COMUNE DI VILLANOVA MONFERRATO

PROVINCIA DI ALESSANDRIA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE N. 20 DEL 28/03/2011

OGGETTO: AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI (DPS)

L'anno duemilaundici addì ventotto del mese di marzo alle ore 10,30 nella sala delle riunioni.
Esaurite le formalità prescritte dalle vigenti norme in materia vennero per oggi convocati i componenti di questa GIUNTA COMUNALE essendo presenti i signori:

		Presente	Assente
Mauro CABIATI	**Sindaco**	x	
Renata AVONTO	**Vice sindaco**		x
Marcello COPPI	**Assessore**	x	
Angelo MILANI	**Assessore**	x	
Giuseppe DE GIORGIO	**Assessore**	x	

Presiede il Sindaco Mauro Cabiati
Assiste il Segretario Comunale Dott. Pierangelo Scagliotti.
Il Presidente, riconosciuta legale l'adunanza, dichiara aperta la seduta.

LA GIUNTA COMUNALE

Premesso che:

- ai sensi dell'art. 28 del D.Lgs. 30/06/2003 n. 196 il Comune di Villanova Monferrato assume la veste formale e giuridica di titolare del trattamento dei dati personali operato nello svolgimento delle proprie funzioni e servizi;
- l'art. 31, comma 1, del D.Lgs. 30/06/2003 n. 196, stabilisce che i dati personali oggetto di trattamento "sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta";
- nel quadro dei più generali obblighi di sicurezza di cui all'art. 31 predetto, il Titolare del Trattamento è comunque tenuto ad adottare le misure minime individuate dal codice, volte ad assicurare un livello minimo di protezione dei dati personali, ai sensi dell'art. 33 del D.Lgs. 30/06/2003 n. 196;
- il complesso delle misure tecniche, informatizzate, organizzate, logistiche e procedurali di sicurezza, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 33 D.Lgs. 30/06/2003 n. 196 è stato definito con il Disciplinare tecnico allegato sotto la lettera B) al codice della Privacy contenuto nel D.Lgs. 196/2003;

Atteso che:

- l'art. 36 del D.Lgs. 30/06/2003 n. 196 prevede che il Disciplinare tecnico sia aggiornato periodicamente con Decreto del Ministero della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore;
- a norma della lettera g) dell'art. 34, comma 1, del D.Lgs. 30/06/2003 n. 196 il titolare del trattamento adotti "un aggiornato documento programmatico sulla sicurezza" per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture proposte al trattamento dei dati stessi:
  - i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
  - i criteri e le procedure per assicurare l'integrità dei dati;
  - i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
  - l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni;
  - che l'efficacia delle misure di sicurezza come sopra determinate deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale;
- che a norma del punto 19 del disciplinare tecnico (allegato B al codice) entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un Documento Programmatico sulla Sicurezza;

Considerato che:

- a fonte delle finalità delle misure di sicurezza date all'art. 31, nonché degli standard minimi delineati dal Disciplinare tecnico, risulta opportuno riportare in un unico Documento Programmatico a contenuto organizzativo ed operativo gli elementi di riferimento necessari per l'adozione, l'adeguamento, lo sviluppo, l'implementazione gestionale delle misure di sicurezza;
- tali elementi si configurano come componenti costitutive di un documento programmatico, rispondente a quanto previsto dalla normativa, volto a fornire adeguate garanzie di fondo per i trattamento dei dati personali da parte degli operatori dell'Amministrazione Comunale, attraverso la definizione di misure di sicurezza organizzative, fisiche e logiche;

- tali misure di sicurezza, periodicamente riviste e comunque soggette a reimpostazione complessiva annualmente, costituiscono il riferimento per la definizione, mediante apposite ed eventuali determinazioni dirigenziali, di soluzioni operative dettagliate, correlate alle specificità e alla complessità dei singoli settori;

Valutati i contenuti del provvedimento del Garante per la protezione dei dati personali del 29/02/2000, finalizzato a sollecitare tutti i soggetti pubblici e privati al rispetto di quanto previsto dal D.P.R. 318/1999;

Ritenuto opportuno approvare il documento programmatico sulla sicurezza dei dati personali aggiornato alla data odierna;

Tenuto conto che risulta necessario conferire al presente provvedimento immediata eseguibilità al fine di poter attivare tempestivamente i processi di definizione e di applicazione delle misure di sicurezza per i trattamenti di dati personali sviluppati dai settori dell'Amministrazione Comunale;

Visto il D.Lgs. 18/08/2000 n. 267;
Visto lo Statuto del Comune di Villanova Monferrato;
Visto il Regolamento sul trattamento dei dati personali;

Dato atto che il Segretario Comunale ha espresso parere favorevole per quanto di competenza ai sensi dell'art. 49, 1° comma del D.Lgs. 18.08.2000 n. 267 relativamente alla regolarità tecnico-amministrativa;

A voti unanimi favorevoli espressi nei modi e forme di legge,

D E L I B E R A

APPROVARE il documento e piano operativo per le misure di sicurezza minime inerenti l'attività degli uffici del Comune di Villanova Monferrato in ordine al trattamento di dati personali, aggiornato alla data odierna, come configurato nell'allegato DPSS, parte integrante e sostanziale del presente atto.

DI DICHIARARE, a voti unanimi favorevoli, la presente deliberazione immediatamente eseguibile per l'urgenza, ai sensi dell'art.134, 4° comma del D. Lgs. 267 / 2000.

=====

Comune di Villanova Monferrato

Documento Programmatico sulla Sicurezza

(Redatto ai sensi del Decreto Legislativo 196/2003)

Anno 2011

Versione n. 01/2011 del:_28.03.2011

Firma del Legale Rappresentante del Titolare:

_____

(Mauro Cabiati)

A. Premessa, Scopo e Campo di Applicazione

Il presente documento é redatto in conformità al Decreto Legislativo 196/2003 ed all'esempio fornito dall'Ufficio del Garante per la Protezione dei Dati Personali in data 11/06/2004. Si applica al trattamento elettronico e non elettronico di dati personali effettuato da Comune di Villanova Monferrato ed é redatto allo scopo di definire criteri e modalità per garantire la sicurezza dei dati personali e del loro trattamento come richiesto dalla Legge.

Per dato personale, si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

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

Il presente documento sarà aggiornato almeno su base annuale, a meno di particolari e significative evoluzioni della struttura organizzativa, della tipologia di dati trattati o degli strumenti tecnologici che impongano una revisione anticipata.

Gli scopi di dettaglio di questo documento sono:

- elencare i trattamenti di dati personali effettuati;
- definire la distribuzione dei compiti e delle responsabilità in relazione a tali dati;
- fornire un'analisi dei rischi di sicurezza che incombono su tali dati;
- elencare le misure di sicurezza atte a mitigare i rischi identificati;
- descrivere criteri e modalità di ripristino di accesso ai dati in caso di loro danneggiamento;
- definire gli interventi formativi sul personale incaricato del trattamento;
- definire i criteri per garantire l'adozione delle misure minime di sicurezza identificate in questo documento, quando il trattamento dei dati personali sia affidato all'esterno (fornitura di servizi e outsourcing);

- definire i criteri tecnici ed organizzativi da adottare per il trattamento di dati personali sensibili.

B. Elenco dei Trattamenti dei Dati personali.

Nell'ambito dell'organizzazione di Comune di Villanova Monferrato sono stati individuati i seguenti trattamenti e le relative basi dati:

Trattamenti *(Finalità)*	***Ufficio di Riferimento***	***Categoria Interessati***	***Base Dati***	***Luogo di Custodia***	***Tipo Dati***	***Strumenti Informatici e Non Inform.***	***Trattamento Interno, Esterno o Misto***
Anagrafe (previsto dalla Legge)	Anagrafe	Residenti	anagrafe-informatico	Sede Municipale	C	Database Generico	Interna
			anagrafe cartaceo	Sede Municipale	C, S	Cartaceo	Interna
Stato Civile (istituzionale)	Stato Civile	Dipendenti	Stato Civile Informatico	Sede Municipale	C, S	Database Generico	Interna
Prenotazione	Amministrativo	Residenti	Trasporti	Sede	C,	Sun	Mista

trasporti convenzionati CRI (Fornitura servizio di trasporto gratuito presso ASL locale)			convenzionati CRI	Municipale	M	OpenOffice	
Protocollo (istituzionale)	Amministrativo	Dipendenti	Protocollo	Sede Municipale	C, S, G, M	Database Generico	Interna
Albo Pretorio (istituzionale)	Amministrativo	Pubblico (generico)	Albo Pretorio	Sede Municipale	C	Sun OpenOffice	Interna
			Nuovo Albo Pretorio online	Sede Municipale	C	Microsoft SQL Server	Interna
Notificazioni (istituzionale)	Amministrativo e Polizia Municipale	Dipendenti	Registro Notificazioni	Sede Municipale	C	Sun OpenOffice	Interna
Gestione del personale (gestione degli adempimenti obbligatori relativi al personale)	Ragioneria e contabilità	Dipendenti	Personale dipendente e collaborazioni	Sede Municipale	C, S	Cartaceo	Interna
Gestione Tributi (accertamento e riscossione tributi)	Ufficio Tributi	Contribuenti	Tributi locali ed erariali, accertamento e riscoss	Sede Municipale	C, S	Database Generico	Mista
Gestione servizi scolastici erogati dal Comune (verifica e riscontro pagamenti servizi scolastici)	Amministrativo	Studenti	Utenti servizi scolastici	Sede Municipale	C	MySQL	Interna
Gestione archivio raccolta rifiuti solidi urbani e (Gestire lassegnazione dei contenitori in comodato)	Amministrativo	Residenti	Gestione raccolta rifiuti differenziata	Sede Municipale	C	MySQL	Mista

Gestione cimiteriale (Situazione contratti di concessione loculi e disponibilità residua)	Segreteria	Pubblico (generico)	Gestione cimitero comunale	Sede Municipale	C	MySQL	Interna

Legenda. Tipo Dati:
C = dati personali Comuni;
S = dati personali Sensibili;
G = dati personali Giudiziari;
M = dati personali Medico-Sanitari.

Titolare del trattamento di questi dati é Comune di Villanova Monferrato nella persona del suo Legale Rappresentante Mauro Cabiati, Sindaco pro tempore .

C. Distribuzione dei Compiti e delle Responsabilità

c.1 Responsabilità Generali

Tutti i dipendenti ed assimilati, collaboratori a qualunque titolo (p.e. consulenti), fornitori di servizi di Comune di Villanova Monferrato ed in particolare i responsabili, incaricati del trattamento di dati personali e personale tecnico, ognuno per i suoi compiti e le proprie responsabilità, dovranno conformarsi alle disposizioni generali di sicurezza del presente documento e ad ogni altra relativa disposizione operativa del Titolare o dei Responsabili del trattamento dei dati personali.

In particolare, tutti dovranno usare i dati personali di cui Comune di Villanova Monferrato è titolare del trattamento solo per le finalità d'ufficio secondo l'incarico e le disposizioni ricevute.

c.2 Responsabilità Particolari

Titolare del trattamento, ai sensi dell'art. 28 d. lgs. 196/03, è Comune di Villanova Monferrato, con sede in PIAZZA FINAZZI 8, 15030 Villanova Monferrato (AL) qui di seguito denominata "amministrazione", nella persona del suo legale rappresentante pro-tempore Mauro Cabiati nato a San Giorgio Monferrato il 15/12/1937.

Data la facoltatività della nomina, il Titolare ha ravvisato l'opportunità di non procedere alla nomina di alcun Responsabile del Trattamento dei Dati Personali.

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta

autorità del Titolare, attenendosi alle istruzioni impartite. Il Titolare individua, nomina ed incarica per iscritto gli Incaricati del trattamento dei dati personali. Per eventuali Incaricati esterni all'organizzazione, si applica anche quanto previsto al paragrafo H di questo documento.

D. Analisi dei Rischi

Scopo della Analisi dei Rischi è individuare e quantificare i rischi che incombono sui trattamenti di dati personali e sui dati stessi trattati dall'Amministrazione, riguardanti:

- la perdita o distruzione accidentale o dolosa, anche parziale, dei dati;
- l'accesso o la diffusione accidentale o dolosa non autorizzata dei dati;
- i trattamenti dei dati non consentiti o non conformi alle finalità della raccolta.

La metodologia adottata è AXAM in auto-valutazione.

Si sono identificate comuni minacce fisiche (incendio, eventi idrogeologici, atti di forza, furto tradizionale di apparati o parti di essi), comuni minacce logiche (malfunzionamenti hardware e software, accessi non autorizzati da rete o da sistemi, furto o sottrazione di supporti di memorizzazione) e comuni minacce organizzative (sottrazione di credenziali, frode, errori operativi, scarsa formazione).

Si sono quindi identificati gli eventuali fattori esistenti che mitighino tali minacce (p.e. sistemi anti-incendio, sistemi anti-intrusione, politiche di salvataggio dei dati, sistemi firewall di rete, esistenza di siti alternativi di custodia, politiche di aggiornamento del software, sistemi anti-virus, etc.).

Incrociando minacce e fattori mitiganti, per ogni base dati sono stati individuati i seguenti livelli di rischio fisico (relativi al contesto):

Base Dati	Incendio	Evento Idrogeol.	Guasto HW	Atti di Forza	Furto
anagrafe-informatico	BASSO	BASSO	BASSO	BASSO	BASSO
anagrafe cartaceo	BASSO	BASSO	**N.A.**	BASSO	BASSO
Stato Civile Informatico	BASSO	BASSO	BASSO	BASSO	BASSO
Tributi locali ed erariali, accertamento e riscossione	BASSO	BASSO	BASSO	BASSO	BASSO
Ragioneria e Contabilità	BASSO	BASSO	BASSO	BASSO	BASSO
Personale dipendente e collaborazioni	BASSO	BASSO	**N.A.**	BASSO	BASSO
Urbanistica, edilizia, ambiente	BASSO	BASSO	BASSO	BASSO	BASSO
Servizi Sociali	BASSO	BASSO	**N.A.**	BASSO	BASSO
Trasporti convenzionati CRI	BASSO	BASSO	BASSO	BASSO	BASSO
Albo Pretorio	BASSO	BASSO	BASSO	BASSO	BASSO
Registro Notificazioni	BASSO	BASSO	BASSO	BASSO	BASSO
Protocollo	BASSO	BASSO	BASSO	BASSO	BASSO
Utenti servizi scolastici	BASSO	BASSO	BASSO	BASSO	BASSO

Nuovo Albo Pretorio online	BASSO	BASSO	BASSO	BASSO	BASSO
Rubrica contatti	BASSO	BASSO	BASSO	BASSO	BASSO
Archivio Atti e Provvedimenti	BASSO	BASSO	BASSO	BASSO	BASSO
Gestione raccolta rifiuti differenziata	BASSO	BASSO	BASSO	BASSO	BASSO
Gestione cimitero comunale	BASSO	BASSO	BASSO	BASSO	BASSO

i seguenti livelli di rischio logico (relativi agli strumenti):

Base Dati	Malfunzionam. SW Applic.	Malfunzionam. SW di Sistema	Virus o Sabotaggio Informatico	Intercettazione o Intrusione
anagrafe-informatico	BASSO	BASSO	BASSO	BASSO
anagrafe cartaceo	**N.A.**	**N.A.**	**N.A.**	BASSO
Stato Civile Informatico	BASSO	BASSO	BASSO	BASSO
Tributi locali ed erariali, accertamento e riscossione	BASSO	BASSO	BASSO	BASSO
Ragioneria e Contabilità	BASSO	BASSO	BASSO	BASSO
Personale dipendente e collaborazioni	**N.A.**	**N.A.**	**N.A.**	BASSO
Urbanistica, edilizia, ambiente	BASSO	BASSO	BASSO	BASSO
Servizi Sociali	**N.A.**	**N.A.**	**N.A.**	BASSO
Trasporti convenzionati CRI	BASSO	BASSO	BASSO	BASSO
Albo Pretorio	BASSO	BASSO	BASSO	BASSO
Registro Notificazioni	BASSO	BASSO	BASSO	BASSO
Protocollo	BASSO	BASSO	BASSO	BASSO
Utenti servizi scolastici	BASSO	BASSO	BASSO	BASSO
Nuovo Albo Pretorio online	BASSO	BASSO	BASSO	BASSO
Rubrica contatti	BASSO	BASSO	BASSO	BASSO
Archivio Atti e Provvedimenti	BASSO	BASSO	BASSO	BASSO
Gestione raccolta rifiuti differenziata	BASSO	BASSO	BASSO	BASSO
Gestione cimitero comunale	BASSO	BASSO	BASSO	BASSO

ed i seguenti livelli di rischio organizzativo (relativi agli operatori):

Base Dati	Errore Umano	Operazioni illecite sui dati	Accesso non autorizzato da interni	Sottrazione credenziali di autenticazione
anagrafe-informatico	BASSO	BASSO	BASSO	BASSO
anagrafe cartaceo	BASSO	BASSO	BASSO	**N.A.**
Stato Civile Informatico	BASSO	BASSO	BASSO	BASSO
Tributi locali ed erariali,	BASSO	BASSO	BASSO	BASSO

accertamento e riscossione				
Ragioneria e Contabilità	BASSO	BASSO	BASSO	BASSO
Personale dipendente e collaborazioni	BASSO	BASSO	BASSO	**N.A.**
Urbanistica, edilizia, ambiente	BASSO	BASSO	BASSO	BASSO
Servizi Sociali	BASSO	BASSO	BASSO	**N.A.**
Trasporti convenzionati CRI	BASSO	BASSO	BASSO	BASSO
Albo Pretorio	BASSO	BASSO	BASSO	BASSO
Registro Notificazioni	BASSO	BASSO	BASSO	BASSO
Protocollo	BASSO	BASSO	BASSO	BASSO
Utenti servizi scolastici	BASSO	BASSO	BASSO	BASSO
Nuovo Albo Pretorio online	BASSO	BASSO	BASSO	BASSO
Rubrica contatti	BASSO	BASSO	BASSO	BASSO
Archivio Atti e Provvedimenti	BASSO	BASSO	BASSO	BASSO
Gestione raccolta rifiuti differenziata	BASSO	BASSO	BASSO	BASSO
Gestione cimitero comunale	BASSO	BASSO	BASSO	BASSO

E. Misure per la sicurezza dei dati personali

In riferimento a:

- le "Misure Minime" definite dal Decreto Legislativo 196/2003;
- il principio di "Misura Idonea" definito dal Decreto Legislativo 196/2003;
- le basi dati usate dall'Amministrazione contenenti dati personali;
- la natura dei dati personali di cui l'Amministrazione è titolare;
- i risultati dell'Analisi di Rischio,

saranno impartite specifiche istruzioni tali da soddisfare i seguenti criteri ed implementare le seguenti misure di sicurezza a cui chiunque, ognuno per il suo incarico e le sue responsabilità, è tenuto a conformarsi:

E.1 Misure per tutti i dati personali trattati con strumenti elettronici

SISTEMA DI AUTENTICAZIONE:

Legenda colonna di stato:

- I = Implementato
- C = in Corso di implementazione

- N = Non applicabile

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implement

1	L'accesso informatico alle basi dati deve essere protetto al minimo da un sistema di autenticazione basato su codice utente e password (credenziali di autenticazione).	1 a. I sistemi contenenti dati personali o tramite cui si accede a dati personali non devono avere utenze (user-id) anonime, di gruppo o prive di password.	C	28/02/2006
		1 b. Verificare con regolarità l'assenza di utenze (user-id) anonime o prive di password e che questa sia mantenuta nel tempo (si suggerisce un controllo almeno trimestrale).	C	28/02/2006
		1 c. Adottare, quando e dove tecnicamente fattibile, funzioni centralizzate di autenticazione nell'accesso ai dati.	C	28/02/2006
		1 d. I sistemi, quando e dove tecnicamente fattibile, saranno configurati in modo tale da verificare la validità delle richieste di accesso prima di consentire l'accesso stesso.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
2	Una o più credenziali di autenticazione sono assegnate individualmente ad ogni Incaricato. L'incaricato è tenuto a conservarle con cura e mantenerne la segretezza non condividendole con alcuno, neanche in via provvisoria.	2 a. Informare mediante ordine di servizio (o equivalente) l'Amministratore di Sistema del suo dovere di creare solo utenze individuali (non di gruppo, non anonime) sul sistema e di assegnarle individualmente.	N	28/02/2006
		2 b. Quando tecnicamente possibile, configurare i sistemi in maniera tale che quando l'amministratore di sistema (o chi per lui) assegna una password ad un utente, l'utente sia forzato a cambiare la password con un'altra di sua scelta al primo accesso.	C	28/02/2006
		2 c. Quando tecnicamente possibile, verificare regolarmente con strumenti automatizzati che non esistano password banali e disabilitare le utenze protette da	C	28/02/2006

		tale tipo di password.		
		2 d. Quando tecnicamente possibile, configurare i sistemi per non accettare la definizione di password banali da parte degli utenti.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
3	Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.	3 a. Il Responsabile del trattamento e l'Amministratore di Sistema sono autorizzati ad assegnare più utenze informatiche ad una sola persona fisica, se e quando necessario (per esempio, più ruoli con privilegi diversi su una stessa persona fisica).	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
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.	4 a. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di mantenere per se la password (ed il PIN e la chiave fisica, se esistono) con cui accedono al sistema.	C	28/02/2006
		4 b. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di segnalare prontamente l'effettivo o sospetto smarrimento, distruzione o diffusione delle loro credenziali di autenticazione (password, PIN o chiave fisica).	C	28/02/2006
		4 c. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di astenersi dal riportare su notes, foglietti o altro supporto facilmente accessibile le proprie	C	28/02/2006

		password (e PIN se esistono).		

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
5	La componente segreta della credenziale di autenticazione (la password) deve contenere non meno di OTTO caratteri. L'Incaricato è tenuto a cambiare la password almeno ogni sei mesi (tre in caso di dati sensibili e/o giudiziari).	5 a. Configurare i sistemi in modo che non accettino password di lunghezza inferiore agli otto caratteri (o al massimo tecnicamente consentito dal sistema in uso).	C	28/02/2006
		5 b. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di cambiare almeno ogni sei mesi (o tre mesi per i dati sensibili e/o giudiziari) la propria password.	C	28/02/2006
		5 c. Quando tecnicamente possibile, configurare i sistemi in modo che allo scadere dei sei (o tre) mesi forzino l'utente a cambiare la password e non accettino una password che sia uguale o un anagramma delle tre (o sei) precedenti.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
6	La componente pubblica delle credenziali di autenticazione (il codice utente) non deve essere riutilizzato per altri Incaricati o comunque altri utenti del sistema, neanche in tempi diversi o successivi.	6 a. Informare mediante ordine di servizio (o equivalente) l'Amministratore di Sistema di gestire le utenze in modo tale che un utente non più attivo non venga cancellato dal sistema, ma disabilitato. In questo modo il sistema non permetterà una duplicazione di user-id, quand'anche lo user-id sia stato disabilitato.	C	28/02/2006
		6 b. Mantenere un registro con queste informazioni: gli user-id assegnati nel tempo, a quali utenti persone fisiche sono stati	C	28/02/2006

		assegnati, data di attivazione e data di disattivazione. In questo modo, in caso di necessità, si potrà risalire con certezza a quale persona fisica corrisponda o abbia corrisposto un dato user-id.		

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
7	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	7 a. Redigere una procedura, se tecnicamente possibile supportata da strumenti automatici, che con frequenza almeno settimanale identifichi le utenze dormienti (nessun accesso) da oltre 180 giorni e che, se esistenti, le disabiliti (non le cancelli, vedi 6a.).	C	28/02/2006
		7 b. Se il sistema informatico non consente l'automatismo di cui al 7a, la verifica dovrà essere condotta manualmente a cura dell'Amministratore di sistema. In questo caso la frequenza sarà almeno mensile, per non essere troppo onerosa. In questo caso deve identificare le utenze dormienti da più di 150 giorni.	C	28/02/2006
		7 c. La lista delle eventuali utenze dormienti sarà messa a disposizione dell'Ufficio del personale, o funzione equivalente, per verificare la motivazione della inattività e l'opportunità di riattivazione dell'utenza (in caso di errori o giustificate situazioni, per esempio maternità o aspettative).	C	28/02/2006
		7 d. Mantenere una lista approvata dal Titolare o dal Responsabile del Trattamento delle utenze riservate alla manutenzione dei sistemi e redigere una procedura che assicuri che queste siano disabilitate quando non più	C	28/02/2006

		necessarie.		

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
8	Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.	8 a. Redigere una procedura che assicuri che l'Ufficio del personale, o funzione equivalente, informi prontamente l'Amministratore di Sistema di eventuali modifiche di incarico di dipendenti, collaboratori e consulenti.	C	28/02/2006
		8 b. Redigere una procedura che assicuri che su segnalazione dell'Ufficio del Personale (vedi 8a) l'Amministratore di Sistema disabiliti prontamente (non cancelli, vedi 6a) un'utenza associata a persona dimissionaria, che abbia cambiato incarico o comunque non abbia più necessità di accedere a dati personali.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
9	Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	9 a. Informare mediante ordine di servizio, clausola contrattuale o altro strumento applicabile ed equivalente gli incaricati di scollegare il terminale o la stazione di lavoro dalla sessione di sistema quando si allontanano da essi, anche per brevi periodi.	C	28/02/2006
		9 b. Configurare i terminali e le stazioni di lavoro, quando tecnicamente possibile, con un salvaschermo (savescreen) protetto da password, scelta	C	28/02/2006

		dall'utente stesso, che si attivi dopo un minimo di due ed un massimo di cinque minuti di inattività.		

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
10	Occorre garantire al Titolare di poter continuare ad accedere ai dati e ad effettuare i trattamenti anche nel caso che l'unico incaricato in possesso della unica password, chiave di cifratura (o PIN o dispositivo fisico) fosse indisponibile per tempi lunghi e/o indefiniti.	10 a. Verificare se e quali dati siano accessibili solo mediante user-id e password o chiavi crittografiche note ad un solo incaricato (utente persona fisica). Mantenere un registro aggiornato con frequenza almeno mensile di questi tipi di dati e dei relativi incaricati unici.	C	28/02/2006
		10 b. Le password, PIN o chiavi che ricadono nei casi di cui alla misura 10a devono essere depositate dall'incaricato presso uno o più responsabili delegati dal Titolare e/o dai Responsabili del Trattamento di custodirle in busta chiusa in luogo sicuro e di aprire la busta solo in caso di assenza e/o irreperibilità prolungata del relativo incaricato.	C	28/02/2006
		10 c. In caso si debba procedere all'apertura della busta, l'incaricato a cui si riferisce deve essere avvisato non appena sia possibile e si deve tenere registrazione dell'ora e data dell'avvenuta apertura.	C	28/02/2006
		10 d. Per il principio di separazione dei ruoli, Legale Rappresentante del Titolare, Responsabili dei Trattamenti, Amministratori di Sistema e altro personale con funzioni tecniche sui sistemi NON possono essere incaricati della custodia della password.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
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.	11 a. Eventuali dati personali destinati alla diffusione possono essere esclusi dalle misure di sicurezza relative al sistema di autenticazione fin qui descritto e dalle misure relative al sistema di autorizzazione (prossima sezione).	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
12	Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.	12 a. Verificare regolarmente, almeno su base annuale in sede di revisione di questo Documento Programmatico sulla Sicurezza, se esistono più utenze relative a più incaricati con diversi gradi di privilegio sul sistema (e sui dati e trattamenti con esso effettuati).	C	28/02/2006
		12 b. Se non esistono diversi gradi di privilegio sul sistema, ovvero se un unico incaricato (o pochi incaricati) dei trattamenti sono autorizzati ad eseguire tutti i trattamenti e ad accedere a tutti i dati, i prossimi punti 13 e 14 sono superflui finquando sussista tale condizione.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di

				Implementazione
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.	13 a. Redigere una procedura che identifichi e mantenga un registro dei ruoli (e dei privilegi di sistema ad essi associati) prima di iniziare i trattamenti e prima di dare accesso ai dati personali.	C	28/02/2006
		13 b. Per ogni incaricato o tipologia di incaricato, i profili di autorizzazione sui sistemi saranno quelli necessari e sufficienti a svolgere i trattamenti delegati a tale incaricato. Ciò sarà fatto preferibilmente in via nominativa o al minimo per classi di incaricato, classi che normalmente coincideranno con l'ufficio di appartenenza e/o i ruoli.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
14	Periodicamente e comunque almeno annualmente è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	14 a. Verificare regolarmente, almeno su base annuale in sede di revisione di questo Documento Programmatico sulla Sicurezza, che i requisiti di autorizzazione degli utenti siano ancora validi e comunicare tempestivamente eventuali variazioni all'Amministratore di Sistema per le azioni sistemistiche del caso.	C	28/02/2006
		14 b. Aggiornare, a cura dell'Amministratore di Sistema, i profili di autorizzazione sui sistemi in caso di variazioni di cui al precedente 14.a .	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione

15	Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale 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.	15 a. Redigere una procedura che identifichi e mantenga un registro dei manutentori e gestori del sistema informatico e dei privilegi ad essi associati.	C	28/02/2006
		15 b. Verificare regolarmente, almeno su base annuale in sede di revisione di questo Documento Programmatico sulla Sicurezza, che i requisiti di autorizzazione dei manutentori e gestori del sistema informatico siano ancora validi e comunicare tempestivamente eventuali variazioni all'Amministratore di Sistema per le azioni sistemistiche del caso.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
16	I dati personali sono protetti contro il rischio di intrusione e dall'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.	16 a. Mantenere un registro aggiornato degli strumenti informatici soggetti a codice maligno (virus, worm. trojan ed altri).	C	28/02/2006
		16 b. Installare programmi antivirus su tutti gli strumenti, individuati come soggetti a codice maligno (vedi 16a.).	C	28/02/2006
		16 c. Verificare l'aggiornamento dei software antivirus su base almeno semestrale.	C	28/02/2006
		16 d. Installare programmi su tutti gli strumenti secondo il principio di necessità, ovvero installare solo quei programmi ed attivare le funzionalità necessarie e sufficienti alle esigenze di servizio, da supporti ufficiali dei produttori ed in conformità agli accordi di licenza sottoscritti col produttore.	C	28/02/2006
		16 e. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di: 1)	C	28/02/2006

		astenersi dallo installare programmi non autorizzati dall'Amministratore di Sistema sulle proprie stazioni di lavoro, con particolare riferimento a quelli scaricabili da internet, a quelli allegati a riviste specializzate e provenienti da supporti non ufficiali, 2) di usare precauzione nell'aprire allegati di posta elettronica, specie se non sollecitati o provenienti da corrispondenti non noti.		
		16 f. Quando tecnicamente possibile, configurare i programmi antivirus i modo tale che si aggiornino automaticamente via internet.	C	28/02/2006
		16 g. Quando tecnicamente possibile, privilegiare l'esecuzione di test di nuovi software su sistemi separati da quelli di produzione e soprattutto da quelli contenenti dati personali o che possono accedere a dati personali.	C	28/02/2006
		16 h. Quando tecnicamente possibile, installare programmi anti-spam ed anti-relay (se non già integrati nel software antivirus adottato) e configurarli in modo che si aggiornino automaticamente via internet	C	28/02/2006
		16 i. Provvedere con sufficiente margine al rinnovo degli abbonamenti di manutenzione del software antivirus, in modo da assicurare la continuità del relativo servizio di aggiornamento.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
17	Gli aggiornamenti periodici dei programmi per elaboratore volti a	17 a. Effettuare semestralmente una verifica sullo stato di aggiornamento del software	C	28/02/2006

	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.	applicativo, verificare la compatibilità degli aggiornamenti resi disponibili dal produttore con l'ambiente informatico e, se del caso, effettuare gli aggiornamenti solo dopo aver effettuato una copia di sicurezza dei dati e dell'ambiente corrente in modo di assicurarsi, se necessaria, la possibilità di recuperare dati e programmi allo stato precedente.		
		17 b. La verifica di cui al 17a. sarà almeno semestrale sui sistemi che trattino dati sensibili o giudiziari.	C	28/02/2006

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione
18	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	18 a. Effettuare le copie di sicurezza (backup) dei dati con frequenza almeno settimanale ed al minimo verificare la leggibilità dei supporti e l'integrità dei dati in essi contenuti dopo ogni backup. Privilegiare un backup giornaliero dei dati, quando possibile.	I	
		18 b. Conservare i supporti di backup al minimo in locale diverso da quello in cui si trovano i sistemi e in armadi metallici chiusi a chiave.	C	28/02/2006
		18 c. Quando possibile, privilegiare la conservazione dei supporti in sede diversa da quella in cui si trovano i sistemi.	N	28/02/2006

Nota: Il prossimo criterio di cui al punto 20 del Discliplinare Tecnico (Allegato B al d.lgs.196/2003) è, alla lettera, riferito ai dati sensibili o giudiziari. Per il principio della adozione di "misure idonee" di cui allo stesso d.lgs.196/2003, questo punto viene applicato a tutti i dati personali.

All.B	Criterio	Misura Di Sicurezza	Stato	Data di Implementazione

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.	20 a. E' definito il principio organizzativo tale per cui nessuna connessione della rete locale interna verso reti esterne (in particolare internet) deve essere lasciata priva di appositi sistemi di filtro noti come firewall.	C	28/02/2006
		20 b. Informare mediante ordine di servizio (o equivalente) gli incaricati del loro dovere di segnalare prontamente incidenti di sicurezza, anche solo presunti tali, al Titolare o al Responsabile dei Trattamenti.	C	28/02/2006
		20 c. Quando fattibile, le stazioni di lavoro degli incaricati sono protette in locali chiusi a chiave fuori dall'orario di lavoro.	C	28/02/2006
		20 d. Quando fattibile, i sistemi server e le apparecchiature di rete (switch, router, ed altre) sono collocati in locali tecnologici ad accesso controllato ed è tenuto un aggiornato registro del personale autorizzato e degli accessi a tale locale.	C	28/02/2006
		20 e. Ogni firewall deve essere configurato in modo idoneo in relazione alla tipologia del traffico desiderato ed indesiderato a cura dell'Amministratore di Sistema secondo il principio di necessità, ovvero di consentire solo il traffico strettamente necessario e sufficiente alle esigenze di servizio (le finalità) degli incaricati.	C	28/02/2006
		20 f. La configurazione del firewall ed il suo stato di aggiornamento sono riverificati su base almeno trimestrale.	C	28/02/2006

E.2 Misure per i dati personali trattati senza strumenti elettronici

Le seguenti basi dati sono trattate senza l'ausilio di strumenti elettronici:

Base Dati	*Ufficio Interno di Riferimento*	*Struttura Esterna Incaricata*	*Dati Sens*	*Natura della Base Dati*	*Luogo di custodia*
anagrafe cartaceo	Anagrafe	-	SI	Cartaceo	Sede Municipale
Personale dipendente e collaborazioni	Segreteria	-	SI	Cartaceo	Sede Municipale
Servizi Sociali	Ragioneria	-	SI	Cartaceo	Sede Municipale

Per queste basi dati, agli incaricati saranno impartite specifiche istruzioni scritte, mediante ordine di servizio o strumento equivalente, che soddisfino i seguenti criteri:

1. garanzia di controllo e custodia, per l'intero ciclo delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali sensibili;
2. verifica e aggiornamento periodico, almeno annuale, della lista degli incaricati e dei trattamenti consentiti ai singoli incaricati;
3. controllo e custodia a cura degli incaricati degli atti e dei documenti contenenti dati personali sensibili affidati agli incaricati per lo svolgimento delle loro mansioni e pronta restituzione al termine delle operazioni affidate;
4. accesso controllato e registrato agli archivi contenenti dati sensibili, con identificazione delle persone ammesse, a qualunque titolo, fuori dell'orario comune di lavoro. Se i locali contenenti l'archivio non sono dotati di sistemi elettronici di accesso o di personale di vigilanza, le persone vi accedono solo dietro preventiva autorizzazione del rispettivo Responsabile del Trattamento dei Dati.

E.3 Ulteriori Misure per i dati sensibili trattati con strumenti elettronici

Le seguenti basi dati elettroniche contengono dati sensibili:

Base Dati	*Luogo di Custodia*	*Struttura di Riferimento*
anagrafe cartaceo	Sede Municipale	Anagrafe
Stato Civile Informatico	Sede Municipale	Stato Civile
Tributi locali ed erariali, accertamento e riscoss	Sede Municipale	ufficio unico amministrativo
Personale dipendente e collaborazioni	Sede Municipale	Segreteria
Trasporti convenzionati CRI	Sede Municipale	Amministrativo
Protocollo	Sede Municipale	Amministrativo

Per queste basi dati, oltre le misure già individuate si identificano le seguenti ulteriori misure:

1. Tutti i supporti rimovibili, anche quelli non destinati alle copie di sicurezza, (floppy, dischetti, nastri, dischi ottici, etc.) su cui sono memorizzati i dati sono fisicamente protetti, quando non utilizzati, in armadi metallici chiusi a chiave.

2. Se i supporti sono destinati al trasporto, alla spedizione o al backup fuori sede, devono essere adeguatamente protetti da perdita, distruzione e accesso non autorizzato.
3. I supporti che hanno contenuto dati sensibili possono essere successivamente destinati ad altro uso, purché il supporto sia completamente sovrascritto con dati casuali (al minimo mediante formattazione del disco) in modo da garantire la non ricostruibilità dei dati sensibili precedentemente contenuti. Se ciò non fosse possibile, il supporto è da considerarsi giunto a fine della sua vita utile e deve essere fisicamente distrutto (v. punto successivo).
4. I supporti giunti alla fine della loro vita utile vanno fisicamente distrutti prima di essere gettati. Tali supporti saranno distrutti con criteri tali da assicurare la non leggibilità dei dati sensibili precedentemente contenuti.
5. Il ripristino dei dati sensibili a seguito di loro distruzione totale o parziale di cui al successivo paragrafo "Criteri e modalità di ripristino dei dati", deve poter avvenire in tempi compatibili con le esigenze del servizio fornito e degli interessati.

F. Criteri e modalità di ripristino dei dati

A seguito di perdita parziale o totale, dovuta a qualunque motivo accidentale o doloso, dei dati personali occorre garantirne il ripristino, in tempi certi e compatibili con i diritti degli interessati e nel caso dei dati sensibili, in tempo non superiore a sette giorni.

Situazione attuale degli strumenti di salvataggio e ripristino delle basi dati:

Base Dati	Dati Sens.	Supporto	Frequenza (in giorni)	Luogo Conserv. Copie	Ufficio o Fornitore Incaricato
anagrafe-informatico	NO	Nastro	1	Sede Municipale	Anagrafe
Stato Civile Informatico	SI	Nastro	1	Sede Municipale	Stato Civile
Tributi locali ed erariali, accertamento e riscoss	SI	Remoto (via rete)	15	Sede Municipale	Biginelli Giampiero
Ragioneria e Contabilità	SI	Nastro	1	Sede Municipale	Backup automatico su server
Urbanistica, edilizia, ambiente	SI	CD/DVD-ROM	200	Sede Municipale	Barbato Pasquale
Trasporti convenzionati CRI	SI	Remoto (via rete)	1	Sede Municipale	Amministrativo
Albo Pretorio	NO	Nastro	1	Sede Municipale	automatico su server
Registro Notificazioni	NO	Nastro	1	Sede Municipale	automatico su server
Protocollo	SI	Nastro	1	Sede Municipale	automatico su server
Utenti servizi scolastici	NO	Remoto (via rete)	2	Sede Municipale	amministrativo

Nuovo Albo Pretorio online	NO	Remoto (via rete)	1	Sede Municipale	AMMINISTRATIVO
Rubrica contatti	NO	Remoto (via rete)	2	Sede Municipale	amministrativo
Archivio Atti e Provvedimenti	NO	Remoto (via rete)	2	Sede Municipale	amministrativo
Gestione raccolta rifiuti differenziata	NO	Remoto (via rete)	2	Sede Municipale	amministrativo
Gestione cimitero comunale	NO	Remoto (via rete)	2	Sede Municipale	amministrativo

Per tutte le basi dati sono implementate le misure organizzative e tecniche idonee a garantire il ripristino in tempi certi e ragionevoli dei dati a seguito di loro perdita, totale o parziale, sulla base dei seguenti criteri:

1. La conservazione delle copie di sicurezza avviene, in modo protetto, in locale diverso da quello di fruizione dei dati al fine di ridurre le probabilità di distruzione o il danneggiamento dei dati originali e delle copie di sicurezza

2. Sono sottoscritti con i fornitori contratti di manutenzione hardware e software che garantiscono l'intervento in giornata e che prevedono prove periodiche di ripristino dei dati salvati

G. Interventi Formativi

Gli Incaricati riceveranno adeguata formazione:

- sui rischi che incombono sui dati,
- sulle misure rese disponibili per mitigare tali rischi
- sulle misure minime di sicurezza da adottare.

Tale formazione sarà erogata in occasione dell'ingresso in servizio, di cambiamento di mansione o di introduzione di modifiche significative a questo Documento Programmatico sulla Sicurezza o agli strumenti informatici o alle procedure di trattamento dei dati personali.

H. Criteri per l'affidamento del trattamento all'esterno.

L'affido del trattamento di dati personali e/o della relativa infrastruttura tecnologica all'esterno della struttura dell'Amministrazione deve avvenire in maniera tale da garantire che il Fornitore rispetti i criteri e le misure minime di sicurezza definite in questo Documento Programmatico sulla Sicurezza.

A tale fine, i contratti di fornitura dovranno contenere:

1. Se l'Azienda fornitrice è italiana o comunque soggetta alla legislazione Italiana, specifica dichiarazione del Fornitore di fornire i propri servizi in conformità al Decreto legislativo 196/2003 e di adottare al minimo i criteri e le misure minime di sicurezza ivi identificate. Tale dichiarazione sarà parte integrante del contratto.
2. Se l'Azienda fornitrice non è italiana, dichiarazione che il trattamento avverrà all'interno dell'Unione Europea, rispondendo alle linee guida Comunitarie in materia di Privacy ed in conformità alla Legge Nazionale in cui l'Azienda opera. Tale dichiarazione sarà parte integrante del contratto.

Inoltre il Titolare si deve riservare la possibilità contrattuale di riscontrare direttamente quanto dichiarato dall'Azienda fornitrice con riferimento alla conformità al D.Lgs. 196/2003.

Il Legale Rappresentante e quanti nell'ambito dell'Amministrazione siano delegati ad impegnarsi in contratti con terze parti, sono tenuti a verificare che i nuovi contratti di fornitura di servizi, che implichino il trattamento di dati personali di cui l'Amministrazione è Titolare del Trattamento, soddisfino questi requisiti. I contratti attualmente in essere, alla loro scadenza naturale saranno rinnovati solo previa integrazione.
Se vengono adottate misure minime di sicurezza avvalendosi di soggetti esterni alla struttura dell'Amministrazione, il Titolare si fa rilasciare una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Disciplinare Tecnico (allegato B) del d.lgs. 196/03.

Sulla presente proposta di deliberazione, ai sensi dell'articolo 49 del D. Lgs. 18 agosto 2000 n. 267, si esprime parere favorevole sulla regolarità tecnico-amministrativa.

IL RESPONSABILE DEL SERVIZIO

Ai sensi dell'art. 49 del D. Lgs. 18 agosto 2000 n. 267, si attesta la copertura finanziaria dell'impegno di spesa assunto con la presente deliberazione.

IL RESPONSABILE DEL SERVIZIO

Sulla presente proposta di deliberazione, ai sensi dell'articolo 49 del D. Lgs. 18 agosto 2000 n. 267, si esprime parere favorevole sulla regolarità tecnica.

IL RESPONSABILE DEL SERVIZIO

Letto, confermato e sottoscritto.

IL SINDACO	**IL SEGRETARIO**
Mauro Cabiati	**Dott. Pierangelo Scagliotti**

RELAZIONE DI PUBBLICAZIONE

La presente deliberazione viene pubblicata all'albo pretorio del Comune di Villanova M.to il per quindici giorni consecutivi

IL SEGRETARIO

COMUNICAZIONE AI CAPIGRUPPO

Si da atto che del presente verbale viene data comunicazioni oggi…….....giorno della pubblicazione ai Capo gruppo consiliari ai sensi dell'art. 125 del D. Lgs. 18 agosto 2000 n. 267.

IL SEGRETARIO COMUNALE

ESTREMI DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva il.....ai sensi dell'art. 134 del D. Lgs. 18 agosto 2000 n. 267.

IL SEGRETARIO

Copia conforme all'originale ad uso amministrativo.

Villanova M.to, lì **IL SEGRETARIO COMUNALE**