DELIBERAZIONE N.98 DEL 29/12/2005

COMUNE DI GALEATA
Provincia di Forlì-Cesena

Trasmessa al C.R.C. il

col Protocollo n.

COPIA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: Documento programmatico sulla sicurezza: approvazione.

L'anno duemilacinque, addì ventinove del mese di dicembre, alle ore 20,00, nella sala delle adunanze, si è oggi riunita la Giunta comunale con l'intervento dei signori:

	PRESENTE	ASSENTE
Valentini Rodolfo	Si	
Ragazzini Giancarlo	Si	
Palareti Federica	Si	
Mazzoli Paolo	Si	
Malpezzi Eros	Si	

Partecipa il Segretario Comunale **Dott. ssa Roberta Fiorini.**

Dato atto che il numero dei presenti è legale per la validità della deliberazione, **il Sig. Rodolfo Valentini, sindaco,** assume la presidenza e dichiara aperta la discussione.

La Giunta comunale prende in esame l'oggetto sopraindicato.

LA GIUNTA COMUNALE

Premesso:

- Che l'entrata in vigore della legge 31.12.1996 n. 675 ha posto a carico degli Enti locali precisi adempimenti da rispettare in materia di tutela della riservatezza dei dati personali;

- Che il DPR 28 luglio 1999 n. 318 ha indicato le norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2, della legge 31.12.1996 n. 675;

- Che la legge 3.11.2000 n. 325, pubblicata sulla gazzetta ufficiale n. 262 del 9.11.2000 ha definito le disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31.12.1996, n. 675;:

Considerato:

- Che il Comune di Galeata, in attuazione delle citate norme di legge ha provveduto ad adottare i seguenti atti:
  - Delibera della Giunta Comunale n. 33 del 29/03/2000, di approvazione delle misure minime di sicurezza nel trattamento dei dati personali in sede di prima applicazione della citata disciplina dell'art. 15 della legge 675/1996 come previste dal DPR n. 318/1999;
  - Determinazioni dei Responsabili Servizi, relative all'adozione del documento relativo alla citata disciplina dell'art. 15 della legge 675/1996

Considerato altresì:

- che il decreto legislativo n. 196 del 30.6.2003 si è posto come testo unico delle numerose norme sulla disciplina della privacy, in ragione della complessa normativa, e che lo stesso decreto legislativo agli artt. 33 e 35 ed all'allegato B stabilisce le misure minime di sicurezza che la disposizione transitoria di cui all'art. 180 stabilisce che l'adozione debba avvenire entro il 30.6.2004 nel caso in cui le stesse non fossero state adottate nell'anno 2000, in attuazione al DPR 318/1999;
- che quindi questo Comune, avendo già ottemperato come sopra evidenziato agli obblighi di cui al DPR 318/1999 non rientra fra gli Enti ai quali si applica tale disposizione transitoria, essendo del resto il documento programmatico della sicurezza in uso rispettoso delle disposizioni normative succedutesi nel tempo e riepilogate come già indicato del decreto legislativo 196/2003;

Considerato infine:

- che il Garante per la protezione dei dati personale tuttavia, con circolare del maggio 2004 ha indicato la formalizzazione dei contenuti del documento programmatico sulla sicurezza, ritenendosi quindi, senza che vi sia obbligo, opportuno uniformare il documento programmatico sulla sicurezza in essere allo schema predisposto dallo stesso garante;
- che quindi è stato predisposto il documento programmatico della sicurezza, riportato in allegato (All.1) e parte integrante del presente atto, che recepisce lo schema indicato dal garante e riporta alla stessa formalizzazione i contenuti sostanziali;

Dato atto che con la presente approvazione si provvede all'adempimento dell'obbligo relativo alla redazione del documento programmatico sulla sicurezza la cui scadenza al 31\12\2005 è stata prorogataq con specifico decreto in corso di pubblicazione sulla Gazzetta Ufficiale al 31\03\2006;

Visti i pareri favorevoli del responsabile del servizio affari generali, del responsabile del servizio tecnico e del responsabile del servizio ragioneria, in ordine alla regolarità tecnica ai sensi dell''art.49 D.Lgs. 18/08/2000, n267;

A voti unanimi, palesemente espressi;

DELIBERA

La premessa costituisce parte integrante del dispositivo;

- Di approvare, in esecuzione al disposto del decreto legislativo 196/2003, il documento programmatico della sicurezza relativo alle misure minime di sicurezza nel trattamento dei dati personali, riportato in allegato (Allegato n. 1) parte integrante e sostanziale del presente provvedimento che recepisce lo schema indicato dal garante e riporta alla stessa formalizzazione i contenuti sostanziali;

- Di riservarsi di uniformare i provvedimenti in esercizio ai contenuti del documento programmatico riportato in allegato (Allegato n. 1)

Con separata ed identica votazione, di dichiarare il presente immediatamente eseguibile, ai sensi dell'art.134 T.U.EE.L. n.267/2000

Parere tecnico: favorevole
Il responsabile del servizio
(geom. Giorgio Ferretti)
F.to
Parere tecnico: favorevole
Il responsabile del servizio
(Marzia Biondi)
F.to
Parere tecnico: favorevole
Il responsabile del servizio
(*Annamaria Albertini*)
F.to

COMUNE DI GALEATA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
(art. 34 e allegato B del codice in materia di protezione dei dati personali)

Indice:

Allegati:

SEZIONE 1:
ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

Questa sezione comprende l'elenco dei trattamenti effettuati dal Titolare direttamente(anche tramite l'impiego dei Responsabili e degli Incaricati) o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura interna od esterna che operativamente effettua il trattamento.

Per ciascun trattamento sono riportate le seguenti informazioni:

- ***Numero d'ordine (identificativo del trattamento)***
- ***Servizio di appartenenza (struttura di riferimento)***
- ***Banca dati***
- ***Natura dei dati trattati (indica la presenza o meno di dati giudiziari o sensibili)***

Si specificano inoltre le seguenti informazioni valide per tutti i trattamenti eseguiti in maniera informatica:

- ***Ubicazione fisica dei supporti di memorizzazione: le banche dati di valenza generale sono collocate sul server del Comune(1-47-eccetto 12,29,34,47);le banche dati specialistiche (12,29,34,47) sono collocate su PC presenti nei vari Uffici interessati;***
- ***Tipologia dei dispositivi d'accesso: i dispositivi d'accesso sono personal computer in rete locale connessi al server centrale (per le banche dati centralizzate oppure PC contenenti le banche dati specialistiche ;***
- ***Tipologia di interconnessione: tutti i personal computer sono collegati in rete locale oppure in rete MAN e WAN attraverso cablaggi in rame e fibra ottica***

Numero d'ordine	*Servizio di appartenenza*	**Denominazione gestita in maniera cartacea**		**Denominazione gestita in maniera informatica**	
		Con presenza dati sensibili	*Senza dati sensibili*	*Con presenza dati sensibili*	*Senza dati sensibili*
1.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI ANAGRAFE DELLA POPOLAZIONE RESIDENTE BANCA DATI ANAGRAFE ITALIANI RESIDENTI ALL'ESTERO		BANCA DATI ANAGRAFE DELLA POPOLAZIONE RESIDENTE BANCA DATI ANAGRAFE ITALIANI RESIDENTI ALL'ESTERO	
2.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI FASCICOLI PERSONALI BANCA DATI SCHEDARIO ELETTORALE (LISTE GENERALI, LISTE SEZIONALI, SCHEDE GENERALI,		BANCA DATI SCHEDARIO ELETTORALE (LISTE GENERALI, LISTE SEZIONALI, SCHEDE GENERALI,	
3.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI ALBO SCRUTATORI DI SEGGIO ALBO PRESIDENTI DI SEGGIO		BANCA DATI ALBO SCRUTATORI DI SEGGIO ALBO PRESIDENTI DI SEGGIO	
4.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI ALBO DEI GIUDICI POPOLARI		BANCA DATI ALBO DEI GIUDICI POPOLARI	
5.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)		BANCA DATI ARCHIVIO DEI PENSIONATI		BANCA DATI ARCHIVIO DEI PENSIONATI
6.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI ARCHIVIO DELLE LISTE DI LEVA ARCHIVIO RUOLI MATRICOLARI		LISTE DI LEVA	

7.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)		BANCA DATI ARCHIVIO CARTELLINI DELLE CARTE D'IDENTITA' RILASCIATE		BANCA DATI ARCHIVIO CARTELLINI DELLE CARTE D'IDENTITA' RILASCIATE
8.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI REGISTRI DI STATO CIVILE		BANCA DATI REGISTRI DI STATO CIVILE	
9.	AREA AMMINISTRATIVA – AFFARI GENERALI (Servizi demografici)	BANCA DATI PRESTAZIONI SOCIALI (ASSEGNO 2° FIGLIO			
Numero D'ordine	***Servizio di Appartenenza***	***Denominazione gestita in maniera cartacea***		***Denominazione gestita in maniera informatica***	
		Con presenza dati sensibili	***Senza dati sensibili***	***Con presenza dati sensibili***	***Senza dati sensibili***
10.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI AMMINISTRATORI COMUNALI		BANCA DATI AMMINISTRATORI COMUNALI	
11.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)		BANCA DATI ARCHIVIO CARTACEO DEI CONTRATTI		BANCA DATI ARCHIVIO CARTACEO DEI CONTRATTI
12.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)		BANCA DATI ANAGRAFE TRIBUTARIA SCRITTURE PRIVATE		BANCA DATI ANAGRAFE TRIBUTARIA SCRITTURE PRIVATE

13.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)		BANCA DATI PER FORNITURE DI BENI E DI SERVIZI		
14.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI ATTI RELATIVI AI PROCEDIMENTI GIUDIZIARI CIVILI, PENALI, AMMINISTRATIVI			
15.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI AUTORIZZAZIONI SANITARIE		BANCA DATI AUTORIZZAZIONI SANITARIE	
16.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI UTENTI SERVIZIO TRASPORTO SCOLASTICO		BANCA DATI UTENTI SERVIZIO TRASPORTO SCOLASTICO	
17.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI UTENTI SERVIZIO MENSA			
18.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI BENEFICIARI CONTRIBUTI DIRITTO ALLO STUDIO		BANCA DATI BENEFICIARI CONTRIBUTI DIRITTO ALLO STUDIO	

19.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI OBIETTORI E VOLONTARI SERVIZIO CIVILE		BANCA DATI OBIETTORI E VOLONTARI SERVIZIO CIVILE	
20.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)		BANCA DATI LICENZE DI PESCA		
21.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)		BANCA DATI DEI TESSERINI PER ESERCIZIO VENATORIO		
22.	AREA AMMINISTRATIVA – AFFARI GENERALI (Segreteria-Archivio Protocollo)	BANCA DATI ALBO DEI BENEFICIARI DI PROVVIDENZE DI NATURA ECONOMICA		BANCA DATI ALBO DEI BENEFICIARI DI PROVVIDENZE DI NATURA ECONOMICA	

Numero d'ordine	*Servizio di appartenenza*	*Denominazione gestita in maniera cartacea*		*Denominazione gestita in maniera informatica*	
		Con presenza dati sensibili	*Senza dati sensibili*	*Con presenza dati sensibili*	*Senza dati sensibili*
23.	AREA CONTABILE (Personale)	BANCA DATI DIPENDENTI DI RUOLO E NON DI RUOLO		BANCA DATI DIPENDENTI DI RUOLO E NON DI RUOLO	
24.	AREA CONTABILE (Personale)	BANCA DATI ISCRITTI ALLE ORGANIZZAZIONI SINDACALI TERRITORIALI E AZIENDALI		BANCA DATI ISCRITTI ALLE ORGANIZZAZIONI SINDACALI TERRITORIALI E AZIENDALI	

25.	AREA CONTABILE (Personale)	BANCA DATI CONCORSI PUBBLICI			
26.	AREA CONTABILE (Personale)		BANCA DATI ANAGRAFE DELLE PRESTAZIONI DIPENDENTI E CONSULENTI		BANCA DATI ANAGRAFE DELLE PRESTAZIONI DIPENDENTI E CONSULENTI
27.	AREA CONTABILE (Personale)	BANCA DATI COMUNICAZIONI DI INFORTUNIO SUL LAVORO			
28.	AREA CONTABILE (Finanziario-econocmato)		BANCA DATI DEI FORNITORI DELL'ENTE E CLIENTI		BANCA DATI DEI FORNITORI DELL'ENTE E CLIENTI
29.	AREA CONTABILE (Finanziario-econocmato		BANCA DATI ILLUMINAZIONE VOTIVA, ECC.		BANCA DATI ILLUMINAZIONE VOTIVA, ECC.
30.	AREA CONTABILE (Finanziario-econocmato		MUTUI, FINANZIAMENTI AGEVOLATI		MUTUI, FINANZIAMENTI AGEVOLATI

Numero d'ordine	*Servizio di appartenenza*	*Denominazione gestita in maniera cartacea*		*Denominazione gestita in maniera informatica*	
31.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI AUTORIZZAZIONE ALLO SCARICO DELLE ACQUE REFLUE IN FOGNATURA		BANCA DATI AUTORIZZAZIONI ALLO SCARICO
32.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI AUTORIZZAZIONE ALL'OCCUPAZIONE SUOLO PUBBLICO		BANCA DATI AUTORIZZAZIONE OCCUPAZIONE SUOLO PUBBLICO
33.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI AUTORIZZAZIONI ALLE EMISSIONI IN ATMOSFERA		
34.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI CATASTALI (SIA URBANO CHE TERRENI) CONSERVAZIONE DEI FOGLI DI MAPPA DEL C.T.		BANCA DATI CATASTALI (SIA URBANO CHE TERRENI) CONSERVAZIONE DEI FOGLI DI MAPPA DEL C.T.
35.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI DEPOSITI PROGETTI PER LE COSTRUZIONI IN ZONA SISMICA		
36.	AREA TECNICA (urbanistica, edilizia privata, ambiente	BANCA DATI PERMESSO A COSTRUIRE IN SANATORIA	BANCA DATI D.I.A. TARDIVI	BANCA DATI PERMESSO A COSTRUIRE IN SANATORIA	BANCA DATI D.I.A. TARDIVI
37.	AREA TECNICA (urbanistica, edilizia privata, ambiente		BANCA DATI CONCESSIONI EDILIZIE, AUTORIZZAZIONI EDILIZIE, D.I.A. (DICHIARAZIONI DI INIZIO ATTIVITA'), CONFORMITÀ' EDILIZIA PERMESSI DI COSTRUIRE		BANCA DATI D.I.A., CONFORMITÀ' EDILIZIA E PERMESSI DI COSTRUIRE

38.	AREA TECNICA (lavori pubblici)		BANCA DATI INCARICHI PROFESSIONALI A PROFESSIONISTI		BANCA DATI INCARICHI PROFESSIONALI A PROFESSIONISTI
39.	AREA TECNICA (lavori pubblici)		BANCA DATI CONCESSIONARI FINANZIAMENTI PER DANNI TERREMOTO		BANCA DATI CONCESSIONARI FINANZIAMENTI PER DANNI TERREMOTO
40.	AREA TECNICA (lavori pubblici)		BANCA DATI CONCESSIONARI MATERIALE INERTE		BANCA DATI CONCESSIONARI MATERIALE INERTE
41.	AREA TECNICA (lavori pubblici)		BANCA DATI RIFERITI A FORNITORI DI BENI ED ESECUTORI DI SERVIZI		BANCA DATI RIFERITI A FORNITORI DI BENI ED ESECUTORI DI SERVIZI
42.	AREA TECNICA (lavori pubblici)		BANCA DATI AUTORIZZAZIONI OPERAZIONI CIMITERIALI		BANCA DATI AUTORIZZAZIONI OPERAZIONI CIMITERIALI
43.	AREA TECNICA (lavori pubblici)	BANCA DATI OFFERTE PER APPALTI LAVORI PUBBLICI, FORNITURE DI BENI E DI SERVIZI			STATISTICA LAVORI PUBBLICI
44.	AREA TECNICA (edilizia)		BANCA DATI AUTORIZZAZIONI IMPIANTI DI ASCENSORE		BANCA DATI AUTORIZZAZIONI IMPIANTI DI ASCENSORE
45.	AREA TECNICA (edilizia)	BANCA DATI DOMANDE ASSEGNAZIONE ALLOGGI E.R.P. E MINIAPPARTAMENTI PER ANZIANI			
46.	AREA TECNICA (edilizia)		ANAGRAFE TRIBUTARIA		BANCA DATI ANAGRAFE TRIBUTARIA (PERMESSI A COSTRUIRE)
47.	AREA TECNICA (edilizia)		BANCA DATI ANAGRAFE CANINA		BANCA DATI ANAGRAFE CANINA

Numero d'ordine	*Servizio di appartenenza*	**Denominazione gestita in maniera cartacea**		**Denominazione gestita in maniera informatica**	
		Con presenza dati sensibili	***Senza dati sensibili***	***Con presenza dati sensibili***	***Senza dati sensibili***
48.	POLIZIA MUNICIPALE	RILASCIO DELLE LICENZE PUBBLICA SICUREZZA		RILASCIO DELLE LICENZE PUBBLICA SICUREZZA	
49.	POLIZIA MUNICIPALE	ATTIVITA RELATIVA ALL'INFORTUNISTICA STRADALE		ATTIVITA RELATIVA ALL'INFORTUNISTICA STRADALE	
50.	POLIZIA MUNICIPALE	ATTIVITA DI POLIZIA ANNONARIA COMMERCIALE ED AMMINISTRATIVA		ATTIVITA DI POLIZIA ANNONARIA COMMERCIALE ED AMMINISTRATIVA	
51.	POLIZIA MUNICIPALE	ATTIVITA DI VIGILANZA IN MATERIA DI AMBIENTE SANITA E POLIZIA MORTUARIA		ATTIVITA DI VIGILANZA IN MATERIA DI AMBIENTE SANITA E POLIZIA MORTUARIA	
52.	POLIZIA MUNICIPALE	BANCA DATI COMMERCIO AMBULANTE		BANCA DATI COMMERCIO AMBULANTE	
53.	POLIZIA MUNICIPALE	PROVVEDIMENTI SANITARI OBBLIGATORI		PROVVEDIMENTI SANITARI OBBLIGATORI	

SEZIONE 2

In questa sezione viene riportata una mappa che associa ai settori i trattamenti da questi effettuati, con l'indicazione della descrizione sintetica e delle responsabilità, rinviando al regolamento sull'ordinamento degli uffici e dei servizi ovvero ad atti specifici di gestione del personale ogni e più completa analisi.
In modo particolare si evidenziano i trattamenti sotto specificati:

Banca Dati	Responsabile area	Trattamenti operati dal servizio	Compiti del servizio
01-22	Responsabile dell'area Amministrativa - Affari Generali	Gestione dei servizi demografici gestione segreteria; gestione protocollo-archivio;	Acquisizione, caricamento dei dati, consultazione, comunicazione a terzi
23-30	Responsabile dell'area contabile	Gestione dei servizio personale;gestione finanziario economato	Acquisizione, caricamento dei dati, consultazione, comunicazione a terzi

31-47	Responsabile dell'area tecnica	Gestione del servizio urbanistica - edilizia	Acquisizione, caricamento dei dati, consultazione, comunicazione a terzi
48-53	Responsabile P.M.	Gestione servizio Polizia Municipale	Acquisizione, caricamento dei dati, consultazione, comunicazione a terzi

Mentre per la funzione specialistica informatica di "manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica delle basi dei dati (salvataggi, ripristini, ecc.)", delegata alla comunità montana dell'Appennino forlivese, questi vengono affidati ad apposita struttura specialistica.
Da cui:

Banca dati	Responsabile	Trattamenti operati	Compiti
01-53	Responsabile dell'Ufficio Associato di Informatica e statistica	Gestione delle attività informatiche	manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica delle basi dei dati (salvataggi, ripristini, ecc.)

Inoltre vengono elencati i compiti e le responsabilità assegnati/e:
A. ai Responsabili del trattamento, identificati nei termini di legge dal Titolare,
B. agli Incaricati del trattamento, identificati nei termini di legge dai Responsabili del trattamento;
C. alla struttura informatica associata (Ufficio per la gestione associato di Informatica e Statistica):
Esse sono:

A. FUNZIONI DEL RESPONSABILE DEL TRATTAMENTO, INDIVIDUATE AI SENSI E PER GLI EFFETTI DEL DLGS 196/2003

Il Responsabile ha il dovere di compiere quanto si renderà necessario ai fini del rispetto e della corretta applicazione del DLGS 196/2003 e può esercitare, in tal senso, autonomi poteri gestionali e di controllo.

Specificatamente il Responsabile è tenuto a:

1. ***In relazione agli incaricati:***
   - Individuare e nominare per iscritto gli incaricati del trattamento, impartendo loro, ancora per iscritto, le idonee istruzioni, anche tenuto conto dei compiti indicati dall'Amministratore del sistema;
   - Vigilare sul rispetto delle istruzioni impartite agli incaricati.

2. ***In relazione al Titolare:***

- Adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare del trattamento,
- Vigilare sul rispetto di dette misure di sicurezza da parte dei soggetti nominativamnte incaricati;
- Verificare (semestralmente) lo stato di applicazione del DLGS 196/2003, nonché verificare il buon funzionamento, la corretta applicazione e la conformità alle indicazioni dell'Autorità Garante dei sistemi e delle misure di sicurezza adottate;
- Comunicare immediatamente al Titolare gli eventuali nuovi trattamenti da intraprendere nella propria Area di competenza, provvedendo alle necessarie formalità di legge.

3. ***In relazione allo sviluppo dell'attività ed all'organizzazione dell'area in cui opera:***
   - Predisporre quanto necessario affinchè siano rispettate le disposizioni già previste degli articoli 9 e 10 del DPR 28.7.1999 n. 318 per il trattamento dei dati personali effettuati con strumenti diversi da quelli elettronici od automatizzati o contenuti in banche dati cartacee, in modo particolare:
     - Predisporre quanto necessario affinchè i dati vengano conservati chiusi a chiave nei contenitori collocati presso i vari uffici e nei locali adibiti ad archivio; dare disposizioni agli incaricati del trattamento affinchè, i dati se prelevati dagli incaricati i dati debbano essere trattenuti diligentemente, evitando accessi indebiti da parte di estranei non autorizzati o non incaricati del trattamento; dare disposizioni affinchè al termine dell'utilizzo vengano ricollocati nei rispettivi contenitori e/o archivi; ed affinchè gli atti e documenti contenenti dati sensibili utilizzati dagli incaricati (solo ed esclusivamente per compiti d'ufficio) siano conservati in contenitori muniti di serratura;
     - Predisporre quanto necessario affinchè i contenitori (armadi, schedari e simili) contenenti dati personali vengano sempre chiusi a chiave dopo l'utilizzo da parte degli incaricati; così pure che ciò avvenga per i locali in cui vengono archiviati dati personali; inoltre deve dare le disposizioni affinchè le chiavi degli armadi, schedari, cassettiere ed archivi siano conservate presso lo stesso Responsabile del trattamento competente oppure in luogo all'interno del l'area conosciuto solamente dagli incaricati interessati e dai rispettivi Responsabili del trattamento; il Responsabile del trattamento potrà designare anche un incaricato per la custodia delle chiavi;
   - Predisporre quanto necessario, seguendo le indicazioni dell'Amministratore del sistema, per il corretto trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori (assumendo in tale veste il ruolo di Amministratore del sistema);
   - Predisporre in caso di necessità una relazione scritta in ordine a tutti gli adempimenti eseguiti ai sensi del DLGS 196/2003, alla documentazione raccolta ed archiviata ai sensi della medesima legge, nonché in ordine alle misure di sicurezza. Tale relazione dovrà essere, successivamente, trasmessa al Titolare del trattamento;
   - Distruggere i dati personali in caso di cessazione del trattamento degli stessi, provvedendo alle necessarie formalità.
   - Verificare la correttezza dei dispositivi antincendio per i locali e/o i siti in cui hanno sede le banche dati contenenti i dati personali e dare pronta comunicazione al Titolare in caso di interventi di adeguamento;
   - Verificare la corretta continuità dell'alimentazione elettrica per i locali e/o i siti in cui hanno sede le banche dati contenenti i dati personali e dare pronta comunicazione al Titolare in caso di interventi di adeguamento.

4. ***In relazione ai cittadini:***
   - Predisporre le soluzioni organizzative e procedurali volte a consentire la massima diffusione in relazione all'attività amministrativa, delle informazioni di cui all'art. 13 D.Lgs 196/2003;
   - Evadere tempestivamente tutte le richieste e gli eventuali reclami degli interessati;
   - Operare al fine di facilitare l'interessato nell'esercizio dei diritti di cui agli artt. 7 e 8 D.Lgs 196/2003.

5. ***In relazione ai rapporti con il Garante e con i soggetti deputati al controllo sull'applicazione del D.Lgs 196/2003:***
   - Evadere tempestivamente le richieste di informazioni da parte del Garante e dare immediata esecuzione alle indicazioni che perverranno dalla medesima Autorità;
   - Interagire con i soggetti incaricati di eventuali verifiche, controlli, ispezioni;
   - Interagire con l'Amministratore del sistema per la migliore organizzazione della sicurezza informatica

B. FUNZIONI DEGLI INCARICATI DEL TRATTAMENTO IDENTIFICATI NEI TERMINI DI LEGGE DAI RESPONSABILI DEL TRATTAMENTO

MANSIONARIO DELL'INCARICATO IN RELAZIONE ALL'APPLICAZIONE DEL D.Lgs 196/2003.

Al fine di una corretta applicazione del DLGS 196/2003 i soggetti individuati come incaricati dovranno:

1. ***In relazione al trattamento:***
   - Trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza, comunque nel rispetto di quanto previsto dall'art. 30 del DLGS 196/2003;
   - Effettuare le operazioni di trattamento di dati personali come individuate esclusivamente per lo svolgimento delle proprie mansioni, nell'ambito dello sviluppo delle funzioni e dei compiti dell'Ente, nel rispetto delle norme di legge, di statuto, di regolamento che disciplinano l'attività;
   - Comunicare o diffondere i dati personali trattati con esplicita autorizzazione del responsabile e comunque nel rispetto delle leggi e regolamenti.

2. ***In relazione alla gestione delle banche dati:***
   - Accedere unicamente alle banche dati specificamente indicate;

- Aggiornare periodicamente le informazioni contenute nelle banche dati sulle quali si opera;
- Evitare di creare banche dati nuove senza espressa autorizzazione del responsabile del trattamento;
- Evitare di asportare, danneggiare o manipolare supporti informatici o cartacei contenenti dati personali di terzi, con procedure non standardizzate/autorizzate.

3. ***In relazione alle misure di sicurezza:***
   - Mantenere assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle proprie funzioni;
   - Osservare scrupolosamente le misure di sicurezza individuate in relazione alla banche dati dell'area di propria afferenza;
   - Fare attento uso di accesso autorizzato (password personali) alle banche dati e verificare che in propria assenza tali sistemi non siano stati violati e rispettare, per quanto attiene al salvataggio dei dati utilizzo di chiavi di accesso, prevenzione dall'intrusione di virus informatici, quanto previsto dal regolamento sull'utilizzo degli strumenti informatici in rapporto alle misure previste nel documento programmatico – piano operativo delle misure di sicurezza dei dati personali comunali;
   - Curare che i dati vengano conservati chiusi a chiave nei contenitori collocati presso i vari uffici e nei locali adibiti ad archivio; se prelevati dagli incaricati dovranno essere trattenuti diligentemente, evitando accessi indebiti da parte di estranei non autorizzati o non incaricati del trattamento; al termine dell'utilizzo dovranno essere ricollocati nei rispettivi contenitori e/o archivi; gli atti e documenti contenenti dati sensibili utilizzati dagli incaricati (solo ed esclusivamente per compiti d'ufficio) debbono essere conservati in contenitori muniti di serratura;
   - Assicurarsi che i contenitori (armadi, schedari e simili) contenenti dati personali vengano sempre chiusi a chiave dopo l'utilizzo; così pure deve avvenire per i locali in cui vengono archiviati dati personali; le chiavi degli armadi, schedari, cassettiere ed archivi sono conservate presso il Responsabile del trattamento competente o in luogo all'interno dell'area conosciuto solamente dagli incaricati interessati e dai rispettivi Responsabili del trattamento;
   - I dati personali debbono essere trattati per il tempo strettamente necessario al trattamento, riposti con cura ed attenzione nel proprio archivio, armadio, cassettiera ed ogni altro sito atto alla conservazione, avendo cura che non vi sia indebito accesso da parte di estranei.

C. FUNZIONI DELLA STRUTTURA INFORMATICA ASSOCIATA (UFFICIO PER LA GESTIONE ASSOCIATA DI INFORMATICA E STATISTICA):

E' il soggetto che si pone come Organo Tecnico Specialistico del Titolare e pertanto come caudiutore dello stesso per la gestione informatica delle sicurezze informatiche.
E' il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati organizzato in archivi gestiti elettronicamente e di consentirne l'utilizzazione, cioè ha la supervisione effettiva sull'adozione delle misure di sicurezza.

1. è il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati organizzato in archivi gestiti elettronicamente e di consentirne l'utilizzazione, cioè ***ha la supervisione effettiva sull'adozione delle misure di sicurezza.***

2. è il soggetto che provvede ai compiti stabiliti dagli artt. 2 e 4 dell'ex DPR 28.7.1999 n. 318;

3. è il soggetto che provvedere ai compiti stabiliti dall'art. 6 dell'ex DPR 28.7.1999 n. 318;

4. è il soggetto che propone e formula i piani formativi in attuazione del documento programmatico – piano operativo delle misure di sicurezza per le componenti informatiche;

5. è il soggetto che dà attuazione al documento programmatico – piano operativo delle misure di sicurezza; controlla l'attuazione e riferisce al Titolare ed ai Responsabili del trattamento per le componenti informatiche.

Il Responsabile dell'Ufficio per la gestione associata di informatica e statistica formulerà, per le funzioni assegnate, apposito piano operativo, tenuto conto delle funzioni specialistiche informatiche, della periodicità e quotidianità dello svolgimento di alcune attività e della distanza dei Comuni dalla propria sede.

Il citato piano comprenderà anche funzioni puntualmente definite per contenuti, tempi e modalità operative *la cui esecuzione, in quanto si è in presenza di una forma associativa, è assegnata a personale dei singoli Comuni*, responsabile comunale del sistema informativo ed informatico e custode delle password, personale che dovrà essere individuato ed incaricato per tale finalità; ed opererà in tale senso come collaboratore del Responsabile dell'Ufficio per la gestione associata delle attività informatiche e statistiche, per perseguire le finalità di sicurezza dei dati contenute nelle banche dati comunali.

Vengono di seguito elencate, a scopo illustrativo, le funzioni comprese in tale funzione di sicurezza dei dati contenuti in banche dati su elaboratori server:

COMPITI A TUTELA DELL'INTEGRITA' DEL SISTEMA AFFIDATI A STRUTTURA SPECIALISTICA

Controllo risorse dei server:

- Check capienza dischi, risorse di sistema (memoria, processi);
- Check dimensionamento spazi DB SQL Server;

- Check applicazioni installate;
- Eliminazione file inutili;

cadenza: almeno trimestrale

Ottimizzazione SQL:

- Check integrità SQL Server;
- Ristrutturazione DB;

cadenza almeno trimestrale

Controllo lettura backup:

(la lettura dei log di backup è effettuata quotidianamente del referente comunale del sistema informativo ed informatico – custode delle password limitatamente all'orario di avvio e chiusura backup).

- Controllo che le cassette di backup siano effettivamente leggibili;
- Controllo che le cassette di backup siano correttamente ruotate una volta raggiunto il numero massimo di riutilizzo e
- Pulizia delle testine DAT a cura del referente comunale

Cadenza almeno trimestrale

Controllo Utenti:

Verifica da compiere unitamente al responsabile comunale del sistema informativo ed informatico

- Controllo degli utenti definiti nel sistema e relative autorizzazioni;
- Eliminazione degli utenti e delle configurazioni obsolete;
- Controllo corrette autorizzazioni di accesso al file system;
- Controllo log collegamenti PC Anywhere;
- Controllo utenti Exchange e di posta Internet;

cadenza almeno annuale

Controllo funzionalità antivirus:

- Attivazione antivirus sui server;
- Aggiornamento files antivirus;
- Controllo antivirus sui server;
- Controllo correttezza esecuzione antivirus su client (a campione);

cadenza almeno trimestrale

Inoltre:

- Monitoraggio accesso rete;
- Controllo corretto funzionamento diap-up dei router al fine di controllare che:
- Funzioni correttamente il dial-up ed il dial-out;
- Funzioni correttamente lo sgancio della linea di trasmissione dati;
- Non ci siano tempi di collegamento inconsueti (eccessivi).

cadenza almeno semestrale

Infine in allegato (ALLEGATO n. 1) vengono riportati gli schemi di atti di nomina di:

A. Responsabile del Trattamento;
B. Incaricato del Trattamento;
C. Responsabile della sicurezza informatica, coadiutore del Titolare per le componenti informatiche specialistiche;
D. Schema per l'affidamento a struttura esterna di servizi che comportano il trattamento dei dati.

SEZIONE 3:
ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Questa sezione individua i principali eventi potenzialmente dannosi per la sicurezza dei dati, cerca di valutarne le possibili conseguenze e la gravità e cerca di porli in correlazione con le misure previste.

Di seguito sono sviluppate le misure di sicurezza di cui alle risorse informatiche e basi informative:

1. Basi informative contenute in elaboratori non accessibili da altri elaboratori o terminali (PC stand alone **(tipologia "A")**.

2. Basi informative accessibili dalle reti comunali **(tipologia "B")**.

3. Basi informative su strumenti cartacei **(tipologia C)**

Occorre procedere all'individuazione dei beni da tutelare, al fine dell'adozione delle misure di sicurezza e per disegnare un quadro completo del Sistema Informativo Automatizzato utilizzato.
Risorse individuate da porre sotto tutela:

- Hardware
- Software
- Dati comuni e sensibili
- Risorse professionali
- Documentazione
- Supporti di memorizzazione

A questo proposito si utilizzano le schede di monitoraggio delle risorse e dei beni da tutelare, e le risultanze del censimento delle banche dati che i singoli Responsabili degli Enti hanno predisposto.

Per l'individuazione dei rischi ci si basa sull'individuazione di due aree principali:

- Safety: rischi derivanti da cause naturali o accidentali come incendi, guasti improvvisi e non preventivabili;
- Security: rischi derivanti da illeciti o atti dolosi

I rischi individuati per la tipologia safety sono:

- Incendio;
- Guasti ad apparati hardware;

Per la tipologia security i rischi individuati sono:

- Accessi fisici non autorizzati o intrusioni all'area in cui sono localizzati i Server;
- Intrusioni o attacchi alla rete dell'ente;
- Debolezza nel sistema d'autenticazione degli utenti e mancanza di sicurezza nel sistema d'attribuzioni password;
- Difetti nella gestione dei supporti.

Questa sezione definisce i rischi individuati e le misure di prevenzione/protezione poste in essere al fine di ridurre o eliminare i rischi stessi.

Tipologie di misure di sicurezza adottate:

A) Misure organizzative;
B) Misure fisiche;
C) Misure logiche.

Le misure organizzative attuate sono:

- Gestione delle contromisure di sicurezza logica;
- Gestione della sicurezza rete;
- Controllo dei sistemi di sicurezza;
- Controllo SW e delle operazioni;
- Gestione degli incidenti e del personale;
- Piano di continuità operativo.

Le misure fisiche attuate o da porre in essere sono:

- Protezione perimetrale dei siti;
- Controlli fisici all'accesso;
- Sicurezza delle server farms;

- Protezione fisica dei supporti di backup;
- Protezione da danneggiamenti hardware accidentali o intenzionali;
- Sicurezza degli impianti d'alimentazione e di condizionamento;
- Manutenzione dell'hardware;
- Protezione da manomissioni o furti.

Le misure logiche individuate e attuate o da attuare sono:

- Autenticazione;
- Controllo accessi;
- Integrità;
- Controllo del traffico in rete (saturazione);

Linee guida individuate:

ANALISI DEI RISCHI

I rischi individuati nel sistema informatico dell'Ente, classificato come rete di calcolatori non aperta al Pubblico, sia per l'accesso ai locali, sia per la dislocazione dei Server, sono i seguenti:
Accesso indesiderato da parte di personale non autorizzato, durante l'orario di lavoro poiché, a volte, per esigenze di servizio gli uffici possono rimanere senza presidio;
Intrusione, fuori orario di servizio, da parte di malintenzionati quando l'Ente non è in attività;
Pericolo d'incendio;
Intrusione di pirati informatici e/o personale non autorizzato nella rete informatica;
Attacco alla rete con introduzione dall'esterno o dall'interno di virus informatici;
Perdita parziale o distruzione totale di dati causati da guasti tecnici non prevedibili come nel caso di rottura o malfunzionamenti delle memoria di massa (Hard Disk), guasti ad unità di salvataggio o al loro supporto rimovibile;
Debolezza nell'attribuzione delle password per l'accesso ai database (non crittografate oppure facilmente deducibili).

LINEE GUIDA PER LA SICUREZZA

Attività di prevenzione allo scopo di impedire accadimenti negativi;
Attività di protezione volta alla riduzione della gravità a fronte d'accadimento negativo.

ISTRUZIONI E PROCEDURE

Produzione di documentazione dettagliata volta a standardizzare le procedure d'intervento.

ASSEGNAZIONI INCARICHI

Attribuzione degli incarichi per il corretto adempimento dei compiti specifici in materia di sicurezza.

MANSIONARI

Individuazione delle procedure in uso al fine della produzione dei mansionari;
Definizione del canone atto a costituire l'insieme dei mansionari relativi agli adempimenti e stesura dei mansionari stessi.

CLASSIFICAZIONE DEI DATI

Classificazione dell'insieme delle informazioni contenute nelle banche dati rilevate come bene da tutelare.

FORMAZIONE E INFORMAZIONE

Attuazione di un piano indirizzato all'aggiornamento costante del personale;
Individuazione con conseguente adozione di una procedura standard finalizzata alla divulgazione dell'informazione.

REGISTRAZIONE CONSULTAZIONI

Concretizzazione del principio di registrazione accessi alle banche dati.

DOCUMENTAZIONE DELLE VERIFICHE

Procedura finalizzata alla produzione di documentazione delle verifiche poste in essere in materia di sicurezza.

VERIFICHE INTERNE

Verifiche annuali atte a valutare il livello di protezione che l'insieme delle misure adottate, in materia di sicurezza, garantiscono.

DISTRUZIONE CONTROLLATA SUPPORTI INFORMATICI

Riciclaggio dei supporti magnetici utilizzati per i backup programmati (cassette, tape, Hd rimovibili, ecc.);
Riutilizzo di floppy disk;

CD Rom prodotti per un obiettivo specifico il cui scopo si è esaurito.

SEZIONE 4:
LE MISURE DI SICUREZZA ADOTTATE

TRATTAMENTO DEI DATI PERSONALI EFFETTUATI CON STRUMENTI ELETTRONICI E COMUNQUE AUTOMATIZZATI
(tipologia "B").

Rischio contrastato	Trattamento interessato	Data base interessato	Misura in essere	Periodicità
4.1.1) Accesso indesiderato da parte di personale non autorizzato, durante l'orario di lavoro poiché, a volte, per esigenze di servizio gli uffici possono rimanere senza presidio; 4.1.2) Intrusione, fuori orario di servizio, da parte di malintenzionati quando l'Ente non è in attività;	Verificare i locali in cui sono disposti i server, che devono prevedere porta di accesso dotata di serratura. Verificare la struttura complessiva degli uffici, al fine di prevedere diffusamente inferriate alle finestre del piano terra, porte d'ingresso resistenti	1 – 53	In essere	annuale

Rischio contrastato	Trattamento interessato	Data base interessato	Misura in essere	Periodicità
4.1.3) Pericolo d'incendio nell'area del CED, perché vi sono diversi apparati elettrici d'elevata potenza in esercizio continuo;	Eliminare la presenza di materiale altamente infiammabile (quale carta, mobili in legno,..) nei pressi dei server. Porre, nei luoghi critici, estintori d'adeguata capacità.	1 – 53	In essere	annuale
4.1.4) Intrusione di pirati informatici e/o personale non autorizzato nella rete informatica;	L'unico punto fisico di accesso esterno è attraverso il router che gestisce canale di collegamento alla rete regionale, utilizzata anche per l'uscita su Internet. Tale canale è protetto tramite gli opportuni strumenti hardware e software da parte dell'Ente gestore (Regione Emilia Romagna + Provincia di Forlì - Cesena). L'accesso al ruoter può poi essere utilizzato in dial-up da parte delle aziende che effettuano operazioni di teleassistenza. Tale accesso viene selezionato tramite nome utente / password. E' compito dell'Amministratore di sistema impostare e mantenere nel tempo tali parametri, che vengono variati con cadenza massima semestrale. Le password di amministrazione dei ruoter vengono pure gestite direttamente dall'Amministratore di Sistema e rese note alla sola ditta incaricata della manutenzione e all'ufficio tecnico dell'Ente fornitore dell'accesso alla rete Regionale.	1 – 53	In essere	annuale

Rischio contrastato	Trattamento interessato	Data base interessato	Misura in essere	Periodicità
4.1.5) Attacco alla rete con introduzione dall'esterno o dall'interno di virus informatici;	Per tutelare il S.I. da attacchi di Virus Informatici ci si è dotati di un software di protezione antivirus; tutti i server e le postazioni di lavoro contengono una copia del programma antivirus. Con cadenza periodica viene effettuato l'aggiornamento. Con cadenza almeno semestrale viene verificata l'effettiva capacità di intercettare infezioni.	1-53	In essere	annuale

Rischio contrastato	Trattamento interessato	Data base interessato	Misura in essere	Periodicità
4.1.6) Perdita parziale o distruzione totale di dati causati da guasti tecnici non prevedibili come nel caso di rottura o malfunzionamenti della memoria di massa (Hard Disk), guasti ad unità di salvataggio o al supporto rimovibile;	Le tecniche di sicurezza messe in atto per annullare i rischi di perdita di dati in caso di guasti HW relativamente alle memorie di massa (hard disk e DAT in genere) sono state impostate secondo le seguenti filosofie: - Per i calcolatori server contenenti dati classificati di tipo critico si è scelto di adottare una configurazione di sicurezza di tipo "mirroring". Questa soluzione tecnica assicura la scrittura dei dati su due supporti diversi rendendoli speculari, offrendo così un elevatissimo livello di sicurezza. - Per tutti i server e i calcolatori in genere, contenenti dati, si applica un'ulteriore misura di sicurezza che si concreta in un backup quotidiano con gestione sistematica dei supporti. La procedura si articola secondo le seguenti fasi: - N.1 salvataggio giornaliero (n.4 nastri a rotazione) - N.1 salvataggio settimanale (n.4 nastri a rotazione) - N.1 salvataggio mensile (n.12 nastri a rotazione) - Verifica della leggibilità dei supporti eseguita semestralmente secondo le indicazioni dirette dell'Amministratore di Sistema; - Mensilmente è conservata una copia di ciascun salvataggio in un luogo sicuro ubicato in locale diverso dal quello normalmente in uso;	1 – 53	In essere	annuale

	Dopo due anni sono distrutte le copie di sicurezza relative ai salvataggi mensili;			

LINEE GUIDA PER LA SICUREZZA				
Misura	Descrizione	Data base interessato	Misura in essere	Periodicità
4.2.1) Attività di prevenzione allo scopo di impedire accadimenti negativi; 4.2.2) Attività di protezione volta alla riduzione della gravità a fronte d'accadimento negativo.	Individuata la finalità di prevenire eventi negativi al Sistema Informatico Automatizzato, come realizzazione di ciò, è attivata la verifica semestrale atta ad individuare nuovi eventuali rischi derivanti, sia dall'evoluzione fisiologica dei Sistemi, sia dall'introduzione di nuove tecnologie e/o architetture di telecomunicazione. Allo stesso tempo è fondamentale, nel caso di un accadimento negativo, attivare, a fronte di ciò, una procedura immediata atta ad aumentare il livello di protezione. Il tutto si traduce in un'analisi dettagliata dei nuovi ambienti, nel caso d'evoluzione o modifica del sistema, oppure, alla presenza di fatti negativi, di uno studio minuzioso dell'evento al fine di adottare le protezioni possibili atte a prevenire e/o a ridurre la gravità del danno nel caso in cui si dovesse ripetere.	1-53	In essere	annuale

ISTRUZIONI E PROCEDURE				
Istruzioni e procedure	Descrizione	Data base interessato	Misura in essere	Periodicità
4.3.1) Produzione di documentazione dettagliata volta a standardizzare le procedure d'intervento.	Al fine di adottare procedure standard, per le stesse tipologie d'intervento, si attiva la tecnica della produzione di documentazione. Le documentazioni prodotte dovranno essere suddivise secondo le seguenti macro - aree: - Documentazione relativa all'installazione e configurazione dei Sistemi Operativi residenti su calcolatori (DOC S.O.); - Documentazione relativa agli applicativi in uso riguardante, sia la loro installazione e configurazione utente, sia le procedure individuate atte a risolvere i problemi contingenti che accadono durante l'utilizzo (DOC APPLICATIVI). - Documentazione, con istruzioni specifiche, rivolta alla corretta esecuzione con relativo controllo dei backup di sicurezza dati (DOC BACKUP). - Documentazione delle configurazioni di rete, LAN, WAN e MAN (DOC RETE). - Documentazione relativa alle filosofie di protezione della rete in senso lato (DOC SICUREZZA). S'impone la regola d'obbligatorietà d'aggiornamento documentazione, infatti, ogni qualvolta è apportata una qualunque modifica, di configurazione, procedurale o logica, la documentazione relativa deve essere aggiornata.	1-53	In essere	annuale

ASSEGNAZIONE INCARICHI				
		Data base interessato	Misura in essere	Periodicità
4.4.1) Attribuzione degli incarichi per il corretto adempimento dei compiti specifici in materia di sicurezza.	Per il corretto adempimento di tutti i compiti specifici, descritti in questo documento, sono individuate le figure competenti, per ciascun adempimento. Con determinazione del Responsabile è attribuita la mansione, il calendario e la responsabilità.	1 – 53	In essere	annuale
MANSIONARI				
		Data base interessato	Misura in essere	Periodicità
4.5.1) Individuazione e censimento delle procedure in uso al fine della produzione dei mansionari;	Data la finalità, si esegue una rilevazione di tutti gli adempimenti e delle procedure in uso.	1 – 53	In essere	annuale
4.5.2) Definizione del canone atto a costituire l'insieme dei mansionari relativi agli adempimenti e stesura dei mansionari stessi.	Per ciascun adempimento, in base all'insieme delle regole individuate, sono attribuite individualmente tutte le competenze specifiche.			

CLASSIFICAZIONE DEI DATI				
		Data base interessato	Misura in essere	Periodicità
4.6.1) Classificazione dell'insieme delle informazioni contenute nelle banche dati rilevate come bene da tutelare.	I dati individuati, come risorse dell'Ente, tramite la rilevazione effettuata con la scheda predisposta dal Responsabile, sono valutati e catalogati secondo le seguenti specifiche: - Dati comuni; - Dati individuali; - Dati sensibili.	1 – 53	In essere	annuale

FORMAZIONE E INFORMAZIONE				
		Data base interessato	Misura in essere	Periodicità
4.7.1) Attuazione di un piano indirizzato all'aggiornamento costante del personale; 4.7.2) Individuazione con conseguente adozione di una procedura standard finalizzata alla divulgazione dell'informazione	Data la rilevanza strategica che implica la gestione dei Sistemi Informativi Automatizzati, e vista la rapidità con cui questi si evolvono, si attiva un piano programmato da rivedere e aggiornare almeno una volta ogni anno al fine di mantenere costante il livello di formazione del personale coinvolto nella gestione e mantenimento del sistema informatico aziendale. Ponendo l'accento sul valore e l'importanza dei sistema informatico., si attiva, in linea con gli adempimenti previsti dalla sezione tre del presente documento, la pubblicazione e la messa a disposizione, al personale coinvolto nella gestione, di tutta la documentazione prodotta.	1 – 53	In essere	annuale

REGISTRAZIONE CONSULTAZIONI				
		Data base interessato	Misura in essere	Periodicità
4.8.1) Concretizzazione del principio di registrazione accessi alle banche dati.	In materia d'applicativi strategici, con funzionalità multi-users, indipendentemente dalla tipologia del dato contenuto (comune o sensibile), ci si è dotati esclusivamente di software che contemplasse le funzioni sia di controllo accessi, sia di registrazione dell'operazione effettuata. La verifica avviene a livello d'accesso tramite controllo utente e relativa password. A seguito di riconoscimento avvenuto, il software concede le abilitazioni previste per quel dato ruolo. Per le applicazioni più critiche la funzione di registrazione memorizza, all'interno delle banche dati, in modo permanente, anche le singole operazioni compiute dagli utenti, compresa data e ora.	1-53	In essere	annuale
DOCUMENTAZIONE DELLE VERIFICHE				
4.9.1) Procedura finalizzata alla produzione di documentazione delle verifiche poste in essere in materia di sicurezza.	Data l'obbligatorietà di verifica dei procedimenti posti in essere in materia di sicurezza, si attiva un registro atto a consuntivare la documentazione relativa a ciascuna verifica messa in atto.	1-53	In essere	annuale

VERIFICHE INTERNE				
		Data base interessato	Misura in essere	Periodicità
4.10.1) Verifiche semestrali atte a valutare il livello di protezione che l'insieme delle misure adottate, in materia di sicurezza, garantisce.	Si attiva un sistema interno di verifica che tende a valutare come l'insieme delle misure adottate protegge il Sistema Informativo Automatizzato da tutti quegli accadimenti negativi, sia di Safety, sia di security, che possono verificarsi ai beni e/o alle risorse dell'Ente. Queste verifiche tendono a correggere e a rafforzare, nel tempo, le misure e i provvedimenti individuati e adottati a seguito dell'applicazione della legge.	1-53	In essere	annuale

DISTRUZIONE CONTROLLATA SUPPORTI INFORMATICI				
		Data base interessato	Misura in essere	Periodicità
4.11.1) Riciclaggio dei supporti magnetici utilizzati per i backup programmati (cassette, tape, ecc.).	Formattazione del supporto fino ad un riutilizzo pari al 50% di quanto dichiarato dal costruttore, indi distruzione fisica.	1-53	In essere	annuale
4.11.2) Riutilizzo di floppy disk.	Formattazione del supporto fino ad un utilizzo massimo pari a sette volte, indi distruzione fisica.	1-53	In essere	annuale
4.11.3) CD Rom prodotti per un obiettivo specifico il cui scopo si è esaurito.	Distruzione fisica (rottura).	1-53	In essere	annuale

CASI DI FORNITURA DI SERVIZI DI HOT LINE				
		Data base interessato	Misura in essere	Periodicità
4.12.1) I Servizi di Hot Line	Nei contratti di HOT LINE e Tele assistenza, dovrà essere sempre applicata la seguente clausola: **NORMA DI RISERVATEZZA E SICUREZZA**: Ai fini dell'applicazione del DLGS 196/2003 l'Appaltatore, nell'erogazione del servizio, si impegna a rispettare gli obblighi di riservatezza e sicurezza previsti dalle norme in oggetto. In tale senso si impegna ad attivare tutte le indicazioni che verranno date dal Comune e dall'Amministratore del Sistema.	1-53	In essere	annuale

TRATTAMENTO DEI DATI PERSONALI EFFETTUATI CON STRUMENTI ELETTRONICI E COMUNQUE AUTOMATIZZATI
(tipologia "A").

Rischio contrastato	Trattamento interessato	Data base interessato	Misura in essere	Periodicità
Accesso indesiderato da parte di personale non autorizzato Intrusione da parte di malintenzionati quando l'Ente non è in attività;	Su tutti i Personal Computer va utilizzata l'opzione della PASSWORD DI ACCENSIONE. Per l'esecuzione di tale azione di vedano le ISTRUZIONI per l'impostazione della Password di accensione (allegato 2). Per la continuità operativa i responsabili del trattamento dovranno rispettare i criteri di sicurezza di seguito indicati	1-53	In essere	annuale

Criteri di sicurezza:

La misura di sicurezza si concreta in un backup con gestione sistematica dei supporti.
La procedura si articola secondo le seguenti fasi:

- Copia con cadenza come minimo settimanale dei dati su supporto magnetico estraibile (floppy disk o, in caso di grandi volumi, Compact Disk); eseguita dall'Incaricato del trattamento che utilizza tale Personal Computer ;
- I supporti utilizzati sono conservati in armadi protetti da serratura;
- La copia viene effettuata utilizzando quattro set diversi dei supporti di memorizzazione, con riciclo (un set ogni settimana del mese);
- Sull'etichetta del supporto di memorizzazione va esplicitamente indicato: contenuto, numero della settimana, data del primo utilizzo, data dell'ultimo utilizzo
- Mensilmente è archiviata una ulteriore copia del salvataggio presso il referente informatico locale, in un luogo diverso rispetto a quello in cui è ubicato il PC;
- Lo stesso set di supporto di salvataggio di tipo floppy è utilizzato al massimo per sei mesi; dopodiché occorre procedere con un nuovo set;
- il set di floppy disk giunto al termine dell'utilizzo va consegnato all'Amministratore di Sistema;

Riutilizzo di floppy disk.	Formattazione del supporto fino ad un utilizzo massimo pari a sette volte, indi distruzione fisica.

TRATTAMENTO DEI DATI PERSONALI EFFETTUATI CON STRUMENTI CARTACEI
(Tipologia "C")

Sedi Uffici Contenitori	Chiusura delle porte di accesso alla sede ed agli uffici. Adozione delle misure fisiche sui contenitori (chiavi, ecc.) di sicurezza in rapporto alla capacità economica dell'Ente e tipologia. Adozione di tutte le idonee misure di sicurezza in rapporto alla capacità economica dell'Ente.
Norme comportamentali per il trattamento di materiale cartaceo nell'ambito dei Settori, - per i trattamenti comportanti trasmissioni di documenti con dati personali interno – interno, interno – esterno, o acquisizioni esterno interno; - per la confluenza e la conservazione dei dati trattati in archivi correnti, di deposito, storici, particolari (ad es., depositi carte d'identità).	Mettere a disposizione dei dipendenti il documento programmatico sulla sicurezza affinché ne recepiscano gli orientamenti e adempiano ai relativi compiti. Nel designare gli incaricati del trattamento per iscritto e nell'impartire l'istruzione ai sensi dell'articolo 30 del D.lgs. 196/2003, il titolare o, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati e di seguito indicati: Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agi incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate. Nel caso di trattamenti di dati sensibili, oltre alle linee – guida sopra indicate, devono essere osservate le seguenti modalità: a,. se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura; L'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

SEZIONE 5:
CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

In questa sezione vengono descritti i criteri e le procedure adottate per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità del database.

Salvataggio				
Database	*Dati sensibili contenuti*	*Criteri per il salvataggio*	*Ubicazione di conservazione delle copie*	*Struttura operativa incaricata del salvataggio*
1 – 53	Come descritti nella sezione 1	Dischi mirrorati; salvataggi ogni notte; conservazione supporti settimanali, conservazione copia mensile, distruzione copie dopo due anni.	In luoghi di sicurezza e distanti dai locali in cui sono ubicati i server	Referente del sistema informatico comunale e custode delle password che operera in tale senso come collaboratore del Responsabile dell'Ufficio per la gestione associata delle attività informatiche e statistiche per perseguire le finalità di sicurezza dei dati contenute nelle banche dati comunali.

Ripristino		
Database	*Scheda operativa*	*Pianificazione delle prove di ripristino*
1 – 53	Come descritte nelle procedure di gestione delle singole banche dati	Annuale

SEZIONE 6:
PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

In questa sezione sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

Corso di formazione	*Descrizione sintetica*	*Soggetti interessati*	*Numero di soggetti interessati*	*Numero di soggetti già formati/da formare nell'anno*	*calendario*
Corso di base sugli aspetti della norma, sui comportamenti, sulle responsabilità	Corso di base	Responsabili del trattamento	4	4	Da stabilire
Corso di base sugli aspetti della norma, sui comportamenti, sulle responsabilità	Corso di base	Incaricati del trattamento	15	15	Da stabilire
Corso avanzato	Corso avanzato	Responsabili del trattamento	1	15	Da stabilire
Corso avanzato	Corso avanzato	Incaricati del trattamento	00	00	Da stabilire

SEZIONE 7:
TRATTAMENTI AFFIDATI ALL'ESTERNO

In questa sezione vengono indicati i servizi e le attività affidate all'esterno e che comportano il trattamento dei dati personali.

Le attività affidate all'esterno sono riportate nel prospetto che segue, da cui emerge la descrizione dell'attività e le indicazioni precise del soggetto affidatario del servizio/attività.

Inoltre è previsto che il soggetto cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale e che il soggetto dichiari:

1 Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2 Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3 Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4 Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenza;
5 Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Attività esternalizzata	Descrizione sintetica	Dati personali/ sensibili interessati	Soggetto esterno	Descrizione dei criteri per l'adozione delle misure
Trasporto scolastico	Trasporto scolastico alunni residenti al di fuori dei centri abitati di Galeata	Dati anagrafici utenti del servizio	ATR (Agenzia per la mobilità) via Lombardini, 2 FORLI'	Essendo la banca dati presente presso l'appaltatore, egli si impegna, nell'erogazione del servizio, ad adottare le misure di sicurezza previste dalle norme in oggetto
Servizio assistenza software gestione stipendi	Aggiornamento software, assistenza al servizio personale	Dati anagrafici e stipendiali dipendenti, amministratori, L.S.U., borse lavoro	CEDAF s.r.l. via Meucci, 17 FORLI'	Essendo la banca dati presente presso l'appaltatore, egli si impegna, nell'erogazione del servizio, ad adottare le

				misure di sicurezza previste dalle norme in oggetto
Servizio assistenza software gestione della popolazione	Aggiornamento software, assistenza ai servizi demografici	Dati anagrafici popolazione residente	CEDAF s.r.l. via Meucci, 17 FORLI'	Non essendo la banca dati presente presso l'appaltatore, ma ubicata nei server del comune, le misure di sicurezza sono quelle previste dal presente documento
Servizio di somministrazione acqua e gas	Somministrazione acqua e gas ai cittadini e riscossione relative tariffe	Dati anagrafici utenti dei servizi	HERA Forlì - Cesena s.r.l. via Spinelli, 60 CESENA	Essendo la banca dati presente presso l'appaltatore, egli si impegna, nell'erogazione del servizio, ad adottare le misure di sicurezza previste dalle norme in oggetto
Servizio alloggi		Dati anagrafici utenti dei servizi	ACER Forli'	Essendo la banca dati presente presso l'appaltatore, egli si impegna, nell'erogazione del servizio, ad adottare le misure di sicurezza previste dalle norme in oggetto

Lo schema di determinazione per i singoli Responsabili viene riportato in allegato (Allegato n. 1).

SEZIONE 8:
CIFRATURA DEI DATI IDENTIFICATI

Non vi sono dati per i quali è richiesta la cifratura.

ALLEGATO n. 1

Schemi di atti per affidamento compiti e le responsabilità assegnati/e:

A. ai Responsabili del trattamento, identificati nei termini di legge dal Titolare;
B. agli Incaricati del trattamento, identificati nei termini di legge dai Responsabili del trattamento;
C. alla struttura informatica associata (Ufficio per la gestione associato di Informatica e Statistica);
D. alla struttura (Società/Associazione) affidataria di servizi che comportano il trattamento dei dati.

Schema Responsabili del trattamento, identificati nei termini di legge dal Titolare,

Comune di _____

IL SINDACO

Premesso:

- che DLGS 196/2003 , reca norme per la tutela delle persone ed altri soggetti rispetto al trattamento dei dati;
- che il Consiglio Comunale con deliberazione n. 13 del 21.12.1999 ha approvato il regolamento sulla tutela dei dati personali raccolti nelle banche dati comunali;
- che la Giunta Comunale con deliberazione n. _____ del _____ ha approvato il **PIANO OPERATIVO PER L'ADOZIONE DELLE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI;**

Visto:

- il regolamento suindicato che individua nei responsabili dell'area i Responsabili delle operazioni di trattamento dei dati personali contenuti nelle banche dati comunali;
- il piano operativo per l'adozione delle misure di sicurezza suindicato che prevede che ad una figura tecnica già denominato nel precedente sistema "Amministratore del Sistema" competa il compito di sovrintendere alle risorse del sistema informatico e delle banche dati inserite nel/nei elaboratore server, e che allo stesso vengono riservati i compiti già stabiliti dagli artt. 2 e 4 del DPR 28.7.1999 n. 318, mentre nel caso di

trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori i compiti attribuiti all'Amministratore del sistema spettano ai Responsabili dell'area, del resto responsabili delle operazioni di trattamento dei dati personali, rimanendo in capo all'amministratore del sistema il compito di sovrintendere allo svolgimento di tali attività impartendo le disposizioni necessarie per garantire uniformità di comportamento, tenuto conto delle risorse assegnate;

- il suddetto piano operativo per l'adozione delle misure di sicurezza che individua nel responsabile comunale del sistema informativo ed informatico le funzioni di "Custode delle password", ovvero prevede che nell'esercizio di tale compito essi fungano da supporto locale alla gestione degli strumenti informatici e che in tale ambito provvedano alla manutenzione dell'archivio delle parole chiave;

Visto:

- l'atto sindacale n. ____ del _____ con il quale è stato nominato responsabile del dell'areaamministrativs-affari generali il Sig. _____, ai sensi dell'art. 107, comma 2, del T.U.E.L.
- l'atto sindacale n. ____ del _____ con il quale è stato nominato responsabile del dell'area contabile il Sig. _____, ai sensi dell'art. 107, comma 2, del T.U.E.L.
- l'atto sindacale n. ____ del _____ con il quale è stato nominato responsabile del dell'area tecnica il Sig. _____, ai sensi dell'art. 107, comma 2, del T.U.E.L. tecnica

Considerato:

- che l'attribuzione delle responsabilità sul trattamento dei dati a ciascuno dei soggetti già individuati come responsabili dei settori in cui è attualmente organizzato l'Ente è correlata all'esperienza ed alla qualificazione professionale maturata da ciascuno;

Rilevato:

- che i responsabili del trattamento saranno titolari delle funzioni di cui al DLGS 196/2003, meglio identificate e specificate nel documento che si allega al presente atto sub "A" in ottemperanza all'art. 29 del decreto legislativo innanzi citato;

DECRETA

1. Di nominare, con decorrenza immediata, per le motivazioni indicate in premessa e qui richiamate, responsabili del trattamento dei dati raccolti nelle banche dati comunali o utilizzate nel perseguimento delle funzioni istituzionali:
   - Sig. _____
   - Sig. _____
   - Sig. _____

2. Di nominare, con decorrenza immediata, per le motivazioni indicate in premessa e qui richiamate, "Custode delle password" il sig. _____

3. Di dare atto che i compiti e le funzioni, nel rispetto delle quali sono tenuti ad operare per il trattamento dei dati, sono quelle specificate nel documento allegato sub "A";

Il presente provvedimento è notificato agli interessati nelle forme di legge; viene reso pubblico mediante affissione all'albo pretorio, da effettuarsi entro 5 giorni dalla data di adozione, per la durata di 15 giorni e trasmesso al Segretario Comunale.

Lì _____

IL SINDACO

Allegato: FUNZIONI DEL RESPONSABILE DEL TRATTAMENTO, INDIVIDUATE AI SENSI E PER GLI EFFETTI DEL DLGS 196/2003

Il Responsabile ha il dovere di compiere quanto si renderà necessario ai fini del rispetto e della corretta applicazione del DLGS 196/2003 e può esercitare, in tal senso, autonomi poteri gestionali e di controllo.

Specificatamente il Responsabile è tenuto a:

1. ***In relazione agli incaricati:***
   - Individuare e nominare per iscritto gli incaricati del trattamento, impartendo loro, ancora per iscritto, le idonee istruzioni, anche tenuto conto dei compiti indicati dall'Amministratore del sistema;
   - Vigilare sul rispetto delle istruzioni impartite agli incaricati.

2. ***In relazione al Titolare:***
   - Adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare del trattamento;
   - Vigilare sul rispetto di dette misure di sicurezza da parte dei soggetti nominativamente incaricati;
   - Verificare (semestralmente) lo stato di applicazione del DLGS 196/2003, nonché verificare il buon funzionamento, la corretta applicazione e la conformità alle indicazioni dell'Autorità Garante dei sistemi e delle misure di sicurezza adottate;
   - Comunicare immediatamente al Titolare gli eventuali nuovi trattamenti da intraprendere nel proprio dell'area di competenza, provvedendo alle necessarie formalità di legge.

3. ***In relazione allo sviluppo dell'attività ed all'organizzazione dell'area in cui opera:***

- Predisporre quanto necessario affinchè siano rispettate le disposizioni già previste degli articoli 9 e 10 del DPR 28.7.1999 n. 318 per il trattamento dei dati personali effettuati con strumenti diversi da quelli elettronici od automatizzati o contenuti in banche dati cartacee, in modo particolare:
- Predisporre quanto necessario affinchè i dati vengano conservati chiusi a chiave nei contenitori collocati presso i vari uffici e nei locali adibiti ad archivio; dare disposizioni agli incaricati del trattamento affinchè, se prelevati dagli incaricati debbano essere trattenuti diligentemente, evitando accessi indebiti da parte di estranei non autorizzati o non incaricati del trattamento; dare disposizioni affinchè al termine dell'utilizzo vengano ricollocati nei rispettivi contenitori e/o archivi, ed affinchè gli atti e documenti contenenti dati sensibili utilizzati dagli incaricati (solo ed esclusivamente per compiti d'ufficio) siano conservati in contenitori muniti di serratura;
- Predisporre quanto necessario affinchè i contenitori (armadi, schedari e simili) contenenti dati personali vengano sempre chiusi a chiave dopo l'utilizzo da parte degli incaricati; così pure che ciò avvenga per i locali in cui vengono archiviati dati personali; inoltre deve dare le disposizioni affinchè le chiavi degli armadi, schedari, cassettiere ed archivi siano conservate presso lo stesso Responsabile del trattamento competente oppure in luogo all'interno dell'area conosciuto solamente dagli incaricati interessati e dai rispettivi Responsabili del trattamento; il Responsabile del trattamento potrà designare anche un incaricato per la custodia delle chiavi;
- Predisporre quanto necessario, seguendo le indicazioni dell'Amministratore del sistema, per il corretto trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori (assumendo in tale vesto il ruolo di Amministratore del sistema);
- Predisporre a seguito di ciascuna verifica una relazione scritta in ordine a tutti gli adempimenti eseguiti ai sensi del DLGS 196/2003, alla documentazione raccolta ed archiviata ai sensi della medesima legge, nonché in ordine alle misure di sicurezza. Tale relazione dovrà essere, successivamente, trasmessa al Titolare del trattamento;
- Distruggere i dati personali in caso di cessazione del trattamento degli stessi, provvedendo alle necessarie formalità.
- Verificare la correttezza dei dispositivi antincendio per i locali e/o i siti in cui hanno sede le banche dati contenenti i dati personali e dare pronta comunicazione al Titolare in caso di interventi di adeguamento;
- Verificare la corretta continuità dell'alimentazione elettrica per i locali e/o i siti in cui hanno sede le banche dati contenenti i dati personali e dare pronta comunicazione al Titolare in caso di interventi di adeguamento.

4. ***In relazione ai cittadini:***
   - Predisporre le soluzioni organizzative e procedurali volte a consentire la massima diffusione in relazione all'attività amministrativa, delle informazioni ex art. 13 D.Lgs 196/2003;
   - Evadere tempestivamente tutte le richieste e gli eventuali reclami degli interessati;
   - Operare al fine di facilitare l'interessato nell'esercizio dei diritti ex art. 7 D.Lgs 196/2003.

5. ***In relazione ai rapporti con il Garante e con i soggetti deputati al controllo sull'applicazione del D.Lgs 196/2003:***

- Evadere tempestivamente le richieste di informazioni da parte del Garante e dare immediata esecuzione alle indicazioni che perverranno dalla mesedima Autorità;
- Interagire con i soggetti incaricati di eventuali verifiche, controlli,ispezioni;
- Interagire con l'Amministratore del sistema per la migliore organizzazione della sicurezza informatica.

Schema Incaricati del trattamento, identificati nei termini di legge dai Responsabili del trattamento:

Comune di _____

DETERMINA DEL RESPONSABILE DELL'AREA N. _____ ***DEL*** _____

OGGETTO: INDIVIDUAZIONE DEGLI INCARICATI AL TRATTAMENTO DEI DATI DI CUI AL DLGS 196/2003

IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Premesso:

- che il DLGS 196/2003 e successive modifiche ed integrazioni, reca norme per la tutela delle persone ed altri soggetti rispetto al trattamento dei dati;
- che il Consiglio Comunale con deliberazione n. 00 del 000000 ha approvato il regolamento sulla tutela dei dati personali raccolti nelle banche dati comunali;
- che la Giunta Comunale con deliberazione n. _____ del _____ ha approvato il **PIANO OPERATIVO PER L'ADOZIONE DELLE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI ;**

Visto:

- l'art. 39 del DLGS 196/2003 prevede, in capo al Titolare od ai Responsabili del trattamento, la facoltà di nominare gli incaricati del trattamento dei dati e fornire agli stessi le istruzioni per la corretta elaborazione dei dati personali;

Rilevato:

- che il presente provvedimento non comporta impegni di spesa e non ha, pertanto, rilevanza sotto il profilo contabile;

DETERMINA

1. Di nominare quali incaricati al trattamento dei dati, di cui del DLGS 196/2003, il personale dipendente riportato nell'allegato "A" per la banca dati a fianco di ciascuno indicata;

2. Di stabilire che gli incaricati debbono elaborare i dati personali a cui hanno accesso attenendosi alle indicazioni del Titolare e del Responsabile del trattamento;

3. Di stabilire che gli incaricati debbono attenersi a quanto previsto nell'allegato mansionario contraddistinto come allegato "B";

4. Di dare atto che la presente determinazione non comporta impegno di spesa per l'Ente.

Il presente provvedimento è notificato agli interessati nelle forme di legge; viene reso pubblico mediante affissione all'albo pretorio, da effettuarsi entro 5 giorni dalla data di adozione, per la durata di 15 giorni e trasmesso al Segretario Comunale.

IL RESPONSABILE DEL TRATTAMENTO DEI DATI

Allegato "A" alle determina: Elenco delle banche dati ed archivi cartacei ***Contenenti dati personali soggetti a tutela della riservatezza***

DELL'AREA:

Generalità dell'incaricato	*Numero progressivo della banca dati*	*Denominazione della banca dati*

ALLEGATO "B" ALLE DETERMINA: MANSIONARIO DELL'INCARICATO IN RELAZIONE ALL'APPLICAZIONE DEL DLGS 196/2003.

Al fine di una corretta applicazione del DLGS 196/2003 i soggetti individuati come incaricati dovranno:

1. ***In relazione al trattamento:***

- Trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza, comunque nel rispetto di quanto previsto dall'art. 30 del DLGS 196/2003;
- Effettuare le operazioni di trattamento di dati personali come individuate esclusivamente per lo svolgimento delle proprie mansioni, nell'ambito dello sviluppo delle funzioni e dei compiti dell'Ente, nel rispetto delle norme di legge, di statuto, di regolamento che disciplinano l'attività;
- Comunicare o diffondere i dati personali trattati con esplicita autorizzazione del responsabile e comunque nel rispetto delle leggi e regolamenti.

2. ***In relazione alla gestione delle banche dati:***
   - Accedere unicamente alle banche dati specificamente indicate;
   - Aggiornare periodicamente le informazioni contenute nelle banche dati sulle quali si opera;
   - Evitare di creare banche dati nuove senza espressa autorizzazione del responsabile del trattamento;
   - Evitare di asportare, danneggiare o manipolare supporti informatici o cartacei contenenti dati personali di terzi, con procedure non standardizzate/autorizzate.

3. ***In relazione alle misure di sicurezza:***
   - Mantenere assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle proprie funzioni;
   - Osservare scrupolosamente le misure di sicurezza individuate in relazione alle banche dati dell'area di propria afferenza;
   - Fare attento uso di accesso autorizzato (password personali) alle banche dati e verificare che in propria assenza tali sistemi non siano stati violati e rispettare, per quanto attiene al salvataggio dei dati l'utilizzo di chiavi di accesso, prevenzione dall'intrusione di virus informatici, quanto previsto dal regolamento sull'utilizzo degli strumenti informatici in rapporto alle misure previste nel documento programmatico – piano operativo delle misure di sicurezza dei dati personali comunali;
   - Curare che i dati vengano conservati chiusi a chiave nei contenitori collocati presso i vari uffici e nei locali adibiti ad archivio; se prelevati dagli incaricati dovranno essere trattenuti diligentemente, evitando accessi indebiti da parte di estranei non autorizzati o non incaricati del trattamento; al termine dell'utilizzo dovranno essere ricollocati nei rispettivi contenitori e/o archivi; gli atti e documenti contenenti dati sensibili utilizzati dagli incaricati (solo ed esclusivamente per compiti d'ufficio) debbono essere conservati in contenitori muniti di serratura;
   - Assicurarsi che i contenitori (armadi, schedari e simili) contenenti dati personali vengano sempre chiusi a chiave dopo l'utilizzo; così pure deve avvenire per i locali in cui vengono archiviati dati personali; le chiavi degli armadi, schedari, cassettiere ed archivi sono conservate presso il Responsabile del trattamento competente o in luogo all'interno dell'area conosciuto solamente dagli incaricati interessati e dai rispettivi Responsabili del trattamento;
   - I dati personali debbono essere trattati per il tempo strettamente necessario al trattamento, riposti con cura ed attenzione nel proprio archivio, armadio, cassettiera ed ogni altro sito atto alla conservazione, avendo cura che non vi sia indebito accesso da parte di estranei.

Schema per affidamento alla struttura informatica associata (Ufficio per la gestione associato di Informatica e Statistica):

IL TITOLARE DEL TRATTAMENTO DEI DATI

Premesso:
- che il DLGS 196/2003, reca norme per la tutela delle persone ed altri soggetti rispetto al trattamento dei dati;
- che la Giunta Comunale con deliberazione n. _____ del _____ ha approvato il **PIANO OPERATIVO PER L'ADOZIONE DELLE MISURE DI SICUREZZA;**

Visto:
- il piano operativo per l'adozione delle misure di sicurezza su indicato che prevede che ad una figura tecnica, già definita quale Amministratore del Sistema nel già citato DPR 318/1999, competa il compito di sovrintendere alle risorse del sistema informatico e delle banche dati inserite nel/nei elaboratore server, e che allo stesso, quale coadiutore tecnico del Titolare, competano i compiti stabiliti dagli artt. 2 e 4 dell'ex DPR 28.7.1999 n. 318, mentre nel caso di trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori i compiti spettano ai Responsabili di area, del resto responsabili delle operazioni di trattamento dei dati personali, rimanendo in capo all'Ufficio per la gestione associata delle attività informatiche e statistiche il compito di sovra intendere allo svolgimento di tali attività impartendo le disposizioni necessarie per garantire uniformità di comportamento, tenuto conto delle risorse assegnate;

Considerato che si pone l'esigenza di individuare un soggetto tecnico informatico che:
- Si ponga come Organo Tecnico Specialistico del Titolare e pertanto come caudiutore dello stesso per la gestione informatica delle sicurezze informatiche.
- Sia il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati organizzato in archivi gestiti elettronicamente e di consentirne l'utilizzazione, cioè ha la supervisione effettiva sull'adozione delle misure di sicurezza.
- sia il soggetto che provvede ai compiti stabiliti dagli artt. 2 e 4 dell'ex DPR 28.7.1999 n. 318;
- sia il soggetto che provvedere ai compiti stabiliti dall'art. 6 dell'ex DPR 28.7.1999 n. 318;
- sia il soggetto che propone e formula i piani formativi in attuazione del documento programmatico – piano operativo delle misure di sicurezza per le componenti informatiche;
- sia il soggetto che dà attuazione al documento programmatico – piano operativo delle misure di sicurezza, ne controlla l'attuazione e riferisce al Titolare ed ai Responsabili del trattamento per le componenti informatiche:

Considerato altresì:

- che questo Comune ha dato vita ad una forma associata per la gestione dei Servizi Informatici e Statistici facente capo alla Comunità Montana dell'Appennino Forlivese e che pertanto in tale contesto va ricercato il "soggetto" cui attribuire i compiti e le funzioni sopra descritte;
- che il Responsabile dell'Ufficio per la gestione associata di informatica e statistica formulerà, per le funzioni assegnate, apposito piano operativo, tenuto conto delle funzioni specialistiche informatiche, della periodicità e quotidianità dello svolgimento di alcune attività e della distanza dei Comuni dalla propria sede;
- Che il citato piano comprenderà anche funzioni puntualmente definite per contenuti, tempi e modalità operative *la cui esecuzione, in quanto si è in presenza di una forma associativa, è assegnata a personale dei singoli Comuni*, responsabile del sistema informatico comunale e custode delle password, personale che dovrà essere individuato ed incaricato per tale finalità ed opererà in tale senso come collaboratore del Responsabile dell'Ufficio per la gestione associata delle attività informatiche e statistiche per perseguire le finalità di sicurezza dei dati contenute nelle banche dati comunali;

Considerato infine:

- che allo stesso Responsabile e all'Ufficio per la gestione associata dei servizi informatici e statistici vengono affidate ed elencate, a scopo illustrativo, le funzioni comprese in tale funzione di sicurezza dei dati contenute in banche dati su elaboratori server:

Controllo risorse dei server:

- Check capienza dischi, risorse di sistema (memoria, processi);
- Check dimensionamento spazi DB SQL Server;
- Check applicazioni installate;
- Eliminazione file inutili;

cadenza: almeno trimestrale

Ottimizzazione SQL:

- Check integrità SQL Server;
- Ristrutturazione DB;

cadenza almeno trimestrale

Controllo lettura backup:

(la lettura dei log di backup è effettuata quotidianamente dal referente comunale – custode delle password-limitatamente all'orario di avvio e chiusura backup).

- Controllo che le cassette di backup siano effettivamente leggibili

-
- Controllo che le cassette di backup siano correttamente ruotate una volta raggiunto il numero massimo di riutilizzo e
- Pulizia delle testine DAT, a cura del referente comunale.

Cadenza almeno trimestrale

Controllo Utenti:

Verifica da compiere unitamente all'incaricato comunale – custode delle password -.

- Controllo degli utenti definiti nel sistema e relative autorizzazioni;
- Eliminazione degli utenti e delle configurazioni obsolete;
- Controllo corrette autorizzazioni di accesso al file system;
- Controllo log collegamenti PC Anywhere;
- Controllo utenti Exchange e di posta Internet;

cadenza almeno annuale

Controllo funzionalità antivirus:

- Attivazione antivirus sui server;
- Aggiornamento files antivirus;
- Controllo antivirus sui server;
- Controllo correttezza esecuzione antivirus su client (a campione);

cadenza almeno trimestrale

Inoltre:

- Monitoraggio accesso rete;
- Controllo corretto funzionamento diap-up dei router al fine di controllare che:
- Funzioni correttamente il dial-up ed il dial-out;
- Funzioni correttamente lo sgancio della linea di trasmissione dati;
- Non ci siano tempi di collegamento inconsueti (eccessivi).

cadenza almeno semestrale

DETERMINA

1. Di affidare, per le motivazioni indicate in premessa e qui richiamate, con decorrenza immediata, le funzioni di amministratore di sistema al dirigente della Comunità Montana dell'Appennino Forlivese, quale coadiutore del Titolare del trattamento;
2. Al citato Amministratore del sistema compete il compito di sovrintendere alle risorse del sistema informatico del Comune e delle banche dati inserite nel/nei elaboratore server, e che allo stesso competano i compiti stabilito i dagli artt. 2 e 4 dell'ex DPR 28.7.1999 n. 318, ed inoltre compete allo stesso il compito di sovrintendere allo svolgimento delle attività nel caso di trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori impartendo le disposizioni necessarie ai Responsabili di area, responsabili delle operazioni di trattamento dei dati personali, per garantire uniformità di comportamento, tenuto conto delle risorse assegnate, con i contenuti e le modalità specificate nell'allegato "A".

ALLEGATO "A" ALLE DETERMINA:

Al fine di una corretta applicazione del DLGS 196/2003 il soggetto individuato come amministratore di sistema:

E' il soggetto che si pone come Organo Tecnico Specialistico del Titolare e pertanto come caudiutore dello stesso per la gestione informatica delle sicurezze informatiche.
E' il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati organizzato in archivi gestiti elettronicamente e di consentirne l'utilizzazione, cioè ha la supervisione effettiva sull'adozione delle misure di sicurezza.

6. è il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati organizzato in archivi gestiti elettronicamente e di consentirne l'utilizzazione, cioè ***ha la supervisione effettiva sull'adozione delle misure di sicurezza.***

7. è il soggetto che provvede ai compiti stabiliti dagli artt. 2 e 4 dell'ex DPR 28.7.1999 n. 318;

8. è il soggetto che provvedere ai compiti stabiliti dall'art. 6 dell'ex DPR 28.7.1999 n. 318;

9. è il soggetto che propone e formula i piani formativi in attuazione del documento programmatico – piano operativo delle misure di sicurezza per le componenti informatiche;

10. è il soggetto che dà attuazione al documento programmatico – piano operativo delle misure di sicurezza; controlla l'attuazione e riferisce al Titolare ed ai Responsabili del trattamento per le componenti informatiche.

Il Responsabile dell'Ufficio per la gestione associata di informatica e statistica formulerà, per le funzioni assegnate, apposito piano operativo, tenuto conto delle funzioni specialistiche informatiche, della periodicità e quotidianità dello svolgimento di alcune attività e della distanza dei Comuni dalla propria sede.

Il citato piano comprenderà anche funzioni puntualmente definite per contenuti, tempi e modalità operative *la cui esecuzione, in quanto si è in presenza di una forma associativa, è assegnata a personale dei singoli Comuni*, responsabile comunale del sistema informativo ed informatico e custode delle password, personale che dovrà essere individuato ed incaricato per tale finalità; ed opererà in tale senso come collaboratore del Responsabile dell'Ufficio per la gestione associata delle attività informatiche e statistiche, per perseguire le finalità di sicurezza dei dati contenute nelle banche dati comunali.

Vengono di seguito elencate, a scopo illustrativo, le funzioni comprese in tale funzione di sicurezza dei dati contenuti in banche dati su elaboratori server:

COMPITI A TUTELA DELL'INTEGRITA' DEL SISTEMA AFFIDATI A STRUTTURA SPECIALISTICA

Controllo risorse dei server:
- Check capienza dischi, risorse di sistema (memoria, processi);
- Check dimensionamento spazi DB SQL Server;
- Check applicazioni installate;
- Eliminazione file inutili;

cadenza: almeno trimestrale

Ottimizzazione SQL:
- Check integrità SQL Server;
- Ristrutturazione DB;

cadenza almeno trimestrale

Controllo lettura backup:

(la lettura dei log di backup è effettuata quotidianamente del responsabile comunale del sistema informativo ed informatico – custode delle password).

- Controllo che le cassette di backup siano effettivamente leggibili;
- Controllo che le cassette di backup siano correttamente ruotate una volta raggiunto il numero massimo di riutilizzo;
- Pulizia delle testine DAT.

Cadenza almeno trimestrale

Controllo Utenti:

Verifica da compiere unitamente al responsabile comunale del sistema informativo ed informatico

- Controllo degli utenti definiti nel sistema e relative autorizzazioni;
- Eliminazione degli utenti e delle configurazioni obsolete;
- Controllo corrette autorizzazioni di accesso al file system;
- Controllo log collegamenti PC Anywhere;
- Controllo utenti Exchange e di posta Internet;

cadenza almeno annuale

Controllo funzionalità antivirus:

- Attivazione antivirus sui server;
- Aggiornamento files antivirus;
- Controllo antivirus sui server;
- Controllo correttezza esecuzione antivirus su client (a campione);

cadenza almeno trimestrale

Inoltre:

- Monitoraggio accesso rete;
- Controllo corretto funzionamento diap-up dei router al fine di controllare che:
- Funzioni correttamente il dial-up ed il dial-out;
- Funzioni correttamente lo sgancio della linea di trasmissione dati;
- Non ci siano tempi di collegamento inconsueti (eccessivi).

cadenza almeno semestrale

Schema per l'affidamento a struttura esterna (Società/Associazione) di servizi che comportano il trattamento dei dati

Comune di _____

Determina del responsabile del trattamento dei dati personali n. _____ del _____

Oggetto: ***Individuazione dell'incaricato esterno al trattamento dei dati di cui alla DLGS 196/2003***

IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Premesso che il servizio _____;

Visto il Decreto Legislativo n. 196 del 30.6.2003 Codice in materia di protezione dei dati personali;

Visto il provvedimento sindacale n. _____ del _____ di individuazione delle banche dati comunali;

Visto il provvedimento n. _____ del _____ di nomina dei Responsabili dei trattamenti dei dati personali contenuti nelle banche dati comunali;

Visto l'art. 5, comma 2) del regolamento per la tutela dei dati personali contenuti nelle banche dati comunali che prevede, in capo ai Responsabili del trattamento, la facoltà di nominare gli incaricati del trattamento dei dati e fornire agli stessi istruzioni per la corretta elaborazione dei dati personali;

Rilevato che il presente provvedimento non comporta impegni di spesa e non ha, pertanto, rilevanza sotto il profilo contabile;

DETERMINA

1. Di nominare, quale incaricato al trattamento dei dati di cui al decreto legislativo 196/2003, il personale di _____ preposto al servizio di _____ ; in particolare assumono la qualifica di incaricati i dipendenti o soci designati a tal fine dal legale rappresentante. In mancanza si intende incaricato lo stesso legale rappresentante.

2. Di stabilire che l/gli incaricato/i debbano elaborare i dati personali a cui hanno accesso attenendosi alle indicazioni del titolare e del sottoscritto Responsabile, in modo particolare gli stessi non potranno effettuare le prestazioni se non previa richiesta del citato Responsabile del trattamento ed alle condizioni dallo stesso indicate;

3. Di stabilire che l/gli incaricato/i debbano attenersi a quanto previsto nell'allegato mansionario riportato nell'allegato "B";

4. Di dare atto che, come stabilito dal documento programmatico della sicurezza di cui alla deliberazione della Giunta Comunale n. ___ del _____ che il personale di _____ preposto al servizio di _____:
   - è consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
   - assume l'impegno di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
   - assume l'impegno di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
   - assume l'impegno a relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenza;
   - assume l'impegno di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

5. Di dare atto che la presente determinazione non comporta impegni di spesa per l'Ente.

_____

ACCETTAZIONE

La Società/Associazione _____ nella persona del Sig. _____ incaricato dal legale rappresentante pro tempore _____, del trattamento dei dati informatici in oggetto, con la presente consapevole dei requisiti, degli obblighi e delle responsabilità che la legge prevede per l'**Incaricato del trattamento**, dichiara di obbligarsi a procedere al trattamento attenendosi al pieno rispetto della vigente normativa e delle specifiche impartite dal Responsabile delle istruzioni qui riportate.

Data,

_____

_____

Allegato "A" alla determina: ELENCO DELLE BANCHE DATI CONTENENTI DATI PERSONALI SOGGETTI A TUTELA DELLA RISERVATEZZA.

AREA _____

INCARICATO DALLA DITTA	*n.ro progressivo della banca dati*	***DENOMINAZIONE***

Firma dell'incaricato della ditta _____

Allegato "B" alla determina MANSIONARIO DELL'INCARICATO, IN RELAZIONE ALL'APPLICAZIONE DEL DLGS 196/2003.

Al fine della corretta applicazione del D.Lgs 196/2003 i soggetti individuati come incaricati dovranno:

1. *IN RELAZIONE AL TRATTAMENTO:*

- Trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza, comunque nel rispetto di quanto previsto dall'art. 30 del DLGS 196/2003;
- Effettuare le operazioni di trattamento di dati personali come individuate esclusivamente per lo svolgimento delle proprie mansioni, nell'ambito dello sviluppo delle funzioni e dei compiti dell'Ente, nel rispetto delle norme di legge, di statuto, di regolamento che disciplinano l'attività;
- Non comunicare ad alcuno i dati personali trattati.
- Ed inoltre:
  - sono consapevoli che i dati che tratteranno nell'espletamento dell'incarico ricevuto sono dati personali e come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
  - assumono l'impegno di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
  - assumono l'impegno di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;

- assumono l'impegno a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenza;
- assumono l'impegno di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

2. *IN RELAZIONE ALLA GESTIONE DELLE BANCHE DATI:*
   - Accedere unicamente alle banche dati di seguito indicate, attenendosi alle indicazioni del Titolare e del Responsabile, in modo particolare non potranno essere effettuate le prestazioni se non previa richiesta del citato Responsabile del trattamento ed alle condizioni dallo stesso indicate;

n.ro progressivo della banca dati	***DENOMINAZIONE***

3. *IN RELAZIONE ALLE MISURE DI SICUREZZA:*
   - Mantenere un assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle su indicate funzioni;
   - Osservare scrupolosamente le misure di sicurezza individuate in relazione alle banche dati indicate;
   - Fare attento uso dei sistemi di accesso autorizzato alle banche dati.

Firma dell'Incaricato ditta _____

Allegato n. 2

REGOLAMENTO SUI MECCANISMI DI AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI IN RAPPORTO ALLE NORME RELATIVE ALLA PRIVACY.

Introduzione relativa ai meccanismi di autenticazione e controllo degli accessi. Descrizione generale.

In generale sono identificabili 5 diversi meccanismi o livelli di protezione e controllo degli accessi sugli elaboratori aziendali:

(A) password di accensione computer
(B) utente/password di accesso a Windows
(C) utente/password di accesso alla rete aziendale
(D) utente/password di accesso alle applicazioni
(E) password di blocco Screen Saver

(A) – password di accensione computer

E' la password che, se configurata, viene richiesta immediatamente all'accensione della macchina, e, se non fornita corretta, ne impedisce la partenza.
La richiesta è evidenziata mediante la figurina di una chiave. Se non fornita corretta per tre volte il sistema si blocca e occorre spegnere e riaccendere il sistema.
L'eventuale sblocco, ignorando la parola riservata, è possibile solo a seguito di una non banale operazione che comporta lo smontaggio dell'elaboratore.
Per inserire e modificare tale password occorre entrare nell'ambiente di Setup del Personal Computer, premendo il tasto F10 (o il tasto Canc) subito dopo l'accensione. Occorre fare estrema attenzione onde non modificare altri parametri di configurazione del sistema che potrebbero inficiarne il corretto funzionamento.

L'utilizzo di questa modalità' di protezione è:
- obbligatorio nel caso di elaboratori destinati ad ospitare "dati sensibili"
- negli altri casi attivabile se ritenuto opportuno dall'interessato; si raccomanda comunque di ricorrere a tale protezione solo per gravi motivi.

(B) - utente/password di accesso a Windows
Si tratta della mascherina che compare dopo l'accensione, una volta avvenuta l'esecuzione delle procedure di caricamento del sistema operativo. (a seconda dei computer dai 15 ai 40/50 secondi dalla pressione dell'interruttore di accensione).

Il nome utente segue lo standard aziendale: riferendosi all'utilizzatore, è composta dai primi tre caratteri del cognome e dai primi due del nome (es: Ugo Mazzetti -> "mazug"), e può indifferentemente essere scritto maiuscolo o minuscolo.

La password, che può essere lasciata vuota, viene impostata la prima volta che l'utente ha utilizzato il computer, e può successivamente essere modificata seguendo le istruzioni successive.

Sullo stesso computer possono comunque operare diversi utenti. Questi utenti condividono comunque le risorse del computer e non è attivo alcun meccanismo di protezione dei dati in esso contenuti. Un nuovo utente può infatti essere definito da chiunque accenda la macchina, cambiando la sigla nella casella "Nome utente". Allora a cosa serve ? A queste due cose:
- ottenere impostazioni diverse del desktop a seconda dell'utente che si e' connesso
- impostare gli accessi agli elaboratori in rete.

Fondamentale e' questo secondo aspetto.
I diritti di accesso agli elaboratori server, e quindi alle applicazioni e data-base aziendali, sono infatti determinati dall'utente che si connette.

In pratica:
Un addetto, anche lavorando sul computer di un collega, può presentarsi con il proprio nome utente e password e:
- avrà completo accesso alle risorse locali del computer (disco C:).
- avrà accesso alle risorse di rete sulla base del propri diritti, e non di quelli del normale utilizzatore di tale computer

In questo senso, in termini di sicurezza, è più protetta una informazione gestita sulle aree apposite dei server aziendali piuttosto che su quelle locali del PC.

(C) - utente/password di accesso alla rete aziendale
Si può confondere con (B).
In realtà l'utente Windows "pippo", cha ha la passoword "XXXXX", può accedere al server NT1 con nome utente "pluto", password "yyyyyy", e al Server NT2 con nome utente "paperino" e password "qqqqq".

Per non generare confusione si è scelto di identificare in generale il nome utente Windows (e relativa password) con quello di accesso ai Server.

Per la gestione e modifica delle password (B) e (C) va utilizzato la apposita funzione di Windows: Menu' Avvio, Impostazioni, Pannello di Controllo, Password.

(D) - utente/password di accesso alle applicazioni
Diverse applicazioni software aziendali richiedono, al momento della partenza, di qualificarsi con nome utente e password (in alcuni casi con la sola password).
Questa ulteriore autenticazione permette un livello di sicurezza aggiuntivo.

L'aspetto della maschera di richiesta varia a seconda della applicazione. Compare in generale la richiesta del nome utente e della relativa password.
Il nome utente va impostato anche in questo caso secondo lo standard aziendale dei tre caratteri del cognome più due del nome.
La password può' in generale essere scelta e modificata nel tempo dal singolo addetto. Non e' necessario che coincida con quelle precedenti (accesso al computer, accesso alla rete).
In generale l'applicazione permette poi, tramite una funzione utente, la modifica della propria password.

Anche le applicazioni di Office Automation Word e Excel permettono l'impostazione di password su di un documento al fine di inibirne l'apertura ad utenti non autorizzati.

(E) password di blocco Screen Saver
Attivando lo screen saver di Windows e' possibile associare una password che ne impedisce lo sblocco. La funzione è quella di impedire l'utilizzo del computer già acceso qualora l'addetto si sia assentato temporaneamente.
Il computer continua a funzionare ma lo schermo non è sbloccabile, e quindi non è accessibile alcun dato, fin quando non viene impostata tale password.

(A) - PASSWORD DI ACCENSIONE

Caso di elaboratore con trattamento di "dati sensibili"
1. E' obbligatoria l'impostazione della password di accensione del computer.

2. La password può essere comunicata solo ad altri "incaricati del trattamento" che dovessero utilizzare lo stesso elaboratore, o, in assenza, al proprio responsabile di servizio.
3. L'elaboratore non può in alcun caso essere usato da altre persone che non siano anch'esse incaricate del trattamento.
4. Foglio contenente la password in busta chiusa e sigillata va consegnato al responsabile del sistema informativo ed informatico dell'Ente, che ne cura la conservazione e l'eventuale utilizzo nei soli casi di emergenza.
5. Ogni 6 mesi la password va modificata
6. L'amministratore di sistema controlla il rispetto di tali scadenze.

Altri casi

7. L'impostazione della password di accensione va adottata solo per giustificati motivi di protezione e riservatezza dei dati conservati nel disco dell'elaboratore, o qualora questi si trovi localizzato in ambienti aperti al pubblico e non presidiati.
8. La password deve comunque essere comunicata al proprio responsabile di servizio.
9. Foglio contenente la password in busta chiusa e sigillata va consegnato al responsabile del sistema informatico comunale, che ne cura la conservazione e l'eventuale utilizzo nei soli casi di emergenza.

(B)/(C) – PASSWORD DI ACCESSO A WINDOWS e alla RETE AZIENDALE

10. Va sempre utilizzato il nome utente standard, composto dai primi tre caratteri del cognome più i primi due del nome. Eventuale eccezioni per omonimia saranno risolte secondo l'indicazione del responsabile del sistema informatico dell'Ente.
11. **E' obbligatoria l'impostazione della password per tutti gli utenti che hanno accesso a dati sensibili memorizzati su elaboratori collegati in rete.**
12. Negli altri casi l'impostazione della password è facoltativa, e va valutata caso per caso sulla base della criticità delle informazioni a cui si ha accesso.
13. Se impostata la password va comunicata al proprio responsabile superiore.
14. L'Amministratore di sistema, coadiuvato dal "Custode delle Password", cura l'amministrazione del catalogo utenti e password, provvedendo a disattivare gli utenti non più operativi per un periodo superiore a 6 mesi.
15. L'Amministratore di sistema provvede all'abilitazione all'accesso ai dati sensibili solo previa identificazione nominativa da parte del responsabile del trattamento o titolare. Tale identificazione va in ogni caso ripetuta annualmente

(D) – PASSWORD DI ACCESSO APPLICAZIONI

16. Va sempre utilizzato il nome utente standard, composto dai primi tre caratteri del cognome più i primi due del nome. Eventuale eccezioni per omonimia saranno risolte secondo l'indicazione dell'Amministratore di sistema.
17. **E' obbligatoria l'impostazione della password per tutti le applicazioni che trattano dati sensibili o dati personali.**
18. E' obbligatoria la modifica della password ogni sei mesi per tutte le applicazioni che trattano dati sensibili.
19. L'Amministratore di sistema controlla il rispetto di tali scadenze.
20. I documenti Office (fogli Excel o testi Word), contenenti dati sensibili o dati personali di evidente criticità vanno protetti associandovi idonea password.

(E)– PASSWORD DELLO SCREEN-SAVER

21. E' obbligatoria l'impostazione della screen saver e della relativa password su tutti i PC in qui sono trattati dati sensibili.

ALTRE NORME GENERALI

22. Le password devono essere lunghe almeno 8 caratteri. Non vanno trascritte su foglietti o post-it facilmente reperibili.
23. L'attivazione di qualsiasi sistema informatico – elettronico che preveda l'accesso via linea telefonica dall'esterno va esplicitamente autorizzato dall'Amministratore di sistema, verificandone le caratteristiche in termini di protezione da collegamenti inattesi.
24. E' vietato modificare la configurazione di sistema delle applicazioni di accesso Internet Microsoft Explorer (browser), Microsoft Outlook Express (posta elettronica), così come installare nuove applicazioni o versioni diverse rispetto allo standard aziendale. Qualsiasi esigenza che comporti modifiche alla configurazione standard va espressamente approvata dall'Amministratore di sistema.
25. Ogni utilizzatore di Personal Computer è tenuto a seguire quanto predisposto per la protezione dai virus, senza modificare le configurazioni di esecuzione automatica e delle procedure centralizzate di accesso alla rete.
26. E' assolutamente vietato leggere con il proprio personal computer Floppy Disk o Compact Disk di provenienza esterna (trovati su riviste, ceduti da conoscenti, ecc..), senza un controllo preventivo da parte del responsabile comunale del sistema informatico.
27. E' assolutamente vietato aprire allegati di tipo "eseguibile" (con suffisso EXE o COM) pervenuti con messaggi di posta elettronica, senza preventiva autorizzazione da parte di un addetto del servizio informatico.
28. I dispositivi di memorizzazione (quali floppy) utilizzati per memorizzare dati sensibili e che venissero riutilizzati per altri scopi, vanno preventivamente riformattati.

INTERVENTI MANUTENTIVI SU APPARECCHIATURE INFORMATICHE

29. La procedura generale per gli interventi manutentivi, anche da parte di ditte esterne, preveda l'esecuzione on-site (presso di noi), senza prelievo della apparecchiatura e trattamento presso laboratorio del fornitore.
30. Qualora risulti necessaria la riparazione presso il laboratorio fornitore, ed il PC contenga sul disco locale dei "dati sensibili", deve essere fatta firmare una notifica all'addetto del fornitore che effettua il prelievo dell'apparecchiatura, riportante l'ingiunzione alla riservatezza sulle informazioni di cui dovessero venire a conoscenza.

Il presente verbale viene letto, approvato e sottoscritto.

IL PRESIDENTE — **IL SEGRETARIO COMUNALE**

f.to Valentini Rodolfo — f.to Dott.ssa Roberta Fiorini

CERTIFICATO DI PUBBLICAZIONE

La presente deliberazione viene pubblicata mediante affissione all'Albo Pretorio del comune in data odierna per rimanervi per quindici giorni consecutivi.

Lì, 14 GEN. 2006

IL RESPONSABILE
f.to (Sergio Scali)

☒ La presente deliberazione viene trasmessa in elenco ai capigruppo consiliari e messa a disposizione dei consiglieri, ai sensi dell'art.125 Testo Unico Enti Locali (D. Lgs n.267/2000).

☐ La presente deliberazione viene trasmessa al Prefetto, ai sensi dell'art.135, comma 2 del Testo Unico Enti Locali (D. Lgs. n.267/2000).

Lì, 14 GEN. 2006

IL RESPONSABILE
f.to (Sergio Scali)

La presente è copia conforme all'originale, per uso amministrativo.

Lì, 14 GEN. 2006

IL RESPONSABILE
(Sergio Scali)

La suestesa deliberazione:

☒ È divenuta esecutiva il 15 GEN 2006 ...ai sensi dell'art.134 comma 3, Testo Unico Enti Locali (D.Lgs. n.267/2000).

☒ E' stata dichiarata immediatamente eseguibile ai sensi dell'art.134, comma 4^ Testo Unico Enti Locali (D.Lgs. n.267/2000).

Lì, 15 GEN. 2006

IL SEGRETARIO COMUNALE
(Dott.ssa Roberta Fiorini)