COMUNE DI CECIMA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

Adottato ai sensi
dell'art. 34 comma 1 lett. g)
e punto 19 del Disciplinare Tecnico Allegato B)
Decreto Legislativo 30 giugno 2003 n. 196

GENERALITA'

SCOPO E AMBITO DI APPLICAZIONI DEL DPSS

Il presente Documento Programmatico Sulla Sicurezza (definito anche DPSS) è adottato, ai sensi delle disposizioni di cui all'Art.34 del Decreto Legislativo n.196 del 30 giugno 2003 e relativo allegato B, per definire le politiche di sicurezza in materia di trattamento di dati personali nonché i criteri tecnico-organizzativi per la loro attuazione. Il documento, inoltre, fornisce idonee informazioni relative alla tipologia di dati sensibili trattati e all'analisi dei rischi connessi all'utilizzo degli strumenti mediante i quali viene effettuato il trattamento.
Gli allegati al presente documento costituiscono parte integrante del Documento Programmatico Sulla Sicurezza dei dati.
Nel presente documento e nei relativi allegati i termini Trattamento, Dato personale, Dati identificativi, Dati sensibili, Dati giudiziari, Titolare, Responsabile, Incaricato, Interessato, Diffusione, Banca dati e tutti gli altri termini sono usati in conformità alle definizioni elencate all'art. 4 del Decreto Legislativo n. 196 del 30 giugno 2003.

In dettaglio il Documento Programmatico Sulla Sicurezza fornisce informazioni relative a:

a) l'elenco dei trattamenti di dati personali;
b) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
c) l'analisi dei rischi che incombono sui dati;
d) le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché le procedure da seguire per controllare l'accesso ai locali nei quali vengono conservati i dati oggetto del trattamento o l'accesso per via telematica;
e) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento garantendone la disponibilità in tempi certi compatibili con i diritti degli interessati;
f) la predisposizione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire i danni, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare o sull'introduzione di nuovi strumenti utilizzati per il trattamento dei dati personali;
g) la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
h) per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato (per gli organismi sanitari e gli esercenti le professioni sanitarie).

Il Documento Programmatico Sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati nominati con apposite lettere di incarico allegate al presente documento.

Il presente documento è valido per un anno. Trascorso tale termine, e non oltre il 31 marzo di ogni anno, sarà oggetto di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o in generale a un mutato assetto organizzativo.

ELENCO DEI TRATTAMENTI DI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare l'elenco dei trattamenti effettuati sui dati.

ELENCO CARICHE

Titolare del trattamento
Ai sensi dell'art. 4, comma 1, lettera f), del D.Lgs. 196/03 il titolare è la pubblica amministrazione cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Titolare del Trattamento è l'Amministrazione comunale, in persona del **Sindaco pro tempore**, ai sensi dell'art. 50 comma 2 del D.Lgs. 18 agosto 2000 n. 267 (T.U.E.L.)
L'amministrazione comunale ha previsto la nomina e la presenza effettiva del "*Responsabile del Trattamento per la sicurezza dei dati*" con l'attribuzione allo stesso di tutti compiti, oneri e responsabilità inerenti il corretto adempimento delle prescrizione contenute nella normativa in materia di tutela dei dati personali.

Responsabile del trattamento
Ai sensi dell'art.4, comma 1, lettera f) del D.lgs 196/2003, il Titolare del Trattamento può nominare uno o più Responsabili del trattamento con apposita lettera di incarico. La nomina avviene per iscritto.
I Responsabili devono essere individuati fra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, con particolare riguardo alla sicurezza dei dati.
I Responsabili, pertanto, dovranno adottare tutte le misure idonee ad assicurare l'integrità dei dati oggetto del trattamento, a ridurre i rischi di diffusione o trattamento di dati non consentiti e mantenere in piena efficienza tutti gli strumenti e la struttura organizzativa al fine di perseguire gli scopi dettati dal presente DPSS.
Per esigenze organizzative il Titolare può suddividere i compiti fra i diversi Responsabili del trattamento nominati.

I Responsabili del trattamento hanno il dovere di informare tempestivamente il Titolare di eventuali incidenti o della sopravvenuta mancanza dei requisiti minimi di sicurezza richiesti.
Ai Responsabili è conferita possibilità di nominare uno o più Incaricati al trattamento e istruirli adeguatamente per renderli idonei a svolgere le mansioni assegnate.
Se non diversamente previsto nella lettera di incarico, la nomina dei Responsabili si intende a tempo indeterminato e decade o per dimissioni o per revoca comunicata per iscritto o con idonei mezzi informatici dal Titolare del trattamento.

In considerazione delle dimensioni dell'ente locale, essi sono individuati nelle seguenti persone:

Cognome e Nome	Ufficio / Ente esterno	Banche dati
Mogni Claudia	Comune di Cecima	1, 2, 5, 8
Rossi Dott. Mariuccio	Comune di Cecima	3, 4, 7
Campetti Geom. Massimo	Comune di Cecima	6

Incaricati del trattamento
Ai sensi dell'art.4, comma 1, lettera h), del D.Lgs. 196/03 gli incaricati del trattamento sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile con apposita comunicazione scritta. Sempre per iscritto devono essere specificati i compiti loro assegnati.
La lettera di incarico deve essere sottoscritta dal soggetto interessato e sarà cura del Responsabile della conservazione.
Loro compito è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente Documento Programmatico Sulla Sicurezza.
In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti minimi di sicurezza, gli Incaricati dovranno comunicare tempestivamente tale circostanza al Responsabile del trattamento o, in mancanza, al Titolare.
Se non diversamente previsto nella lettera di incarico, gli Incaricati del trattamento vengono nominati a tempo indeterminato e decadono per dimissioni o per revoca.

Nomina dell'Amministratore di sistema
Il Responsabile del trattamento o il Titolare conferiscono a uno o più incaricati le mansioni di gestione delle soluzioni informatiche sia hardware che software adottate per la gestione e la tenuta in sicurezza delle banche dati.
E' compito dell'"Amministratore di Sistema":

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup;
- assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- fare in modo che sia prevista la disattivazione dei *"Codici identificativi personali"* (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei *"Codici identificativi personali"* (USER-ID) per oltre 6 mesi;
- proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

Considerate le dimensioni dell'ente locale nonché il numero di elaboratori connessi in rete, l'amministrazione ha ritenuto opportuno individuare detta figura nella persona di seguito indicata, la quale dimostra le necessarie cognizioni e competenze anche tecniche.

Cognome e Nome	Ufficio / Ente esterno
Chiapparoli Bruno	Comune di Cecima

Nomina del custode delle credenziali di autenticazione
Il Responsabile, di concerto con il Titolare, nomina custode delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati.
E' compito del *"Custode delle Password"* gestire e custodire le *"Password"* per l'accesso ai dati da parte degli incaricati.

L'amministrazione comunale lo ha individuato nella persona di:

Cognome e Nome	Ufficio / Ente esterno
Chiapparoli Bruno	Comune di Cecima

Il Custode delle Password deve predisporre, per ogni Incaricato del trattamento, una busta sulla quale sia indicato lo *"USER-ID"* da questi utilizzato: all'interno della busta deve essere collocata la *"Password"* usata per accedere alla Banca Dati, fornita in forma non leggibile dall'Incaricato del Trattamento.
Le buste con le Password debbono essere conservate in luogo chiuso e protetto, non accessibile da altri all'infuori del custode.
Il Custode delle Password deve revocare tutte le password non utilizzate per un periodo superiore a 6 (sei) mesi.

Ogni password deve essere variata periodicamente, con cadenza almeno semestrale per dati personali e con cadenza almeno trimestrale per dati sensibili o giudiziari. Ogni variazione di password deve constare per atto iscritto, con l'indicazione delle ragioni che ne hanno determinato l'esigenza. Il custode conserva apposito **Registro indicante Incaricato del trattamento e data di variazione della password.**

ANALISI DEI RISCHI

L'analisi dei rischi ai quali sono soggetti i dati trattati vengono dettagliati nel presente DPSS**.** Verrà compilata un'apposita lista dei rischi incombenti sui dati derivanti dal sistema di elaborazione, dal Sistema operativo e dagli Applicativi. Nello stesso documento verranno proposte le azioni correttive o preventive.
L'analisi dei rischi è redatta in relazione al progresso tecnologico, alla sostituzione, integrazione e sostituzione di hardware, agli aggiornamenti o alla sostituzione di sistemi operativi e\o programmi applicativi.

MISURE DI SICUREZZA E CONTROLLO ACCESSO AI LOCALI

In ottemperanza agli artt.31, 32, 33, 34, 35 e 36 del D.Lgs 30/06/2003 n. 196, il presente DPSS prevede l'organizzazione di idonee misure di sicurezza da adottare volte a garantire la sicurezza dei dati.
La sicurezza dei dati si esplica nella loro diligente custodia al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.
Il Responsabile del trattamento approntera tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico.
Sono previste specifiche misure di sicurezza sia per quanto riguarda la custodia di archivi elettronici e non, che l'accesso ai locali ove i dati oggetto del trattamento fisicamente sono conservati.

La procedura di preservazione dal rischio di perdita dei dati trattati con mezzi informatici o dalla divulgazione non autorizzata si esplica nella previsione di un piano basato su:

Copie periodiche di Backup.
Tale procedura, che il Responsabile del trattamento stilerà di concerto con l'amministratore di sistema, dovrà fornire le istruzioni e le modalità in merito al tipo di supporto utilizzato, all'impiego di specifici software per salvataggi automatizzati, alla nomina degli Incaricati del trattamento che eseguiranno le copie di Backup, alla custodia dei supporti nei quali sono stati memorizzati i dati, alla distruzione dei supporti dopo un certo lasso di tempo o comunque alla cancellazione dei dati dai supporti di Backup in maniera tale da impedire ogni possibile consultazione. La procedura di salvataggio prevede anche il monitoraggio di tutte le operazioni affinché il Responsabile possa individuare periodicamente circostanze che impongano l'adozione di un diverso piano di Backup o il suo aggiornamento.
Il salvataggio dei dati dovrà avvenire con cadenza almeno settimanale.
.
Protezione da virus informatici o intrusioni non autorizzate nella propria rete informatica.
Il Responsabile del trattamento incarica l'amministratore del sistema ad approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da Virus informatici o da intrusioni non autorizzate nel sistema.
L'amministratore provvederà a dettagliare tutte le misure adottate compresi l'utilizzo di appositi programmi Antivirus, Firewall e qualsiasi ulteriore soluzione informatica che ritenesse opportuna per diminuire la vulnerabilità del sistema.
E' anche compito dell'amministratore pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione delle case produttrici di software per correggere i difetti dei programmi o dei sistemi operativi utilizzati.
L'amministratore può prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal D. Lgs 30/06/2003 n. 196.
Tutte le misure di sicurezza previste dall'amministratore di sistema dovranno essere periodicamente valutate per adattare la procedura all'evoluzione tecnologica.
In caso di infezione del sistema da parte di Virus informatici, l'amministratore del sistema dovrà tempestivamente adottare tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; dovrà quindi individuare le cause di tale infezione e provvedere a rimuoverle.

Sistema di autenticazione informatica.
Così come previsto dall'Allegato B al D.lgs 196/2003, il trattamento dei dati con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione.
Il Responsabile del trattamento, in accordo con gli Amministratori di sistema, definisce le modalità di assegnazione delle credenziali di autenticazione agli incaricati del trattamento.
Le credenziali possono consistere nell'assegnazione di UserID e password o nell'utilizzo di dispositivi associati ad un codice identificativo o anche ad una caratteristica biometrica.
Ad ogni soggetto autorizzato all'accesso alle banche dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche dati gestite.
Se fra le credenziali è prevista l'assegnazione di una password, questa non deve essere di lunghezza inferiore agli otto caratteri (o al numero massimo possibile se lo strumento elettronico utilizzato non lo consente).

L'incaricato provvederà a modificarla con cadenza almeno semestrale, a meno che la banca dati non contenga dati sensibili; in quest'ultimo caso la parola chiave andrà modificata ogni tre mesi.
Ogni persona incaricata al trattamento dei dati deve adottare tutte le cautele possibili per garantire la segretezza delle credenziali di autenticazione assegnatele.

Per ciò che concerne la gestione dei dati non trattati con strumenti elettronici, viene appositamente definita la modalità di trattamento e i vari supporti utilizzati.
Vengono altresì definite tutte le misure di sicurezza da adottare per evitare l'accidentale perdita o danneggiamento dei dati.
Il DPSS conterrà le modalità di accesso ai locali dove fisicamente vengono gestite le banche dati, sia nel caso di dati trattati con l'ausilio di strumenti elettronici che con altri strumenti. Sarà cura del Responsabile redigere tale documento.

In ogni caso è fatto divieto a qualunque soggetto di divulgare informazioni concernenti i dati oggetto del trattamento, effettuarne copie di qualsiasi natura (su supporti cartacei, informatici, audiovisivi, ecc.) e distruggere, sottrarre o manipolare il contenuto delle banche dati se non espressamente autorizzato dal Responsabile o dal Titolare.

CRITERI DI RIPRISTINO DATI DANNEGGIATI

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, ogni incaricato, di concerto con l'Amministratore del sistema, provvederà a ripristinare i dati mediante utilizzo delle copie di backup realizzate.
L'amministratore può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, registrazioni audiovisive, ecc.) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici che quelli trattati con altri tipi di strumenti.
In caso di distruzione o danneggiamento degli strumenti utilizzati per l'accesso ai dati, l'Amministratore di sistema provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.
La procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità al punto 23 dell'allegato B del D.Lgs 196/2003.
Ad ogni evento che comporti distruzione, danneggiamento o problemi di accesso ai dati dovrà essere opportunamente aggiornata l'analisi dei rischi del presente DPSS.

PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile spetta il compito di provvedere all'opportuna formazione di tutti gli incaricati al trattamento dei dati al fine di:

- garantire il massimo rispetto delle procedure elencate nel presente DPSS
- rendere edotto il personale sui rischi che incombono sui dati
- informare il personale sulle responsabilità che ne derivano

Il Responsabile valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.
Il Responsabile, con cadenza almeno annuale, provvederà a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.

DATI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

Qualora il trattamento dei dati venisse affidato in parte o in toto a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico.
La scelta dei Responsabili del trattamento dati in esterno deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti dal D.Lgs 196/2003 (art. 29 comma 2).
Sarà compito del Responsabile esterno nominare gli incaricati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.
Ogni trattamento di dati affidato a terzi verrà elencato nel DPSS.
Al *Responsabile del trattamento* spetta il compito di vigilare sull'operato del *Responsabile esterno* affinché non vengano mai meno le misure minime di sicurezza dei dati.

CIFRATURA DEI DATI RELATIVI ALLO STATO DI SALUTE

Qualora la tipologia dei dati trattati comprendesse anche quelli di tipo sanitario relativi allo stato di salute o alla vita sessuale, verranno previste idonee misure per gestire la separazione dei dati dall'individuazione diretta dell'interessato ed individuare i casi in cui necessita la loro cifratura.

CENSIMENTO DELLE BANCHE DATI E DEI TRATTAMENTI

L'efficace compilazione del presente DPSS richiede l'effettuazione di una preliminare ricognizione generale di tutti i trattamenti di dati personali svolti all'interno dell'amministrazione comunale ovvero affidati ad entità esterne. La ricognizione interesserà l'intero ciclo di vita dei dati, quindi ogni operazione di trattamento, separando i dati trattati con strumenti elettronici o informatici da quelli cartacei.
La ricognizione è orientata anche al controllo delle finalità e delle modalità con le quali sono svolti i trattamenti, distinguendo tra le varie ipotesi di trattamento.

ANALISI DELLE STRUTTURE FISICHE

La presente parte ha lo scopo di individuare i luoghi (fisici) utilizzati dall'amministrazione comunale per lo svolgimento della propria attività (istituzionale e non) presso i quali siano presenti dati personali ovvero vengano effettuati trattamenti di dati personali.
Contestualmente, si procede all'analisi dei rischi di distruzione e perdita, anche accidentali, dei dati personali trattati, di accessi non autorizzati, di trattamenti non consentiti o non conformi alle finalità della raccolta.

Il censimento dei luoghi fisici avviene utilizzando apposite **schede** che, debitamente compilate, dovranno essere sottoscritte dal Responsabile del trattamento ed allegate al presente DPSS.

ANALISI DEI RISCHI SPECIFICI
nelle strutture fisiche

L'analisi dei rischi viene focalizzata su circostanze possibili, probabili, prevedibili e prevenibili, che possano comportare il verificarsi di rischi di distruzione o di perdita, anche accidentale, dei dati stessi.
I rischi individuati nella presente categoria, vengono chiamati **Rischi Specifici** ed in essi sono comprese tutte le minacce derivanti dalla collocazione territoriale dell'ente, quindi dell'ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento.

TIPO DI RISCHIO	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Ingressi non autorizzati a locali/aree da cui si può accedere ai dati	Impianto di allarme, via d'accesso dotata di inferriate, protezione degli uffici/armadi con serratura, porte interne con serratura.	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione. In particolare si fa notare che non vi è la presenza di nessuna porta blindata agli ingressi.
Sottrazione di strumenti contenenti dati	Impianto di allarme, via d'accesso dotata di inferriate, protezione degli uffici/armadi con serratura, porte interne con serratura.	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione. In particolare si fa notare che non vi è la presenza di nessuna porta blindata agli ingressi.
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, …), nonché dolosi, accidentali o dovuti ad incuria	Armadi a pareti ignifughe, backup dei dati.	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di sicurezza. In particolare si fa notare che: • non tutti i dati vengono salvati tramite procedure di backup; • la totalità dei personal computer non dispone di un gruppo di continuità per filtrare sbalzi di tensione; • non esiste un impianto antincendio e non sono presenti estintori
Guasto a sistemi complementari (impianto elettrico, climatizzazione, …)	Manutenzione correttiva (contratti di manutenzione).	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione. In particolare si suggerisce di prevedere interventi di manutenzione preventiva e programmata dei sistemi, al fine di impedire il verificarsi di guasti che

		possano interrompere le operazioni di trattamento dati.
Errori umani nella gestione della sicurezza fisica	Protezione degli uffici/armadi con serratura, istruzioni impartite al personale tramite la lettera di incarico.	**media** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione solamente se applicate in maniera corretta dal personale incaricato.

SCHEDA RILEVAZIONE LUOGHI FISICI - UFF01

Sportello (primo piano)

BANCHE DATI TRATTATE / OSPITATE

X	Servizi demografici (Scheda rilevazione BD1)	X	Cartaceo	X	Elettronico	X	Tributi comunali (Scheda rilevazione BD2)	X	Cartaceo	X	Elettronico	X	Amministrativo - contabile (Scheda rilevazione BD3)	X	Cartaceo	X	Elettronico
X	Personale (Scheda rilevazione BD4)	X	Cartaceo	X	Elettronico	X	Socio assistenziale (Scheda rilevazione BD5)	X	Cartaceo	X	Elettronico		Ufficio tecnico (Scheda rilevazione BD6)		Cartaceo		Elettronico
X	Segreteria (Scheda rilevazione BD7)	X	Cartaceo	X	Elettronico	X	Commercio e attività prod. (Scheda rilevazione BD8)	X	Cartaceo	X	Elettronico						

TIPOLOGIA DELLE ATTIVITÀ SVOLTE

[X] archiviazione delle banche dati
[X] operazioni di trattamento con strumenti elettronici / informatici
[X] operazioni di trattamento manuale
[X] contemporanea presenza di più uffici o servizi

STRUMENTI DI PROTEZIONE

[X] antifurto	[ ] estintori
[ ] videosorveglianza	[ ] sistema antincendio
[ ] citofoni, segnalatori di ingresso	[ ] porte esterne blindate
[ ] protezioni alle finestre a rischio di intrusione	[X] porte interne con serratura
[ ] divisori, separatori di zona	[X] delimitazione della zona di accesso al pubblico

ACCESSO / PERMANENZA

[ ] accesso da altri locali	[X] accesso da corridoi

Pubblico	Impiegati addetti ad altri uffici
[ ] non consentito	[ ] non consentito
[X] consentito	[X] consentito
[X] orario di sportello	[ ] orario di sportello
[ ] su appuntamento	[X] senza limitazioni

Nominativo incaricato	Presenza stabile
Mogni Claudia	SI

Denominazione risorsa hardware presente	Scheda di riferimento
SERVER	PC01

SCHEDA RILEVAZIONE LUOGHI FISICI - UFF02

Ufficio Sindaco (primo piano)

BANCHE DATI TRATTATE / OSPITATE									
[ ]	Servizi demografici (Scheda rilevazione BD1)	[ ] Cartaceo	[ ] Elettronico	[X]	Tributi comunali (Scheda rilevazione BD2)	[X] Cartaceo	[ ] Elettronico	[X]	Amministrativo - contabile (Scheda rilevazione BD3)	[X] Cartaceo	[ ] Elettronico
[X]	Personale (Scheda rilevazione BD4)	[X] Cartaceo	[ ] Elettronico	[X]	Socio assistenziale (Scheda rilevazione BD5)	[X] Cartaceo	[ ] Elettronico	[ ]	Ufficio tecnico (Scheda rilevazione BD6)	[ ] Cartaceo	[ ] Elettronico
[X]	Segreteria (Scheda rilevazione BD7)	[X] Cartaceo	[X] Elettronico	[X]	Commercio e attività prod. (Scheda rilevazione BD8)	[X] Cartaceo	[ ] Elettronico				

TIPOLOGIA DELLE ATTIVITÀ SVOLTE
[X] archiviazione delle banche dati
[X] operazioni di trattamento con strumenti elettronici / informatici
[X] operazioni di trattamento manuale
[ ] contemporanea presenza di più uffici o servizi

STRUMENTI DI PROTEZIONE	
[ ] antifurto	[ ] estintori
[ ] videosorveglianza	[ ] sistema antincendio
[ ] citofoni, segnalatori di ingresso	[ ] porte esterne blindate
[X] protezioni alle finestre a rischio di intrusione	[X] porte interne con serratura
[ ] divisori, separatori di zona	[ ] delimitazione della zona di accesso al pubblico

ACCESSO / PERMANENZA	
[ ] accesso da altri locali	[X] accesso da corridoi
Pubblico	**Impiegati addetti ad altri uffici**
[ ] non consentito	[ ] non consentito
[X] consentito	[X] consentito
[ ] orario di sportello	[ ] orario di sportello
[X] su appuntamento	[X] senza limitazioni

Nominativo incaricato	Presenza stabile
Chiapparoli Bruno	NO

Denominazione risorsa hardware presente	Scheda di riferimento
CLIENT1	PC02

SCHEDA RILEVAZIONE LUOGHI FISICI - UFF03

Ufficio Segretario Comunale (primo piano)

BANCHE DATI TRATTATE / OSPITATE

[ ]	Servizi demografici (Scheda rilevazione BD1)	[ ] Cartaceo	[ ] Elettronico	[X]	Tributi comunali (Scheda rilevazione BD2)	[X] Cartaceo	[ ] Elettronico	[X]	Amministrativo - contabile (Scheda rilevazione BD3)	[X] Cartaceo	[ ] Elettronico
[X]	Personale (Scheda rilevazione BD4)	[X] Cartaceo	[ ] Elettronico	[X]	Socio assistenziale (Scheda rilevazione BD5)	[X] Cartaceo	[ ] Elettronico	[ ]	Ufficio tecnico (Scheda rilevazione BD6)	[ ] Cartaceo	[ ] Elettronico
[X]	Segreteria (Scheda rilevazione BD7)	[X] Cartaceo	[X] Elettronico	[X]	Commercio e attività prod. (Scheda rilevazione BD8)	[X] Cartaceo	[ ] Elettronico				

TIPOLOGIA DELLE ATTIVITÀ SVOLTE

[X] archiviazione delle banche dati
[X] operazioni di trattamento con strumenti elettronici / informatici
[X] operazioni di trattamento manuale
[ ] contemporanea presenza di più uffici o servizi

STRUMENTI DI PROTEZIONE

[ ] antifurto	[ ] estintori
[ ] videosorveglianza	[ ] sistema antincendio
[ ] citofoni, segnalatori di ingresso	[ ] porte esterne blindate
[X] protezioni alle finestre a rischio di intrusione	[X] porte interne con serratura
[ ] divisori, separatori di zona	[ ] delimitazione della zona di accesso al pubblico

ACCESSO / PERMANENZA

[ ] accesso da altri locali	[X] accesso da corridoi

Pubblico	Impiegati addetti ad altri uffici
[ ] non consentito	[ ] non consentito
[X] consentito	[X] consentito
[ ] orario di sportello	[ ] orario di sportello
[X] su appuntamento	[X] senza limitazioni

Nominativo incaricato	Presenza stabile
Dott. Rossi Mariuccio	NO

Denominazione risorsa hardware presente	Scheda di riferimento
PC-SEGRETARIO	PC03

SCHEDA RILEVAZIONE LUOGHI FISICI - UFF04

Ufficio Ufficio Tecnico (primo piano)

BANCHE DATI TRATTATE / OSPITATE

[ ]	Servizi demografici (Scheda rilevazione BD1)	[ ] Cartaceo	[ ] Elettronico	[ ]	Tributi comunali (Scheda rilevazione BD2)	[ ] Cartaceo	[ ] Elettronico	[ ]	Amministrativo - contabile (Scheda rilevazione BD3)	[ ] Cartaceo	[ ] Elettronico
[ ]	Personale (Scheda rilevazione BD4)	[ ] Cartaceo	[ ] Elettronico	[ ]	Socio assistenziale (Scheda rilevazione BD5)	[ ] Cartaceo	[ ] Elettronico	[X]	Ufficio tecnico (Scheda rilevazione BD6)	[X] Cartaceo	[X] Elettronico
[X]	Segreteria (Scheda rilevazione BD7)	[X] Cartaceo	[X] Elettronico	[ ]	Commercio e attività prod. (Scheda rilevazione BD8)	[ ] Cartaceo	[ ] Elettronico				

TIPOLOGIA DELLE ATTIVITÀ SVOLTE

[X] archiviazione delle banche dati
[X] operazioni di trattamento con strumenti elettronici / informatici
[X] operazioni di trattamento manuale
[ ] contemporanea presenza di più uffici o servizi

STRUMENTI DI PROTEZIONE

[ ] antifurto	[ ] estintori
[ ] videosorveglianza	[ ] sistema antincendio
[ ] citofoni, segnalatori di ingresso	[ ] porte esterne blindate
[X] protezioni alle finestre a rischio di intrusione	[X] porte interne con serratura
[ ] divisori, separatori di zona	[ ] delimitazione della zona di accesso al pubblico

ACCESSO / PERMANENZA

[ ] accesso da altri locali	[X] accesso da corridoi

Pubblico	Impiegati addetti ad altri uffici
[ ] non consentito	[ ] non consentito
[X] consentito	[X] consentito
[ ] orario di sportello	[ ] orario di sportello
[X] su appuntamento	[X] senza limitazioni

Nominativo incaricato	Presenza stabile
Campetti Massimo	NO
Serra Silvano	NO

Denominazione risorsa hardware presente	Scheda di riferimento
CLIENT2	PC04
SERVER	PC05

ANALISI DELLE BANCHE DATI

La presente parte ha lo scopo di **individuare** le banche di dati oggetto di trattamento da parte dell'amministrazione comunale per lo svolgimento della propria attività (istituzionale e non). Contestualmente, si procede all'analisi dei rischi di distruzione e perdita, anche accidentali, dei dati personali trattati, di accessi non autorizzati, di trattamenti non consentiti o non conformi alle finalità della raccolta. Il censimento delle banche dati avviene utilizzando apposite **schede per ogni banca dati** che, debitamente compilate, dovranno essere sottoscritte dal Responsabile del trattamento ed allegate al presente DPSS.

CLASSIFICAZIONE DELLE TIPOLOGIE DEI DATI

Dato personale:
Per dato personale si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione, come numeri di identificazione personale.
Dato sensibile:
Per dati sensibili si intendono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dato giudiziario:
Per dati giudiziari si intendono i dati personali idonei a rivelare informazioni relative al casellario giudiziale, alle sanzioni amministrative, ai carichi pendenti, alla qualità di imputato o di indagato.

AUTORIZZAZIONI, DIVIETI E PERMESSI

L'aggiornamento e la consultazione delle banche dati indicate implicano l'**autorizzazione all'accesso** per i soli dati la cui conoscenza sia strettamente necessaria all'adempimento delle funzioni assegnate.
Al Responsabile del trattamento è affidato il compito di verificare ogni anno, entro il 31 dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'**elenco degli Incaricati** del trattamento che deve essere conservato a cura dello stesso in luogo sicuro. Salva in ogni caso ogni più restrittiva disposizione impartita dal Titolare ovvero dal Responsabile del trattamento, **è fatto divieto a chiunque di**:

- effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento di dati oggetto del trattamento;
- effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- consegnare a persone non autorizzate, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

Archivi elettronici ed informatici
Gli archivi elettronici ed informatici sono conservati esclusivamente per il tramite dei supporti censiti nell'osservanza dei criteri stabiliti dal presente documento. In caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo **USER-ID** assegnato. In caso di dimissioni di un Incaricato o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento deve darne immediata comunicazione al Custode delle password ed all'Amministratore di sistema, i quali provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione. Al Responsabile del trattamento è affidato il compito di verificare ogni anno, entro il 31 dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli Incaricati del trattamento che deve essere conservato a cura dello stesso in luogo sicuro e deve essere trasmesso in copia controllata all'amministratore di sistema ed al custode delle password. Al Responsabile del trattamento è affidato il compito di redigere e di aggiornare ad ogni variazione la **Tabella dei permessi di accesso** che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato. In particolare per ogni Incaricato del trattamento e per ogni Banca di dati debbono essere indicati i privilegi assegnati tra i seguenti:

- inserimento di dati
- lettura e stampa di dati
- variazione di dati
- cancellazione di dati

La tabella dei permessi di accesso deve essere conservata a cura del Responsabile del Trattamento in luogo sicuro e deve essere trasmesso in copia controllata all'amministratore di sistema ed al custode delle password.

Archivi cartacei
Gli archivi cartacei devono essere conservati esclusivamente all'interno dei corrispondenti fascicoli (o faldoni o schede). Ciascun fascicolo (o faldone o scheda) deve essere custodito nei locali archivio e deve esservi ricollocato al termine della sua consultazione da parte dell'incaricato. Eventuali fascicoli in cui siano compresi atti o documenti che contengano dati c.d. sensibili, devono essere custoditi in supporti muniti di serratura il cui accesso deve essere controllato, annotando i soggetti che vi sono ammessi eventualmente dopo l'orario di chiusura dell'ufficio interessato. Gli atti ed i documenti personali devono essere restituiti all'interessato ove la conservazione

non sia imposta da specifica norma di legge. Quanto precedentemente indicato, si applica anche a qualunque tipo di **copia** effettuata sui documenti contenenti dati personali.

ANALISI DEI RISCHI
relativi alle banche dati

L'**integrità dei dati** riguarda la gestione dell'accuratezza e completezza del procedimento di acquisizione, la salvaguardia dell'esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate.
La **disponibilità** assicura che l'accesso ai dati sia disponibile quando necessario. Una garanzia quindi per gli interessati, circa la fruibilità dei dati e/o dei servizi, evitando la perdita o la riduzione dei dati o dei servizi stessi.
Principio cardine di tutta la normativa sulla privacy è la **confidenzialità**, finalizzata a garantire che i dati personali siano conoscibili e/o accessibili soltanto alle persone autorizzate, anche proteggendo le trasmissioni, il controllo degli accessi.

SCHEDA RILEVAZIONE BANCA DATI BD1

BANCA DATI ANAGRAFE ELETTORALE E STATO CIVILE		
TIPOLOGIA RISORSA	**ARCHIVIO ELETTRONICO**	**ARCHIVIO CARTACEO**
Banca dati della popolazione residente	Software DemosWin, sito web INA-SAIA, sito web ISI-ISTATEL	X
Pratiche immigrazione – emigrazione	Software DemosWin, sito web ISI-ISTATEL	X
Cartellini carte d'identità	Software DemosWin	X
Banca dati degli elettori (fascicoli personali)	Software DemosWin	X
Liste sezionali e generali degli elettori	Software DemosWin	X
Banca dati degli incarichi elettorali (presidenti – segretari – scrutatori di seggio)	Software DemosWin, documenti Microsoft Office	X
Atti di stato civile	Software DemosWin	X
Liste di leva	Software DemosWin	X
Registri dei defunti	Software DemosWin	X
Contratti cimiteriali	Documenti Microsoft Office	X
Banca dati AIRE	Software AnagAire	X
Banca dati cittadini AIRE votanti all'estero	Software GestOP	
Banca dati cittadini stranieri (appartenenti alla Comunità Europea ed Extracomunitari)	Software DemosWin, sito web Polizia di Stato	X
Dati anagrafici, dichiarazioni dei redditi e atti del registro dei contribuenti, sia persone fisiche che società, dati delle Commissioni Tributarie	Sito web SIATEL, sito web Telematici Agenzia Entrate	X

HARDWARE SU CUI È OSPITATA:	SERVER	Scheda riferimento: PC01
HARDWARE DI ACCESSO:	SERVER	Scheda riferimento: PC01
UBICAZIONE FISICA (LOCALE)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	Sì
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	Sì
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	SI

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

MODALITÀ DI CONSERVAZIONE ARCHIVI CARTACEI (INDICARE CON UNA X)							
	armadi	x	armadi con chiusura		cassettiere	x	cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento				
Cognome e Nome Incaricato/i	**Inserimento**	**Variazione**	**Lettura / Stampa**	**Cancellazione**
MOGNI CLAUDIA	X	X	X	X
SERRA SILVANO			X	
CHIAPPAROLI BRUNO			X	

SCHEDA RILEVAZIONE BANCA DATI BD2

BANCA DATI TRIBUTI COMUNALI		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati ICI	Software SICI StudioK, sito web SIATEL, sito web SISTER, Portale Comune, sito Equitalia, sito BancoPosta on line	X
Banca dati TRSU	Software SICI StudioK, sito web SIATEL, sito web SISTER, sito Risconet Equitalia, sito Poste Italiane	X
Banca dati Imposta Pubblicità e Pubbliche Affissioni	Documenti Microsoft Office, sito web SIATEL	X
Banca dati Addizionale Comunale Irpef	Sito BancoPosta on line	X
Banca dati TOSAP	Sito BancoPosta on line	X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER	Scheda riferimento: PC01
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	NO
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	NO

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

	armadi	X	armadi con chiusura		cassettiere		cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento				
Cognome e Nome Incaricato/i	**Inserimento**	**Variazione**	**Lettura / Stampa**	**Cancellazione**
MOGNI CLAUDIA	X	X	X	X

Altre strutture/società che concorrono al trattamento

- FM CONSULENZE DI FILIPPO MAGISTRALI & C. SAS – VIA PAOLO BORSELLINO 5 – BORE (PR)
- POSTE ITALIANE SPA - VIALE EUROPA 190 - ROMA

SCHEDA RILEVAZIONE BANCA DATI BD3

BANCA DATI AMMINISTRATIVO - CONTABILE		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati debitori e creditori	Software WinEuro, sito sportello unico previdenziale, sito Acquisti in rete PA	X
Tenuta dati albo di fornitori	Software WinEuro	X
Banca dati Mandati/Reversali	Software WinEuro, servizio Extensive Enti BRE, sito sportello unico previdenziale, sito Acquisti in rete PA	X
Banca dati modello IVA		X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER	Scheda riferimento: PC01
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	NO
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	NO

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

	armadi	X	armadi con chiusura		cassettiere		cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento

Cognome e Nome Incaricato/i	Inserimento	Variazione	Lettura / Stampa	Cancellazione
MOGNI CLAUDIA	X	X	X	X
ROSSI DOTT. MARIUCCIO			X	

Altre strutture/società che concorrono al trattamento

STUDIO ALBERA RAG. PAOLO - PIAZZA DUOMO 33 - VOGHERA (PV)

SCHEDA RILEVAZIONE BANCA DATI BD4

BANCA DATI PERSONALE		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati dei dipendenti	Documenti Acrobat Reader	X
Banca dati rilevazione presenze del personale del Comune		X
Banca dati modello 730 dipendenti		X
Banca dati INPDAP	Sito web INPDAP gestione utenze	X
Banca dati modello 770	Documenti Acrobat Reader	X
Banca dati modello IRAP		X
Banca dati inquadramento contrattuale	Documenti Microsoft Office	X
Banca dati degli incarichi professionali o stagionali del Comune	Documenti Microsoft Office, sito Dipartimento Funzione Pubblica	X
Banca dati degli amministratori del Comune	Documenti Microsoft Office	X
Banca dati stipendi	Software F24 On-line	X
Banca dati distacchi aspettative permessi	Sito Gedap	X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER	Scheda riferimento: PC01
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	SI
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	SI
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	SI

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

	armadi	X	armadi con chiusura		cassettiere	X	cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento

Cognome e Nome Incaricato/i	Inserimento	Variazione	Lettura / Stampa	Cancellazione
ROSSI DOTT. MARIUCCIO			X	
MOGNI CLAUDIA	X	X	X	X
CHIAPPAROLI BRUNO			X	

Altre strutture/società che concorrono al trattamento

INFORMA SRL - P.IVA 01540680038 - CORSO SEMPIONE 39 - CAMERI (NO)
STUDIO ALBERA RAG. PAOLO - PIAZZA DUOMO 33 - VOGHERA (PV)

SCHEDA RILEVAZIONE BANCA DATI BD5

BANCA DATI SOCIO-ASSISTENZIALE		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati associazioni culturali, ricreative, sportive		
Banca dati Isee	Sito Inps	X
Banca dati Dote Scuola	Sito Regione Lombardia (dote scuola)	X
Banca dati Fondo Sostegno Affitto	Sito Regione Lombardia (FSA)	X
Banca dati voucher comunale	Sito Inps Isee	X
Banca dati assitenza minori		X
Banca dati servizi socio assistenziali		X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER	Scheda riferimento: PC01
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	SI
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	NO

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

	armadi	X	armadi con chiusura		cassettiere	X	cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento

Cognome e Nome Incaricato/i	Inserimento	Variazione	Lettura / Stampa	Cancellazione
MOGNI CLAUDIA	X	X	X	X
CHIAPPAROLIU BRUNO			X	
ROSSI DOTT. MARIUCCIO			X	

Altre strutture/società che concorrono al trattamento

C.O.D.A.M.S. DUE - VIA GARIBALDI 108 – VOGHERA (PV)
50&PIU' CAAF - VIA LUIGI MASI 7 - ROMA

SCHEDA RILEVAZIONE BANCA DATI BD6

BANCA DATI UFFICIO TECNICO		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati ditte per gare d'appalto del Comune	Documenti MICROSOFT Office, sito Regione Lombardia (osserv. ll.pp.)	X
Banca dati condono edilizio	Documenti MICROSOFT Office	X
Concessioni edilizie e DIA	Documenti MICROSOFT Office	X
Banca dati stato avanzamento lavori	Documenti MICROSOFT Office, sito Sportello Unico Previdenziale, sito Regione Lombardia (osserv. ll.pp.)	X
Banca dati degli insediamenti produttivi	Documenti MICROSOFT Office, Sito C.C.I.A.A.	X
Banca dati degli insediamenti produttivi ai fini della legge 319 (depurazione acque)	Documenti MICROSOFT Office	X
Banca dati catasto comunale	Software CATASTO 2000	

Hardware su cui è ospitata:	CLIENT2	Scheda riferimento: PC04
Hardware di accesso:	CLIENT2, SERVER	Scheda riferimento: PC04, PC05
Ubicazione fisica (locale)	Archivio elettronico: UFF04	Archivio cartaceo: UFF04

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	NO
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Nessun salvataggio previsto
Frequenza backup	####
Incaricato backup	####
Note	####

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione)	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)							
	armadi	X	armadi con chiusura		cassettiere		cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento				
Cognome e Nome Incaricato/i	**Inserimento**	**Variazione**	**Lettura / Stampa**	**Cancellazione**
ROSSI DOTT. MARIUCCIO			X	
CAMPETTI MASSIMO	X	X	X	X
CHIAPPAROLI BRUNO			X	
SERRA SILVANO			X	

SCHEDA RILEVAZIONE BANCA DATI BD7

BANCA DATI SEGRETERIA		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Protocollo del Comune e Archivio generale	Software SICI StudioK	X
Verbali delle deliberazioni di Giunta Comunale	Documenti MICROSOFT Office	X
Verbali di deliberazioni di Consiglio Comunale	Documenti MICROSOFT Office	X
Determinazioni dei Responsabili	Documenti MICROSOFT Office	X
Banca dati notificazioni messi comunali		X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER, PC-SEGRETARIO	Scheda riferimento: PC01, PC03
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01, UFF03

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	SI
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	SI
dati personali idonei a rivelare lo stato di salute e la vita sessuale	SI
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	NO

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

X	armadi		armadi con chiusura	X	cassettiere		cassettiere con chiusura
X	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento				
Cognome e Nome Incaricato/i	**Inserimento**	**Variazione**	**Lettura / Stampa**	**Cancellazione**
ROSSI DOTT. MARIUCCIO			X	
MOGNI CLAUDIA	X	X	X	X
CHIAPPAROLI BRUNO			X	
SERRA SILVANO			X	
CAMPETTI MASSIMO			X	

SCHEDA RILEVAZIONE BANCA DATI BD8

BANCA DATI COMMERCIO E ATTIVITA' PRODUTTIVE		
Tipologia risorsa	**Archivio elettronico**	**Archivio cartaceo**
Banca dati cessioni di fabbricato legge n.191/78	Documenti MICROSOFT Office	X
Banca dati titolari di autorizzazione al commercio fisso	Documenti MICROSOFT Office, sito Regione Lombardia (Oss. Commercio)	X
Banca dati titolari pubblici esercizi	Documenti MICROSOFT Office, sito Regione Lombardia (Oss. Commercio)	X
Banca dati commercio su aree pubbliche	Documenti MICROSOFT Office, sito Regione Lombardia (Oss. Commercio)	X
Banca dati utenti soggetti a controllo pesi e misure	Documenti MICROSOFT Office	X
Banca dati servizio raccolta smaltimento rifiuti	Sito web O.R.S.O.	X

Hardware su cui è ospitata:	SERVER	Scheda riferimento: PC01
Hardware di accesso:	SERVER	Scheda riferimento: PC01
Ubicazione fisica (locale)	Archivio elettronico: UFF01	Archivio cartaceo: UFF01

TIPOLOGIA DATI PRESENTI SULL'ARCHIVIO	SI/NO
dati personali idonei a rivelare l'origine razziale ed etnica	NO
dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere	NO
dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati	NO
dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	NO
dati personali idonei a rivelare lo stato di salute e la vita sessuale	NO
dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1, lettere da a) a o) e da r) a u), del D.P.R. 14.11.2002 n.13, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti	SI
dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	NO

STRUMENTI E POLITICHE DI BACKUP	
Dispositivo di backup:	Hard disk esterni USB 2.0
Frequenza backup	Giornaliera
Incaricato backup	Mogni Claudia
Note	Il salvataggio della banca dati viene eseguito su n.2 hard disk esterni alternati con cadenza giornaliera. I dati restano salvati per 2 settimane circa prima di essere sostituiti da un nuovo backup.

RISCHI RELATIVI AGLI OPERATORI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Sottrazione di credenziali di autenticazione	Password personale di accesso alla procedura informatica, modifica periodica delle credenziali, logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Carenza di consapevolezza, disattenzione o incuria	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Comportamenti sleali e/o fraudolenti	Logging delle operazioni effettuate nei software e nei siti web che lo prevedono	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Errore materiale	Informazione / formazione specifica sul rischio, backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.

RISCHI RELATIVI AGLI STRUMENTI	MISURE ADOTTATE	GRAVITA' (bassa / media / alta)
Azione di virus informatici o di programmi suscettibili di recare danno	Antivirus	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Spamming o tecniche di sabotaggio		**alta** Non sono adottate misure di sicurezza per contrastare questo tipo di rischio.
Malfunzionamento, indisponibilità o degrado degli strumenti	Manutenzione correttiva (contratto di manutenzione), backup	**media** Si ritiene che le misure adottate siano sufficienti solo in parte a garantire un adeguato livello di protezione.
Accessi esterni non autorizzati	Indirizzamento NAT del router ISDN, firewall software	**alta** Si ritiene che le misure adottate non siano sufficienti a garantire un adeguato livello di protezione.
Intercettazione di informazioni in rete	Cifratura dei dati trasmessi	**bassa** Si ritiene che le misure adottate siano sufficienti a garantire un adeguato livello di protezione.

Modalità di conservazione archivi cartacei (indicare con una X)

	armadi	X	armadi con chiusura		cassettiere	X	cassettiere con chiusura
	scaffali		mensole		altro_____		altro_____

Persone coinvolte nelle operazioni di trattamento				
Cognome e Nome Incaricato/i	**Inserimento**	**Variazione**	**Lettura / Stampa**	**Cancellazione**
MOGNI CLAUDIA	X	X	X	X
CHIAPPAROLI BRUNO			X	
ROSSI DOTT. MARIUCCIO			X	

ANALISI DEGLI STRUMENTI DI LAVORO

La presente parte ha lo scopo di **individuare** gli strumenti elettronici ed informatici utilizzati dall'amministrazione per lo svolgimento della propria attività per il tramite dei quali vengano effettuati trattamenti di dati personali.
Contestualmente, si procede all'analisi dei rischi di distruzione e perdita, anche accidentali, dei dati personali trattati, di accessi non autorizzati, di trattamenti non consentiti o non conformi alle finalità della raccolta.
Il censimento degli strumenti di lavoro avviene utilizzando apposite **schede per ogni strumento** che verranno allegate al presente DPSS.

ANALISI DEI RISCHI
relativi agli strumenti di lavoro

Le principali **fonti di rischio** per i sistemi informatici derivano da: maltempo, inondazioni, fulmini, terremoto, fuoco, attentati, guasti all'hardware, caduta di corrente, omissioni dell'hardware, errori del software, sabotaggi, virus, worm, comportamenti errati, cattiva organizzazione, errata logistica.

Per ogni evento indesiderabile è necessario chiedersi se esso sia possibile, probabile, prevedibile e prevenibile. Tutti questi eventi possono verificarsi con frequenze diverse e presentare un fattore di rischio estremamente diverso.

Tra i rischi da prevenire vi sono quegli eventi che potrebbero causare modifiche, alterazioni, cancellazioni, distruzioni accidentali o deliberate. Vanno inoltre comprese le cause di una possibile gestione non corretta dei trattamenti, ovvero di trattamenti non conformi alle finalità. Una certa attenzione sarà infine dedicata alla possibilità che i dati siano divulgati in assenza di consenso, autorizzazione o comunicazione.

MISURE DI SICUREZZA
PER GLI STRUMENTI ELETTRONICI ED INFORMATICI
MANUTENZIONE DEI SISTEMI INFORMATICI ED ELETTRONICI

Al Responsabile del trattamento per la sicurezza dei dati è affidato il compito di **verificare** ogni anno, avvalendosi dell'Amministratore di sistema, la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.
La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- la sicurezza dei dati trattati;
- il rischio di distruzione o di perdita;
- il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica.

La verifica dei sistemi operativi e delle applicazioni software utilizzate dall'ente, comporta di tener conto di:

- disponibilità di nuove versioni migliorative dei sistemi e delle applicazioni utilizzati;
- segnalazioni di aggiornamenti per la rimozione di errori o malfunzionamenti;
- segnalazioni di aggiornamenti per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il Responsabile del trattamento deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

CUSTODIA ED USO DEI SUPPORTI DI BACKUP

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Responsabile del trattamento della sicurezza dei dati, stabilisce, con il supporto tecnico dell'Amministratore del sistema la **periodicità** con cui debbono essere effettuate le copie di sicurezza delle Banche di dati trattate.

Per ogni Banca di dati sono definite le seguenti **specifiche**:

- il tipo di supporto da utilizzare per le Copie di Back-Up;
- il numero di copie di back-up effettuate ogni volta;
- se i supporti utilizzati per le copie di back-up" sono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate;
- le modalità di controllo delle copie di back-up.
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- l'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di back-up;
- le istruzioni e i comandi necessari per effettuare le copie di Back-Up;

Il **Documento con le istruzioni di copia**, relativo ad ogni banca di dati deve essere conservato a cura dell'amministratore di sistema dei dati in luogo sicuro e deve essere trasmesso in copia al responsabile del trattamento dati ed agli incaricati del trattamento.
Le seguenti istruzioni, impartite dall' amministratore di sistema e rivolte ad ogni incarico del trattamento dei dati personali, vanno attuate tenendo conto dei supporti normalmente utilizzati (floppy disk, CDRom, nastri e dispositivi rimuovibili).
Per l'utilizzo di ogni supporto, dovranno osservarsi le disposizioni di sicurezza riportate dal costruttore/fornitore e, in particolare:

- non debbono essere asportati dall'apparecchiatura che li ospita quando è in corso una elaborazione;

- non deve essere acceso o spenta l'unità di elaborazione quando il dischetto è inserito nella sede di lettura;
- il dischetto va inserito nella finestra nel verso esatto, senza mai forzarne l'ingresso;
- il dischetto è costruito con materiale semirigido, va perciò custodito e trasportato in custodie rigide;
- la parte deputata alla registrazione potrebbe smagnetizzarsi, in tutto od in parte, se accostata a campi magnetici, pur se di debole potenza;
- ulteriori difetti possono insorgere se esposti a temperature basse o alte;
- i supporti danneggiati andranno distrutti evitando che restino in circolazione per evitare il rischio che i dati in essi contenuti possano essere recuperati da persone non autorizzate, in grado di porre in essere sofisticate, ma fattibili, procedure di recupero dei dati.

Quanto ai dati contenuti sul disco fisso, la migliore prevenzione la si ottiene operando in maniera che il disco fisso non contenga informazioni riservate e di carattere sensibile che possano essere lette in chiaro o accessibili a chiunque. E' comunque necessario che l'accesso al disco fisso sia consentito solo al personale autorizzato (incaricato) e dotato di credenziali di autenticazione adeguate.
Infine si presti attenzione alle modalità con le quali vengono applicate le etichette sulle custodie dei supporti. Dalla chiarezza e leggibilità delle sigle riportate sulle etichette o sui supporti stessi (ove consentito) potranno dipendere sia la velocità di ripristino in caso di necessità, sia il grado di riservatezza dei loro contenuti. Allo scopo si consideri l'opportunità di utilizzare codici di siglatura non a tutti riconoscibili, per l'identificazione delle registrazioni riservate.
Nell'ipotesi in cui i supporti di back-up ovvero i dischi fissi debbano essere oggetto di interventi di riparazione da eseguirsi al di fuori della struttura comunale, dovrà prestarsi particolare attenzione a che gli stessi siano smagnetizzati o comunque resi illeggibili prima che il tecnico addetto alla riparazione li trasferisca all'esterno dei locali comunali.
Il Responsabile del trattamento della sicurezza dei dati, è responsabile della **custodia** e della **conservazione** dei supporti utilizzati per il backup dei dati. Per ogni banca di dati deve essere indicato il luogo di conservazione dei supporti utilizzati per il back-up dei dati, individuato in modo che sia protetto da:

- agenti chimici;
- fonti di calore;
- campi magnetici;
- intrusioni e atti vandalici;
- incendio ;
- allagamento;
- furto.

L'**accesso** ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati al Responsabile del trattamento della sicurezza dei dati, agli incaricati del trattamento ed all'amministratore di sistema.
E' fatto **divieto** a chiunque di effettuare copie - su supporti magnetici - non autorizzate dal Responsabile del trattamento per la sicurezza dei dati.

OPERAZIONI DI RIPRISTINO DEI DATI

IL **ripristino dei dati** viene inteso nel senso della possibilità di ripristino di tutti i files di dati, dei programmi, del software di base che l'evento indesiderato ha alterato o distrutto, ovvero nella sostituzione delle componenti tecnologiche hardware che hanno provocato l'interruzione del trattamento.
Una corretta organizzazione richiede necessariamente:

- il censimento dei dati da tutelare (in particolare quelli sensibili e giudiziaria);
- la produzione di copie di sicurezza;
- la custodia delle copie di sicurezza;
- la prova di funzionamento delle copie di sicurezza;
- individuazione dei soggetti incaricati a produrre le copie di sicurezza;
- il ripristino dei dati in tempi accettabili e, comunque, non superiori a sette giorni lavorativi.

E' fatto **divieto** a chiunque di effettuare il ripristino - di copie su supporti magnetici – non autorizzato dal Responsabile del trattamento per la sicurezza dei dati.

SCHEDA RILEVAZIONE RISORSE HARDWARE PC1

Dislocazione	Il personal computer si trova nell'ufficio UFF01

Dati generali			
Nome computer	SERVER	Descrizione	File server
Modello	Assemblato		

Caratteristiche HW/SW salienti			
processore	AMD Athlon64 X2 5200+	memoria RAM	2 Gb
HDD	N.2 MAXTOR 160 Gb S-ATA2 RAID1	sistema operat.	Windows XP Professional SP3
ambiente operat.	Office 2007	browser	Internet Explorer 7
client e-mail	Outlook Express 6	altro	####

Tipologia PC

[X] server [ ] client [ ] stand alone [ ] altro _____

Tipologia rete

[ ] non in rete [X] rete LAN [ ] rete pubblica [ ] altro _____

Connessione internet

[ ] non connesso [ ] modem [X] router ISDN [ ] altro _____

Password di protezione PC e/o sistema operativo

[ ] all'accensione [ ] windows [ ] screen saver [X] nessuna password

Protezione contro virus

[X] permanente [ ] manuale [ ] programmata [ ] altro _____

Frequenza di aggiornamento	giornaliera. Il programma controlla automaticamente la presenza di aggiornamenti quando è attiva una connessione ad Internet.
Denominazione software	KASPERSKY Antivirus 2009

Protezione contro intrusioni dall'esterno

[X] presente [ ] non presente

Denominazione software	Windows Firewall + indirizzamento NAT nel router ISDN

Protezione antispam sulle caselle di posta

[X] presente [ ] non presente

Denominazione software	presente solo sulla casella di posta elettronica certificata

Protezione contro sbalzi di tensione

[ ] presente [X] non presente

Descrizione dispositivo	

Dispositivi acquisizione / registrazione dati

[X] floppy disk [ ] CD-ROM [ ] DVD [X] masterizzatore DVD
[ ] chiave USB [ ] scanner [X] HDD (q.tà 2) [ ] altro:

segue⇨

⇦ continua

Banche dati ospitate / trattate			
Descrizione	**Rif. scheda**	**Ospitata**	**Trattata**
Servizi demografici	BD1	X	X
Tributi comunali	BD2	X	X
Amministrativo – contabile	BD3	X	X
Personale	BD4	X	X
Socio assistenziale	BD5	X	X
Segreteria	BD7	X	X
Commercio e attività produttive	BD8	X	X

SCHEDA RILEVAZIONE RISORSE HARDWARE PC2

Dislocazione	Il personal computer si trova nell'ufficio UFF02

Dati generali

Nome computer	CLIENT1	Descrizione	PC Sindaco
Modello	IBM Netvista 6830-TFG		

Caratteristiche HW/SW salienti

processore	INTEL Pentium 3 1 GHz	memoria RAM	256 Mb
HDD	20 Gb	sistema operat.	Windows 2000 SP4
ambiente operat.	Microsoft Office 2000	browser	Internet Explorer 6
client e-mail	Outlook Express 6	altro	####

Tipologia PC

[ ] server	[X] client	[ ] stand alone	[ ] altro _____

Tipologia rete

[ ] non in rete	[X] rete LAN	[ ] rete pubblica	[ ] altro _____

Connessione internet

[ ] non connesso	[ ] modem	[X] router ISDN	[X] altro: _____

Password di protezione PC e/o sistema operativo

[ ] all'accensione	[ ] windows	[ ] screen saver	[X] nessuna password

Protezione contro virus

[X] permanente	[ ] manuale	[ ] programmata	[ ] altro: _____

Frequenza di aggiornamento	giornaliera. Il programma controlla automaticamente la presenza di aggiornamenti quando è attiva una connessione ad Internet.
Denominazione software	Avira AntiVir Personal v.8

Protezione contro intrusioni dall'esterno

[X] presente	[ ] non presente
Denominazione software	indirizzamento NAT nel router ISDN

Protezione contro sbalzi di tensione

[ ] presente	[X] non presente
Descrizione dispositivo	

Dispositivi acquisizione/registrazione dati

[X] floppy disk	[X] CD-ROM	[ ] DVD	[ ] masterizzatore
[ ] chiave USB	[ ] scanner	[X] HDD (q.tà 1)	[ ] altro:

Banche dati ospitate / trattate

Descrizione	Rif. scheda	Ospitata	Trattata
Segreteria	BD7		X

SCHEDA RILEVAZIONE RISORSE HARDWARE PC3

Dislocazione	Il personal computer si trova nell'ufficio UFF03

Dati generali

Nome computer	PC-SEGRETARIO	Descrizione	PC Segretario Comunale
Modello	COMPAQ EVO		

Caratteristiche HW/SW salienti

processore	INTEL Pentium 4 1.4 GHz	memoria RAM	256 Mb
HDD	20 Gb	sistema operat.	Windows 98SE
ambiente operat.	Microsoft Office 2000	browser	Internet Explorer 6
client e-mail	Outlook Express 6	altro	####

Tipologia PC

[ ] server	[X] client	[ ] stand alone	[ ] altro _____

Tipologia rete

[ ] non in rete	[X] rete LAN	[ ] rete pubblica	[ ] altro _____

Connessione internet

[ ] non connesso	[ ] modem	[X] router ISDN	[X] altro: _____

Password di protezione PC e/o sistema operativo

[ ] all'accensione	[ ] windows	[ ] screen saver	[X] nessuna password

Protezione contro virus

[X] permanente	[ ] manuale	[ ] programmata	[ ] altro: _____

Frequenza di aggiornamento	giornaliera. Il programma controlla automaticamente la presenza di aggiornamenti quando è attiva una connessione ad Internet.
Denominazione software	Avira AntiVir Personal v.8

Protezione contro intrusioni dall'esterno

[X] presente	[ ] non presente
Denominazione software	indirizzamento NAT nel router ISDN

Protezione contro sbalzi di tensione

[ ] presente	[X] non presente
Descrizione dispositivo	

Dispositivi acquisizione/registrazione dati

[X] floppy disk	[X] CD-ROM	[ ] DVD	[ ] masterizzatore
[ ] chiave USB	[ ] scanner	[X] HDD (q.tà 1)	[ ] altro:

Banche dati ospitate / trattate

Descrizione	Rif. scheda	Ospitata	Trattata
Segreteria	BD7	X	X

SCHEDA RILEVAZIONE RISORSE HARDWARE PC4

Dislocazione	Il personal computer si trova nell'ufficio UFF04

Dati generali

Nome computer	CLIENT2	Descrizione	PC Tecnico Comunale
Modello	IBM Netvista 6830-TFG		

Caratteristiche HW/SW salienti

processore	INTEL Pentium 3 1 GHz	memoria RAM	256 Mb
HDD	20 Gb	sistema operat.	Windows 2000 SP4
ambiente operat.	Microsoft Office 2000	browser	Internet Explorer 6
client e-mail	Outlook Express 6	altro	####

Tipologia PC

[ ] server	[X] client	[ ] stand alone	[ ] altro _____

Tipologia rete

[ ] non in rete	[X] rete LAN	[ ] rete pubblica	[ ] altro _____

Connessione internet

[ ] non connesso	[ ] modem	[X] router ISDN	[X] altro: _____

Password di protezione PC e/o sistema operativo

[ ] all'accensione	[ ] windows	[ ] screen saver	[X] nessuna password

Protezione contro virus

[X] permanente	[ ] manuale	[ ] programmata	[ ] altro: _____

Frequenza di aggiornamento	giornaliera. Il programma controlla automaticamente la presenza di aggiornamenti quando è attiva una connessione ad Internet.
Denominazione software	Avira AntiVir Personal v.8

Protezione contro intrusioni dall'esterno

[X] presente	[ ] non presente
Denominazione software	indirizzamento NAT nel router ISDN

Protezione contro sbalzi di tensione

[ ] presente	[X] non presente
Descrizione dispositivo	

Dispositivi acquisizione/registrazione dati

[X] floppy disk	[X] CD-ROM	[ ] DVD	[ ] masterizzatore
[ ] chiave USB	[ ] scanner	[X] HDD (q.tà 1)	[ ] altro:

Banche dati ospitate / trattate

Descrizione	Rif. scheda	Ospitata	Trattata
Ufficio tecnico	BD6	X	X

SCHEDA RILEVAZIONE RISORSE HARDWARE PC5

Dislocazione	Il personal computer si trova nell'ufficio UFF04

Dati generali			
Nome computer	SERVER	Descrizione	PC Silvano
Modello	IBM Netvista 6830-TFG		

Caratteristiche HW/SW salienti			
processore	INTEL Pentium 3 1 GHz	memoria RAM	256 Mb
HDD	20 Gb q.tà 2	sistema operat.	Windows 2000 SP4
ambiente operat.	Microsoft Office 2000	browser	Internet Explorer 6
client e-mail	Outlook Express 6	altro	####

Tipologia PC

[ ] server	[ ] client	[X] stand alone	[ ] altro _____

Tipologia rete

[X] non in rete	[ ] rete LAN	[ ] rete pubblica	[ ] altro _____

Connessione internet

[X] non connesso	[ ] modem	[ ] router ISDN	[X] altro: _____

Password di protezione PC e/o sistema operativo

[ ] all'accensione	[ ] windows	[ ] screen saver	[X] nessuna password

Protezione contro virus

[ ] permanente	[ ] manuale	[ ] programmata	[X] nessun antivirus installato

Frequenza di aggiornamento	
Denominazione software	

Protezione contro intrusioni dall'esterno

[ ] presente	[X] non presente

Denominazione software	

Protezione contro sbalzi di tensione

[ ] presente	[X] non presente

Descrizione dispositivo	

Dispositivi acquisizione/registrazione dati

[X] floppy disk	[X] CD-ROM	[ ] DVD	[ ] masterizzatore
[ ] chiave USB	[ ] scanner	[X] HDD (q.tà 2)	[ ] altro:

Banche dati ospitate / trattate

Descrizione	Rif. scheda	Ospitata	Trattata
Ufficio tecnico (software CATASTO 2000)	BD7	X	X

INTERVENTI FORMATIVI

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua l'ambito del trattamento consentito. Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento.

Formazione da impartire	Intervento formativo
Custodia dello strumento elettronico durante una sessione di trattamento di dati personali	Con apposito corso formativo, organizzato a cura del Responsabile del Trattamento, è stato sensibilizzato il personale incaricato al trattamento e alla custodia dello strumento elettronico in particolare durante una sessione di trattamento.
Rischi incombenti sui dati	Apposito corso formativo organizzato dal Responsabile del trattamento ha illustrato i rischi che incombono sui dati. E' stato istruito il personale incaricato del trattamento all'utilizzo corretto degli applicativi che consentono l'acceso ai dati.
Misure preventive di eventi dannosi	Con apposito corso è stato sensibilizzato il personale incaricato del trattamento a non attuare azioni che possano danneggiare gli elaboratori elettronici ed i dati in essi contenuti. Il personale incaricato è stato ammonito sulle responsabilità a loro carico dettate dalla normativa vigente ed è stato sensibilizzato sulle misure minime di sicurezza da adottare.
Conoscenza delle norme e del DPSS o delle parti rilevanti in relazione al trattamento dei dati.	In un corso oculatamente organizzato è stata data lettura dell'allegato B del Dlgs 196/2003 e del Documento di Programmazione sulla Sicurezza dei dati personali. Si è rapportata la norma alle esigenze della nostra attività aziendale chiarendo contestualmente i dubbi che il personale incaricato del trattamento ha posto.
Custodia ed uso dei supporti rimovibili contenenti dati personali, sensibili o giudiziari.	Il responsabile del trattamento ha fornito apposite istruzioni sulle misure in caso di trattamento di dati sensibili o giudiziari. Quindi si è invitato il personale incaricato del trattamento a non lasciare incustoditi i supporti rimovibili contenenti dati personali, di non condurre supporti rimovibili all'esterno degli uffici in cui il trattamento è effettuato. Infine è stato fatto assoluto divieto di condurre dati sensibili o giudiziari all'esterno dei locali in cui si effettua il trattamento se non preventivamente autorizzati.
Controllo e custodia per l'intero ciclo di trattamento di dati senza supporto di strumenti elettronici	Le procedure per il controllo, la custodia ed il trattamento di dati personali senza l'ausilio di strumenti elettronici. A cura del responsabile è stato organizzato apposito corso formativo che ha coinvolto tutti gli incaricati elencati in cui sono state illustrate le modalità del trattamento.

Formazione degli incaricati al trattamento

Agli incaricati al trattamento, il titolare (direttamente o tramite soggetti da lui identificati) fornisce la necessaria formazione:

- al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansione
- in occasione dell'introduzioni di nuovi strumenti e programmi informatici

La formazione interesserà sia le norme generali in materia di privacy, sia gli aspetti peculiari dei trattamenti effettuati.

ALLEGATI

Formano parte integrante del presente Documento tutti gli allegati di seguito elencati.

A) lettere d'incarico:
    1) lettera d'incarico al responsabile del trattamento dati;
    2) lettera all'incaricato del trattamento dei dati;
    3) lettera d'incarico all'amministratore del sistema;
    4) lettera d'incarico al custode delle credenziali;
    5) lettera d'incarico al responsabile esterno.
B) registro variazione password;
C) registro copie di backup;
D) registro dei rischi informatici;
E) registro interventi formativi.