mesi, al cambio delle password, le buste contenenti le password del semestre precedente verranno distrutte .
In caso di prolungata assenza dell'incaricato dei trattamenti per i quali non sono previsti meccanismi di flessibilità, l'incaricato in via di sostituzione potrà aprire la busta chiusa al fine di utilizzare la password ivi contenuta.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Nel nostro ente molti sono i dati destinati alla diffusione, come tutti i dati contenuti nelle deliberazioni del Consiglio e della Giunta (esclusi i dati sensibili), le determinazioni dei responsabili di servizio, le concessioni, le autorizzazioni e in genere gli atti amministrativi per i quali è esercitabile il diritto di accesso.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

Nel nostro ente sono stati creati profili diversi di accesso alla rete LAN, alcuni profili di sola lettura, altri profili di lettura ed intervento sui programmi. Ai vari profili di accesso sono collegate diverse parole chiave.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Tali profili di autorizzazione sono creati al momento della messa in rete dei software.

14. Periodicamente è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Ogni incaricato dovrà fare presente indicativamente nel mese di marzo di ogni anno, la necessità di modificare o di conservare i profili di autorizzazione, precisando che per quest'anno i profili di autorizzazione in essere sono confermati.

Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico eventuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Si intende fin d'ora come ambito operativo di ciascun incaricato, quanto inerente la propria sfera di attività professionale all'interno del Comune, come disposta da: proclamazione o elezione, provvedimenti di nomina, da preposizione a servizio o ufficio, contratto di lavoro, mansioni verbalmente affidate afferenti il proprio ambito di competenza; oppure, nel caso di soggetti esterni, quanto afferente l'incarico affidato.

Gli incaricati del trattamento coincidono pertanto con il Sindaco, i dipendenti comunali, gli assessori, i consiglieri, le imprese esterne con affidamento in outsourcing, altri soggetti ai quali sono affidati compiti, attività, servizi, forniture comportanti il trattamento dei dati personali.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

I computer sono dotati di antivirus annuali aggiornati automaticamente ad ogni accesso ad internet.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

La funzione di cui sopra è svolta dall'antivirus, che si aggiorna automaticamente ad ogni accesso ad internet.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
Si richiama quindi l'attenzione degli incaricati, sullo scrupoloso rispetto delle disposizioni sulla frequenza del salvataggio dei dati; in particolare, ogni incarico deve provvedere al salvataggio dei dati la cui perdita può compromettere la funzionalità delle attività e dei servizi, sul server.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

Nel nostro ente i principali dati sensibili trattati con strumenti elettronici sono quelli relativi ai servizi demografici (origine etnica). Attualmente sono protetti con i sistemi descritti sopra, principalmente con la password di accesso e dell'antivirus.Inoltre i locali sono opportunamente protetti così come le attrezzature.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

I backup contenenti dati devono essere conservati o in cassaforte o in armadi o cassetti chiusi a chiave, e la chiave deve essere custodita a cura dell'incaricato.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a **sette giorni.**

Per l'attuazione di quanto sopra sono disposti appositi contratti di manutenzione del software con la ditta fornitrice.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie …
(il n. 24 non è applicabile al Comune)

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
Si raccomanda agli incaricati di rispettare rigorosamente quanto indicato al n. 25, chiedendo all'installatore **la dichiarazione di conformità** al disciplinare tecnico contenuto nell'allegato b al decreto legislativo n. 196/2003.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
Si ritiene il n. 26 non applicabile agli enti pubblici.

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Gli incaricati debbono attenersi a regole di cautela, sicurezza, conservazione dei dati conformemente al d. lgs. N. 196/2003..

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti **sono controllati e custoditi dagli incaricati** fino alla restituzione in **maniera che ad essi non accedano persone prive di autorizzazione**, e sono restituiti al termine delle operazioni affidate.

29.L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Si stabilisce di redigere un elenco dei soggetti in possesso delle chiavi del Comune oltre ai dipendenti comunali (disposizione in atto ad opera dell'ufficio tecnico).
Per riunioni non strettamente istituzionali è previsto l'utilizzo di sale a piano cortile non interferenti con gli uffici. Qualora si rendesse necessario l'uso di locali al piano superiore, come già in atto, si dispone idonea chiusura dei locali uffici e, occorrendo, la presenza di addetti autorizzati.
Con l'occasione si rammenta che l'articolo 169 del Codice sulla protezione dei dati personali prevede per la omessa adozione delle misure di sicurezza sanzioni penali ed amministrative.

Revello, 17.3.2010

IL SINDACO – rappresentante del titolare del trattamento- geom. Ugo Motta