COMUNITA' MONTANA SALTO - CICOLANO
ZONA VII

Fiumata di Petrella Salto **Provincia di Rieti**

DELIBERAZIONE DELLA GIUNTA

OGGETTO: APPROVAZIONE AGGIORNAMENTO DOCUMENTO PROGRAMMATICO SICUREZZA DATI ANNUALITA' 2012-

N. 14

DEL 22/03/2012

L'anno **DUEMILADODICI addì VENTIDUE** del mese di MARZO alle ore **15.00** e seg.ti, in Fiumata di Petrella Salto e nella consueta sala delle adunanze, convocata nelle forme consuete, la giunta esecutiva della Comunità Montana si è ivi riunita.

			Fatto l'appello nominale risultano	
			PRESENTE	ASSENTE
1. **RINALDI**	Carmine	Presidente	X	θ
2. **MOZZETTI**	Sergio	Assessore	X	θ

Assiste all'adunanza il Segretario D.ssa Silvia Ridolfi .

Il PRESIDENTE, ING. **Carmine Rinaldi,** visto che il numero degli intervenuti è legale per deliberare, assume la presidenza e dichiara aperta la seduta.

OGGETTO: MODIFICA DOCUMENTO PROGRAMMATICO SULLA SICU2REZZA DEI DATI – D. L.VO 196/2003 – RIF. DG. N° 19 DEL 19/04/2011 -

LA GIUNTA

Della Comunità Montana ***"Salto Cicolano" zona VII del Lazio,***

RICHIAMATA la precedente delibera di giunta n° 19 del 19.04.2011, con la quale ai sensi del D. Lgs 30/06/2003 n° 196 " Codice in materia di protezione dei dati personali" è stato approvato il documento Programmatico sulla sicurezza dei Dati;

VISTA la regola tecnica n° 19 dell'allegato B al D. Lgs 196/2003 e la direttiva della Funzione Pubblica dell'11 febbraio 2005, che prevede che entro il 31 marzo di ogni anno le pubbliche amministrazioni, ivi compresi gli Enti Locali, devono provvedere ad aggiornare il DPSS;

RITENUTO quindi di procedere all'integrazione del DPSS aggiornando le relative schede allegate al presente provvedimento;

PRESO ATTO del parere favorevole espresso dal Responsabile del Servizio interessato, ai sensi e per gli effetti di quanto stabilito dall'art. 49, comma 1 del T.U. approvato con D. lgs. 267/2000, in merito alla regolarità Tecnica dell'atto;

RILEVATO che il presente atto non comporta impegno di spesa a carico del bilancio comunitario e quindi non necessita il parere di regolarità contabile;

SENTITO il Segretario della Comunità Montana,

DELIBERA

1. *Di modificare le schede allegate relative al Documento programmatico sulla Sicurezza dei Dati ai sensi e per gli effetti dell'art. 34 comma 1, lettera g) del D.L.vo 196/2003 (rif. D.G. n° 25/ del 14/03/2006)*

Premessa

Il Codice sulla privacy (D.lgs.vo 196/03) impone a chiunque tratta informazioni relative ad altre persone, imprese, enti od associazioni, di rispettare alcuni principi fondamentali a garanzia della riservatezza dei dati stessi.

Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattare dati; questi obblighi sono sanzionati anche penalmente: è necessario, pertanto, procedere all'adeguamento dell'organizzazione al fine di rispettare gli obblighi imposti dal Codice.

La finalità del "documento programmatico della sicurezza" è quella di definire i criteri e le procedure per garantire la sicurezza nel trattamento di dati personali.

Si rende noto che la rilevazione dello stato di fatto è stata congelata alla data del **25.02.2006**. Eventuali cambiamenti che si dovessero rendere necessari saranno introdotti in questo DPSS indicando in copertina, le revisioni effettuate entro il 31 marzo, data entro la quale le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno) di un Documento Programmatico sulla Sicurezza dei dati.

Fonti normative

Le disposizioni di legge principali concernenti la corretta gestione di sistemi informatici sono:

R.D. 22.4.1941 n. 633 e D.Lgs. 29.12.1992 n. 518 (tutela del diritto di autore sul software);

L. 23.12.1993 n. 547 (reati legati all'informatica - modifiche al Codice penale);

D.lgs.vo 30.6.2003 n.196 (recante il Codice in materia di protezione dei dati personali) e suo Disciplinare Tecnico.

Scopo di questo documento

E' delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali affinché siano rispettati gli obblighi previsti dalle Leggi vigenti.

Validità del documento

Il presente documento **è valido un anno**, si potranno aggiornare alcune informazioni qualora le stesse per motivi diversi non risultassero più coerenti con l'organizzazione o con il trattamento dei dati.

Inoltre le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno) di un Documento Programmatico sulla Sicurezza dei dati.

Il presente DPSS è stato redatto per :

Comunità Montana "Salto Cicolano"
Via del Lago, n. 12
02025 FIUMATA – Comune di Petrella Salto (RI)

Titolare al trattamento dei dati a cui spetta la vigilanza sul rispetto da parte dei Responsabili e degli Incaricati delle proprie istruzioni nonché sulla puntuale osservanza delle disposizioni vigenti in materia di trattamento dei dati e loro sicurezza è la Comunità Montana **"Salto Cicolano"** rappresentata dal Presidente – ***Ing. Carmine Rinaldi*** (art. 28 D.Lgs 196 del 30 giugno 2003).

Definizioni:

Responsabile del trattamento al trattamento dei dati: Spetta il compito di promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente **D**ocumento **P**rogrammatico **S**ulla **S**icurezza dei Dati Personali di seguito denominato **DPSS**; informare il titolare del trattamento sulle eventuali non corrispondenze con le norme di sicurezza e sugli eventuali incidenti; promuovere lo svolgimento di un continuo programma di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza; promuovere e garantire l'esecuzione del programma di audit.

Responsabile del trattamento del sistema informativo : Spetta il compito di promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento programmatico sulla sicurezza dei Dati Personali di seguito denominato DPS; informare il titolare del trattamento sulle eventuali non corrispondenze con le norme di sicurezza e sugli eventuali incidenti; promuovere lo svolgimento di un continuo programma di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza; promuovere e garantire l'esecuzione del programma di audit. Garantire il funzionamento di tutti i dispositivi elettronici, degli strumenti, dei sistemi operativi, dei software, con particolare riferimento ai sistemi Antivirus, Firewall, al sistema di back-up, al sistema per il ripristino dei dati, alle reti, al controllo degli accessi.

Incaricati al trattamento: Nominati dal Responsabile del trattamento per iscritto devono svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente DPS e secondo le direttive del Responsabile del trattamento al trattamento dei dati; rispettare e far rispettare le norme di sicurezza e le misure per la protezione dei dati personali; segnalare al Responsabile del trattamento eventuali anomalie o comportamenti pregiudizievoli sul trattamento dei dati; informare il Responsabile del trattamento in caso di incidente di sicurezza che coinvolga i dati personali;

Incaricato al trattamento della custodia delle password: Nominato dal Responsabile del trattamento per iscritto svolge le attività previste dal Responsabile del trattamento alla gestione del sistema informatico; in particolare deve custodire in luogo sicuro ed a chiave le buste contenenti le password che gli perverranno dal/i Responsabile del trattamento/i al trattamento dei dati, dal Responsabile del trattamento al Sistema Informatico e dagli incaricati al trattamento dei dati. In caso di necessità il Responsabile del trattamento al trattamento dei dati o il Responsabile del trattamento al sistema informatico potrà richiedere la busta contenente una password, in tal caso il mittente della busta dovrà essere immediatamente avvertito affinché la possa sostituire consegnando all'incaricato alla custodia delle password la nuova busta contenente la nuova password. E' compito dell'incaricato verificare che vi siano le buste di tutti i responsabili e di tutti gli incaricati al trattamento dei dati comunicati dal/dai Responsabile del trattamento/i. L'incaricato alla custodia delle password deve rispettare e far rispettare le norme di sicurezza e le misure per la protezione dei dati personali; segnalare al Responsabile del trattamento eventuali anomalie o comportamenti pregiudizievoli sul trattamento dei dati; informare il Responsabile del trattamento in caso di incidente di sicurezza che coinvolga i dati personali;

Strumenti: Gli elaboratori, i programmi per elaboratori, qualunque dispositivo elettronico automatizzato o qualsiasi contenitore o mezzo impiegato per effettuare il trattamento dei dati

Rischi: Situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: lieve, medio, grave e gravissimo.

Misure: Il complesso delle misure cautelari tecniche, informatiche organizzative, logistiche e procedurali di sicurezza atti ad eliminare i rischi valutati e stimati nella progettazione della sicurezza in relazione alla soglia di gravità

Profilo di autenticazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione (l'insieme degli strumenti elettronici, dei software e delle procedure atte a verificare l'identità) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

1. Le credenziali di autenticazione (i dati ed i dispositivi , in possesso di una persona da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica) 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.

2. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

3. 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. E' un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per la protezione dei dati. Un corretto utilizzo ed impiego delle password è a garanzia dell'utente. Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation (server, postazioni PC client, portatili, ecc.) tramite le quali si po' accedere alla rete o alle banche dati contenenti i dati personali. 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. Non deve essere comunicata ad alcuno per alcun motivo, non deve essere conservata annotazione scritta in alcun posto specie nei pressi della postazione di lavoro.

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

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

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

8. Sono impartite le seguenti istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. L'incaricato se si allontana dalla propria postazione dovrà mettere in protezione il suo sistema (PC client o portatile) affinché persone non autorizzate non abbiano accesso ai dati protetti. La responsabilità sull'efficacia di tale sistema è assegnata al Responsabile del trattamento dei servizi informativi.

9. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite le seguenti 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.

a. Per ogni PC si è stabilito a seconda del suo Sistema operativo la seguente procedura

b. Il Responsabile del trattamento del sistema informativo affida l'incarico al trattamento della custodia delle password ad un addetto. La responsabilità sull'efficacia di tale sistema è assegnata al Responsabile del trattamento del sistema informativo.

c. 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.

d. Ogni utente dovrà obbligatoriamente consegnare in busta chiusa la propria password alla persona incaricata alla custodia delle chiavi di accesso che gli sarà indicata dal Responsabile del trattamento al

sistema informatico. In caso di necessità il Responsabile del trattamento al sistema informativo chiederà la busta contenente la password al custode per disporre della password di accesso al sistema. Al termine dei lavori comunicherà all'addetto della necessità di modificare la password. Per questo motivo ogni qualvolta per qualsiasi motivo un addetto modifica la sua password è OBBLIGATO ALLA CONSEGNA IMMEDIATA DELLA BUSTA SIGILLATA CONTENENTE LA NUOVA PASSWORD AL CUSTODE. La violazione di tale norma è grave e porta ad estreme conseguenze in quanto mette a repentaglio l'accesso ai dati da parte dell'organizzazione in caso di necessità. In tal caso i dati dovranno risiedere su di un server il cui accesso sarà limitato e vincolato al profilo della persona.

e. Se il sistema operativo non consente una gestione degli utenti differita tra amministratore del PC ed utilizzatore si utilizzeranno profili differenti affinché sia sempre possibile l'accesso al PC in caso di necessità, di tale possibilità andrà avvisato l'utilizzatore.

f. 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.

Sistema di autorizzazione

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

11. 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.

12. La normativa prevede che periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale.

Altre misure di sicurezza

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.

La normativa prevede che i dati personali debbano essere 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; grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale.

Allo scopo un gateway deve essere protetto. E' definito Gateway l'insieme di hardware, software e applicazioni che permettono l'interconnessione (Internet) o l'accesso remoto a sistemi esterni. I Gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati attraverso sistemi di controllo specifici (Proxy/Firewall). Pertanto per tutte le cpu che sono collegate verso internet è necessario predisporre un sistema che impedisca accessi indesiderati. Tali sistemi anche se l'accesso è limitato nel tempo servono a prevenire l'accesso da parte di "intrusi" ai vostri sistemi di gestione dati. Tali sistemi sono denominati "Firewall". Di tutti i vostri sistemi attraverso il server dati (se è quest'ultimo a consentire la connessione all'esterno) o direttamente per ogni singola cpu se ciascuno si connette ad internet con un modem deve disporne. Ogni trimestre è necessario verificare se sono disponibili degli aggiornamenti sul Firewall. Le sottoscrizioni di un servizio di notifica sugli aggiornamenti del prodotto sono consigliate. La responsabilità sull'efficacia di tale sistema è assegnata al Responsabile del trattamento dei servizi informativi. Le istruzioni riguardanti l'utilizzo del sistema FIREWALL e del relativo aggiornamento sono riportate nelle guide operative del prodotto.

La normativa prevede che gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti debbano essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari la normativa prevede che tale aggiornamento debba avvenire almeno a livello semestrale. I sistemi sensibili ai virus informatici (sistemi operativi, programmi informatici, data base) devono essere protetti con opportuni programmi antivirus che devono essere aggiornati per garantire la loro efficacia.

Trimestralmente dovrà essere verificato se il numero interno riportato da tutti i programmi antivirus è stato aggiornato al fine di verificare se il sistema di aggiornamento è funzionante; grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale. Resta facoltà degli interessati procedere con un controllo più frequente. In caso di mancato aggiornamento del software antivirus si dovrà provvedere a ripristinarne immediatamente il funzionamento. Le cpu che ricevono le mail direttamente dall'esterno dovranno disporre di un Antivirus in grado di controllare le mail in arrivo e quelle in partenza, inoltre su tutte le cpu che contengono banche dati o su quelle che hanno accesso ad Internet dovrà essere condotto un controllo settimanale con evidenza oggettiva. In caso di segnali allarmanti (mail sospette, comportamenti della cpu imprevedibili) è necessario verificare immediatamente l'efficienza dell'antivirus ed il suo stato di aggiornamento. La responsabilità sull'efficacia di tale sistema è assegnata al Responsabile del trattamento dei servizi informativi. Le istruzioni riguardanti l'utilizzo del sistema antivirus e del relativo aggiornamento sono riportate nelle guide operative del prodotto.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

2. Distribuzione dei compiti e delle Responsabilità (regola 19.2 disciplinare tecnico allegato b)

2.1 Elenco dei responsabili al trattamento dei dati e relativi incaricati

Il Titolare al trattamento dei dati è **La Comunità Montana "Salto Cicolano"** rappresentato dal Presidente Ing. Carmine Rinaldi

Il Titolore ha individuato e quindi conferito, **L'INCARICO di RESPONSABILE DEL TRATTAMENTO AL TRATTAMENTO DEI DATI** al Segretario della Comunità Montana:

Nominativo	Data Assunzione Incarico	Data Scadenza Incarico	Data Formazione
D.ssa SILVIA RIDOLFI	14/03/2006	31/03/2013	28/02/2007

Il Titolore ha individuato e quindi conferito, **GLI INCARICHI di RESPONSABILI DI AREA** ai seguenti Responsabii di Posizione Organizzativa della Comunità Montana:

Nominativo	Area	Data Assunzione Incarico	Data Scadenza Incarico	Data Formazione
D.ssa Silvia Ridolfi	Area 1	14.03.2006	31/03/2013	28/02/2007
Rag. Mirella De Angelis	Area 2	14.03.2006	31/03/2013	28/02/2007
Arch. Amedeo Riccini	Area 3	14.03.2006	31/03/2013	28/02/2007

LEGENDA: (Area 1 = *Amministrativa* , Area 2 = *Finanziaria*, Area 3 =*Tecnica*)

Il Responsabile del trattamento dei dati conferisce con lettera allegata in copia al presente documento **l'INCARICO al TRATTAMENTO DEI DATI** alle seguenti persone appartenenti al personale della Comunità Montana :

Cognome e Nome	Data Assunzione Incarico	Data Scadenza Incarico	Data Formazione	Modalità di Accesso				
				I	M	C	L	S
Napoleone Anna Maria	14.03.2006	31/03/2013	28/02/2007	X	X	X	X	X
Pasqualone Rita	14.03.2006	31/03/2013	28/02/2007	X	X	X	X	X
Palluzzi Lido	14.03.2006	31/03/2013	28/02/2007	X	X	X	X	X
Vupiani Claudio	14.03.2006	31/03/2013	28/02/2007	X	X	X	X	X

LEGENDA: (I=Inserimento, M=Modifica, C=Cancellazione, L=Solo Lettura, S=Scrittura)

Inoltre predispone per ogni impiegato della Comunità Montana "Salto Cicolano" specifica lettera di incarico per i trattamenti di loro competenza contenente le seguenti informazioni:

- categorie dei dati cui può avere accesso;
- tipologia di trattamento e vincoli specifici applicabili alle varie tipologie di dati;
- istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

2.2 *Elenco dei responsabili di altre attività*

Il Titolare al trattamento dei dati della Comunità Montana "Salto Cicolano" rappresentato dal Presidente **Ing. Carmine Rinaldi** ha individuato e quindi conferito, con lettera allegata in copia al presente documento, **L'INCARICO** di **Responsabile del trattamento dei Sistemi informativi** a:

Nominativo	Sede	Data Assunzione	Data Scadenza Incarico	Data Formazione
Dott.ssa Silvia Ridolfi	**In organico**	**14.03.2006**	**31/03/2013**	**28/02/2007**
Arch. Amedo Riccini	**In organico**	**14.03.2006**	**31/03/2013**	**28/02/2007**

Con i seguenti compiti :

- Deve custodire i software originali e relative licenze
- Deve provvedere agli aggiornamenti che si rendessero necessari dei software di sistema e degli applicativi
- Installare eventuali nuovi programmi, dopo aver scansionato con l'apposito programma antivirus, stampata la relativa relazione, i supporti di installazione.back up dei dati settimanale;
- Custodire delle copie di back up;
- Coordinamento degli incaricati per la corretta manutenzione ordinaria dei PC, dell'adozione delle norme di comportamento,regole operative e rispetto del regolamento interno(vedi allegati)
- Regolamento interno per gli incaricati
- Manutenzione ordinaria incaricati
- Rapporti con il soggetto manutentore esterno del sistema informativo

MANUTENZIONE ORDINARIA DEL RESPONASBILE INFORMATICO

Il Responsabile del trattamento del sistema informativo (RSI) è tenuto a fare ogni sabato:

- COPIA DI BACK-UP su dischi rimovibili, dei dati presenti sul server (o sui singoli PC se non è presente una rete interna LAN), conservando le copie in cassaforte;
- DEFRAMMENTAZIONE del disco fisso del server dell'amministrazione;
- SCAN DISK del disco fisso e PULITURA
- AGGIORNAMENTO e SCANSIONE del software ANTIVIRUS;
- annotare ogni operazione svolta su un apposito registro.

Analisi delle misure riguardanti la sicurezza fisica dei luoghi dove vengono effettuati i trattamenti tramiti strumenti elettronici

Misura	**Chiave**
Descrizione	Protezione dei locali contenente gli strumenti (PC e Server)atti al trattamento dei dati
Rischio Contrastato	Uso non Autorizzato Hardware, Sabotaggio, Furto
Trattamenti	Tutti
Banche Dati	Tutte
Effettività	In Essere
Data Scheda	1.03.2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.03.2013
Periodicità del controllo	Annuale
Tipologia della misura	Misura preventiva

Sicurezza Fisica

Misura	Password Bios
Descrizione	Aggiornamento periodico della password per evitare l'accesso
Rischio Contrastato	Uso non Autorizzato Hardware
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01.03.2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Misura preventiva

Misura	Password di rete
Descrizione	Aggiornamento periodico delle password di rete
Rischio Contrastato	Manomissione- Sabotaggio - Accesso non Autorizzato - Cancellazione dati non autorizzata
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01.03.2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Misura Preventiva

Misura	Manutenzione
Descrizione	Manutenzione Periodica
Rischio Contrastato	Guasto
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01.03.2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.03.2013
Periodicità del controllo	Annuale
Tipologia della misura	Misura preventiva

Misura	Backup
Descrizione	Copie di Backup per il ripristino dei dati sabotati
Rischio Contrastato	Sabotaggio- Eventi Naturali - Perdita Dati
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Preventiva

Misura	Criptazione
Descrizione	Criptazione dei dati trasmessi
Rischio Contrastato	Intercettazione Trasmissione Dati
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC

Effettività	In essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	31.03.2013
Periodicità del controllo	Annuale
Tipologia della misura	Preventiva

Misura	**Sistema Antiintrusione digitale (Firewall)**
Descrizione	Sistema Antiintrusione digitale Firewall software o hardware
Rischio Contrastato	Accesso non Autorizzato
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2013
Periodicità del controllo	Trimestrale
Tipologia della misura	Preventiva

Misura	**Manutenzione Backup**
Descrizione	Manutenzione e Test Periodico del sistema di Bakup
Rischio Contrastato	Impossibilità ripristino copie di backup
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Misura preventiva

Misura	**Aggiornamento Password**
Descrizione	Aggiornamento Periodico delle Password dei sistemi hardware e software correlati alla banca dati
Rischio Contrastato	Sabotaggio Dati
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In Essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Misura preventiva

Misura	**Aggiornamento Software**
Descrizione	Aggiornamento periodico del software
Rischio Contrastato	Bugs
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In Essere

Data Scheda	01/03/2007
Data ultimo controllo	01/03/2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Misura preventiva

Misura	**Gestione Patch al Software**
Descrizione	Controllare le modifiche segnalate del software
Rischio Contrastato	Modifiche
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In Essere
Data Scheda	01/03/2007
Data ultimo controllo	01.03.2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Automatica o avviso
Tipologia della misura	Correttiva

Misura	**Antivirus**
Descrizione	Aggiornamento Periodico Antivirus
Rischio Contrastato	Aggressione da Virus-
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In Essere
Data Scheda	01/03/2007
Data ultimo controllo	01/03/2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Preventiva

Misura	**Spyware**
Descrizione	Acquisto Software Anti Spyware e Aggiornamento Periodico
Rischio Contrastato	Spyware
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In Essere
Data Scheda	01/03/2007
Data ultimo controllo	01/03/2012
Data prossimo controllo	01.06.2012
Periodicità del controllo	Trimestrale
Tipologia della misura	Preventiva

Si è realizzata, nel durante il mese di febbraio 2007 l'informazione di tutto il personale della **Comunità Montana "Salto Cicolano"** in servizio, attraverso l'organizzazione di una specifica attività formativa per complessive 30 ore.

8. Elenco delle banche dati utilizzate dai diversi trattamenti

Nome Banca Dati	PERSONALE
Descrizione della banca dati	Anagrafica personale Comunità Montana, retribuzioni, certificazioni medico-sanitarie e contabilità fiscale – gestione contratti -
Formato Banca Dati	Elettronico - cartaceo
Tipo di dato trattato	Dati Personali e sensibili e giudiziari
Luogo in cui vengono trattati i dati	Vedi Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

Nome Banca Dati	Microsoft Office
Descrizione della banca dati	Determine e Delibere del consiglio della Comunità Montana, Determine e Delibere della giunta della Comunità Montana
Formato Banca Dati	Elettronico - cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari
Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

Nome Banca Dati	BILANCIO – CONTABILITA'
Descrizione della banca dati	Bilancio di esercizio, buste paga, gestione fiscale, gestione patrimoniale, magazzino, gestione contratti e rapporti con debitori e creditori, gestione fornitori.
Formato Banca Dati	Elettronico - cartaceo
Tipo di dato trattato	Dati Personali e sensibili
Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

Nome Banca Dati	PROTOCOLLO
Descrizione della banca dati	Posta in entrata e in uscita, protocollo in entrata e in uscita e corrispondenza generica.
Formato Banca Dati	Elettronico - Cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari
Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

Nome Banca Dati	ARCHIVIO STORICO E CORRENTE CARTACEO
Descrizione della banca dati	Fascicoli riferiti alle banche dati : • riferite all'anno in corso • non riferite all'anno in corso.
Formato Banca Dati	Cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari

Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Consultazione autorizzata e stampati in genere come da riferimenti normativi

Nome Banca Dati	RILEVAZIONE PRESENZE
Descrizione della banca dati	Sistema di rilevazione delle presenze del personale della Comunità Montana
Formato Banca Dati	Elettronico - cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari
Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Consultazione autorizzata e stampati in genere come ad riferimenti normativi

Nome Banca Dati	OPERE PUBBLICHE
Descrizione della banca dati	Incarichi professionali, ditte per gare d'appalto, stato avanzamento lavori
Formato Banca Dati	Elettronico - Cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari
Luogo in cui vengono trattati i dati	Scheda 7 (riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

Nome Banca Dati	SERVIZI SOCIALI
Descrizione della banca dati	Servizio di segretariato sociale, Servizio Assistenza Domiciliare, servizio di pronto intervento sociale, contributi economici e alle famiglie, piano affido borse lavoro sociali, contributi e servizi per la non autosufficienza, prevenzione tossico dipendenza, integrazione degli stranieri, centro diurno disabili, centri ricreativi, associazioni culturali, ricreative, sportive, utenti, servizi trasporti sociali
Formato Banca Dati	Elettronico - Cartaceo
Tipo di dato trattato	Dati Personali , sensibili e giudiziari
Luogo in cui vengono trattati i dati	Scheda 7(riferimento delibera n° 25 del 14/03/2006)
Trattamenti	Vedi scheda 1 elenco dei trattamenti (riferimento delibera n° 25 del 14/03/2006)
Modalità di diffusione dei dati	Stampati in genere come da riferimenti normativi

9. Elenco degli strumenti utilizzati nei diversi trattamenti

Strumento 1			
Nome	computer N° 2		
Descrizione	PC desktop N° 2		
Luogo di utilizzo	Ufficio amm.vo		
Descrizione luogo	Segreteria C.M.		
Marca e modello	1 Pentium – AMD ATHLON		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Napoleone Anna Maria – Pasqualone Rita		
Incaricato alla custodia delle password	Napoleone Anna Maria – Pasqualone Rita		
Effettività password	BIOS	Rete	SW
	SI	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Microsoft Windows XP Professional 2002		
Versione sistema operativo	(SE)oem		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido Lettore DVD Lettore masterizzatore CD		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Mensile		
Elenco dei software installati	Microsoft Office 2003 - 2007 Protocollo Protocollo Arco/c Rilevazione presenze Internet Explorer		
Accesso ad Internet	SI		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 2			
Nome	COMPUTER		
Descrizione	PC desktop		
Luogo di utilizzo	Ufficio Tecnico		
Descrizione luogo	Ufficio del Tecnico incaricato		
Marca e modello	Pentium		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Arch. Riccini Amedeo		
Incaricato alla custodia delle password	Arch. Riccini Amedeo		
Effettività password	BIOS	Rete	SW
	SI	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Microsoft Windows XP 2000		

Versione sistema operativo	(SE)oem		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido LETTORE DVD Lettore CD		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Mensile		
Elenco dei software installati	Microsoft Office AUTOCAD LIGHT PRIMUS Protocollo Arco/c Internet Explorer		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 3			
Nome	COMPUTER		
Descrizione	PC desktop		
Luogo di utilizzo	Ufficio Tecnico		
Descrizione luogo	Ufficio del Tecnico Incaricato		
Marca e modello	Pentium		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Geom. Lido Palluzzi		
Incaricato alla custodia delle password	Geom. Lido Palluzzi		
Effettività password	BIOS	Rete	SW
	SI	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	WINDOWS XP Home Edition 2002		
Versione sistema operativo	NT		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido Lettore masterizzatore CD Lettore DVD		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	In fase di predisposizione		
Frequenza aggiornamento antivirus	2012		
Elenco dei software installati	Microsoft Office PRIMUS Autocad Light 97 Software SIT per gestione mappe Protocollo Arco/c Internet Explorer		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 4			
Nome	computer		
Descrizione	PC desktop		

Luogo di utilizzo	Ufficio tecnico		
Descrizione luogo	Ufficio del Tecnico Incaricato		
Marca e modello	Pentium		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Geom. Vulpiani Claudio		
Incaricato alla custodia delle password	Geom. Vulpiani Claudio		
Effettività password	BIOS	Rete	SW
	SI	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Windows Professional XP 2002		
Versione sistema operativo	(SE)OEM		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Lettore Masterizzatore CD Lettore DVD Disco rigido		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Automatica		
Elenco dei software installati	Microsoft office PRIMUS Protocollo Arco/c Internet Explorer		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 5			
Nome	COMPUTER N° 2		
Descrizione	PC desktop N° 2		
Luogo di utilizzo	Area Finanziaria		
Descrizione luogo	Ufficio FINANZIARIO		
Marca e modello	Pentium Pc Olidata Vassant HM 5322		
Manutentore	Seteck Group S.r.l.		
Incaricato all'utilizzo dello strumento	RAG. DE ANGELIS MIRELLA RAG. CHERUBINI MARIA		
Incaricato alla custodia delle password	RAG. DE ANGELIS MIRELLA		
Effettività password	BIOS	Rete	SW
	SI	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Windows nt Windows XP Professional Windows 7		
Versione sistema operativo	(SE)OEM 2002		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Lettore Masterizzatore CD Lettore DVD Disco rigido		

Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Automatica		
Elenco dei software installati	Microsoft office 2003 - 2007 PAGHE SICI CONTABILITA' FINANZIARIA Internet Explorer Protocollo Arco/c		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 6			
Nome	computer		
Descrizione	PC Dekstop		
Luogo di utilizzo	Ufficio del Segretario Comunitario		
Descrizione luogo	Ufficio Amministrativo		
Marca e modello	AMD ATHLON		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	D.ssa Silvia Ridolfi		
Incaricato alla custodia delle password	D.ssa Silvia Ridolfi		
Effettività Password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Windows XP		
Versione sistema operativo	(SE) oem		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Lettore Masterizzatore CD Lettore DVD Disco rigido		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Automatica		
Elenco dei software installati	Microsoft Office De Agostini Giuridica Internet Explorer Protocollo Arco/c		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 7			
Nome	COMPUTER n° 2		
Descrizione	PC desktop n° 2		
Luogo di utilizzo	Ufficio Coordinamento Servizi		
Descrizione luogo	Ufficio Servizi Sociali		
Marca e modello	AMD ATHLON – Pentium		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Anna Rita Rossetti Stefania Coccetti		

	Costantino Cesarini Loredana Colle Annunziata Gatti Maria Rita Fornari Marilisa Gallina Gilda Lauri		
Incaricato alla custodia delle password	Anna Rita Rossetti Stefania Coccetti Costantino Cesarini Loredana Colle Annunziata Gatti Maria Rita Fornari Marilisa Gallina Gilda Lauri		
Effettività password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Mensile		
Sistema operativo	S.O. MS WINDOWS 7 HOME PREMIUM Microsoft Windows XP Professional 2000		
Versione sistema operativo	(SE)oem		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido LETTORE CD		
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012		
Versione sw antivirus	2012		
Frequenza aggiornamento antivirus	Automatica		
Elenco dei software installati	Microsoft office Internet Explorer		
Accesso ad Internet	Si		
Tipo Di accesso	LAN		
Back up	Su supporto esterno		
Strumento 9			
Nome	COMPUTER		
Descrizione	PC desktop		
Luogo di utilizzo	Ufficio SIT		
Descrizione luogo	Ufficio del Sistema Informativo Territoriale		
Marca e modello	Pentium		
Manutentore	Reateck S.r.l.		
Incaricato all'utilizzo dello strumento	Arch Riccini Amedeo		
Incaricato alla custodia delle password	Arch Riccini Amedeo		
Effettività password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	MENSILE		
Sistema operativo	Windows Home Edition versione 2002		
Versione sistema operativo	(SE)oem		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido Lettore DVD		

	Lettore masterizzatore CD
Nome sw antivirus	KASPERSKY ANTIVIRUS 2012
Versione sw antivirus	2012
Frequenza aggiornamento antivirus	Mensile
Elenco dei software installati	Software gestione mappe
Accesso ad Internet	Si
Tipo Di accesso	LAN
Back up	Su supporto esterno
Strumento 10	
Nome	Archivio Server
Descrizione	Archivio Server
Manutentore	Reateck S.r.l.
Incaricato all'utilizzo dello strumento	Arch. Riccini
Strumento 11	
Nome	Computer n° 7
Descrizione	PC desktop
Luogo di utilizzo	Ufficio Tecnico
Descrizione luogo	Ufficio del Tecnico Incaricato
Marca e modello	Pentium
Incaricato all'utilizzo dello strumento	N° 1 PC c/o Comune di Borgorose N° 1 PC c/o Comune di Pescorocchiano N° 1 PC c/o Comune di Fiamignano N° 1 PC c/o Comune di Marcetelli N° 1 PC c/o Comune di Varco Sabino N° 1 PC c/o Comune di Petrella Salto N° 1 PC c/o Comune di Concerviano
Incaricato alla custodia delle password	N° 1 PC c/o Comune di Borgorose N° 1 PC c/o Comune di Pescorocchiano N° 1 PC c/o Comune di Fiamignano N° 1 PC c/o Comune di Marcetelli N° 1 PC c/o Comune di Varco Sabino N° 1 PC c/o Comune di Petrella Salto N° 1 PC c/o Comune di Concerviano
Effettività password	BIOS: NO; Rete: SI; SW: SI
Possibilità di aggiornare autonomamente la password	SI
Sistema operativo	Microsoft Windows Home edition vers. 2002
Versione sistema operativo	(SE) oem
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Floppy Disco rigido Lettore DVD Lettore masterizzatore CD
Elenco dei software installati	Software SIT per gestione mappe Internet Explorer
Accesso ad Internet	Si
Back up	Su supporto esterno
Strumento 12	
Nome	Computer n° 8
Descrizione	PC desktop
Luogo di utilizzo	Ufficio Amm.vo

Descrizione luogo	Ufficio del Settore Amm.vo Incaricato		
Marca e modello			
Incaricato all'utilizzo dello strumento	N° 2 PC c/o Ufficio Servizi Sociali N° 1 PC c/o Settore Tecnico N° 1 PC c/o Settore Finanziario N° 1 PC c/o Comune di Borgorose N° 1 PC c/o Comune di Fiamignano N° 1 PC c/o Comune di Marcetelli N° 1 PC c/o Comune di Concerviano		
Incaricato alla custodia delle password	N° 2 PC c/o Ufficio Servizi Sociali N° 1 PC c/o Settore Tecnico N° 1 PC c/o Settore Finanziario N° 1 PC c/o Comune di Borgorose N° 1 PC c/o Comune di Fiamignano N° 1 PC c/o Comune di Marcetelli N° 1 PC c/o Comune di Concerviano		
Effettività password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Windows 7 HOME PREMIUM AOC		
Versione sistema operativo	2012		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	Disco rigido Lettore DVD Lettore masterizzatore CD		
Elenco dei software installati	Internet Explorer OFFICE ADOBE READER MICROSOFT ILLUSTRATOR PAINT		
Accesso ad Internet	Si		
Back up	Su supporto esterno		

10 .Elenco Struttura Organizzativa della Comunità Montana

Struttura interna (organigramma amministrativo):

Nome	CARMINE		
Cognome	RINALDI		
Ruolo	***Titolare del Trattamento Dati –*** Presidente della Comunità Montana "SALTO CICOLANO"		
ANAGRAFICA	12/11/1953	FIAMIGNANO	Cod.Fisc. RNL CMN 53S 12D 560L

Nome	SILVIA		
Cognome	RIDOLFI		
Ruolo	***Responsabile del Trattamento Dati –*** Segretario Generale della Comunità Montana "Salto Cicolano"		
ANAGRAFICA	26/03/1962	ROMA	Cod.Fisc. RDL SLV 62C 66H 501R

Nome	ANNA MARIA		
Cognome	NAPOLEONE		
Ruolo	Incaricato al Trattamento Dati *(Area Amministrativa)*		
ANAGRAFICA	20/11/1956	BORGOROSE	Cod. Fisc. NPL NMR 56S 60B 008Q

Nome	RITA		
Cognome	PASQUALONE		
Ruolo	Incaricato al Trattamento Dati *(Area Amministrativa)*		
ANAGRAFICA	02/07/1965	TORNIMPARTE	Cod.Fisc. PSQ RTI 65L 42L 227E

Nome	AMEDEO		
Cognome	RICCINI		
Ruolo	*Responsabile Area Tecnica*		
ANAGRAFICA	15/02/1958	FERENTINO	Cod.Fisc. RCC MDA 58B 15D 539F

Nome	LIDO		
Cognome	PALLUZZI		
Ruolo	*Incaricato al Trattamento Dati (Aria Tecnica)*		
ANAGRAFICA	01/01/1951	PESCOROCCHIANO	Cod.Fisc. PLL LDI 51° 01G 498Y

Nome	CLAUDIO		
Cognome	VULPIANI		
Ruolo	*Incaricato al Trattamento Dati (Aria Tecnica)*		
ANAGRAFICA	09/08/1960	MARCETELLI	Cod.Fisc. VLP CLD 60M 09E 927B

Nome	MIRELLA		
Cognome	DE ANGELIS		
Ruolo	*Responsabile Area Finanziaria*		
ANAGRAFICA	05/04/1957	ROMA	Cod.Fisc. DNG MMR 57D 45H 501Q

IL TITOLARE DEL TRATTAMENTO
Il Presidente
Ing. Carmine Rinaldi

Il presente verbale viene letto, approvato e sottoscritto come segue:

IL SEGRETARIO
D.SSA SILVIA RIDOLFI

IL PRESIDENTE
Ing. Carmine Rinaldi

Visto: si esprime parere favorevole in ordine alla regolarità tecnica del presente provvedimento, ai sensi e per gli effetti dell'art. 49 del D.L.vo 18 agosto 2000 n° 267.

Il Responsabile del Procedimento

Il Responsabile del Settore Amm.vo
D.ssa Silvia Ridolfi

Visto: si esprime parere favorevole in ordine alla regolarità contabile del presente provvedimento, ai sensi e per gli effetti dell'art. 49 del D.L.vo 18 agosto 2000 n° 267.

Il Responsabile del Settore Fin.rio
Rag. Mirella DE ANGELIS

PUBBLICAZIONE E SPEDIZIONE DELL'ATTO

Si attesta che la presente deliberazione è affissa all'albo pretorio della Comunita' Montana dal 13 LUG. 2012 al 27 LUG. 2012 per quindici giorni consecutivi.

IL SEGRETARIO
D.ssa Silvia Ridolfi

Lì 13 LUG. 2012

COPIA CONFORME

è copia conforme all'originale, si rilascia per uso d'ufficio

Lì _____

IL SEGRETARIO

D.ssa Silvia Ridolfi

La presente deliberazione è stata comunicata ai Capigruppo Consiliari con nota n° 12082 del 13 LUG. 2012. La stessa è divenuta esecutiva ai sensi del D.L..vo 267/2000 il _____.

- ☐ poiché dichiarata immediatamente eseguibile (art. 134, comma 4, D.L..vo 267/2000)
- ☐ decorsi 10 giorni dalla pubblicazione (art. 134, comma 3, D.L..vo 267/2000)
- ☐ in quanto confermata con il voto favorevole della maggioranza dei componenti il Consiglio (art. 127, comma 2, D.L..vo 267/2000)

LI, 13 LUG. 2012

IL SEGRETARIO

Sottoposta al controllo eventuale
Ai sensi del T.U. D.Lvo n° 267/2000
- ☐ per iniziativa della Giunta Comunitaria (art. 17, comma 34)
- ☐ per richiesta dei Consiglieri

(art. 17, comma 38)
IL SEGRETARIO
f.to _____