☐ Comunicazione Prefettura ex art. 135
Dlgs. 267/2000

COPIA WEB
Deliberazione **N. 18**
in data **28/03/2011**
Prot. N**. 4997**

COMUNE DI ROSSANO VENETO

PROVINCIA DI VICENZA

Verbale di Deliberazione della **Giunta Comunale**

OGGETTO:

REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA. ADEGUAMENTO DELLE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS N. 196 DEL 2003 - ANNO 2011.

L'anno **DUEMILAUNDICI** addì **VENTOTTO** del mese di **MARZO** alle **ore 19.00** nella sala delle adunanze del Comune suddetto, convocata con appositi avvisi, la Giunta Comunale si è riunita con la presenza dei Signori:

	Presenti	**Assenti**
1. TREVISAN Gilberto - Sindaco	*	
2. GIACCHERI Paola - Assessore	*	
3. MARCON Ezio "	*	
4. SARTORE ALDO "	*	
5. ROSSI FRANCO "		*
6. VICO SABRINA "	*	
7. GASTALDELLO ANDREA "	*	

Assiste alla seduta il **Segretario Comunale ORSO Dott. Paolo.**

Il Sindaco TREVISAN Gilberto assume la presidenza e, riconosciuta legale l'adunanza, dichiara aperta la seduta.

LA GIUNTA COMUNALE

OGGETTO: REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA. ADEGUAMENTO DELLE MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS N. 196 DEL 2003 - ANNO 2011.

PREMESSO:

CHE con deliberazione di G.C. n. 57 in data 20.04.2000 è stato approvato il documento programmatico – Piano Operativo per le misure di sicurezza per il trattamento dei dati personali;

CHE tale documento è stato revisionato ed adeguato alle disposizioni del D.P.R. 318/99, come da deliberazione di G.C. n. 146 del 31.12.2002, con la quale è stata altresì disposta l'adozione da parte di ogni Responsabile di Area di un provvedimento di nomina dei dipendenti incaricati al trattamento dei dati sensibili e/o particolari;

DATO ATTO che, in attuazione del provvedimento succitato, i Responsabili di Area hanno provveduto a nominare gli incaricati al trattamento dei dati personali;

VISTO il D.lgs. 196 del 30.06.2003 "Codice in materia di protezione dei dati personali" che introduce significativi elementi di novità, tenuto conto della giurisprudenza del Garante per la protezione dei dati personali e della Direttiva UE 2000/58 sulla riservatezza delle comunicazioni elettroniche;

CONSIDERATO che la finalità della predetta normativa risulta essere quella di garantire che il trattamento dei dati *Personali, Identificativi, Sensibili e Giudiziari*, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, identificativi, sensibili e giudiziari;

VISTA la deliberazione di G.C. n. 68 del 22.06.2004, con la quale è stato operato l'adeguamento del Documento programmatico sulla Sicurezza (DPS) alle previsioni introdotte dall'art. 180 del D.lgs. 196/03;

RAVVISATA la necessità di aggiornare annualmente entro il 31 marzo il DPS, sulla scorta delle linee guida contenute nell'Allegato B del d.lgs. n. 196 del 30.06.2003, finalizzato all'analisi, elaborazione, implementazione e gestione di soluzioni nell'ambito delle applicazioni in uso presso il comune di Rossano Veneto;
VISTO il provvedimento generale del garante per la protezione dei dati personali del 31.03.2004 con il quale sono state prorogate alcune scadenze generali tra le quali quella dell'adozione del D.P.S. e quelle di approvazione del documento di differimento per l'adozione delle misure minime stabilite dal comma 2 art. 180 del d.lgs. 196/2003;

DATO ATTO che in data 30.04.2004 il Comune di Rossano Veneto ha provveduto ad effettuare la notificazione al Garante, ai sensi e per gli effetti di cui all'art. 37 del d.lgs. 196/03;

VISTA la deliberazione di C.C. n. 105 del 28.12.2005 avente ad oggetto "Adozione Regolamento relativo all'identificazione delle attivita' che perseguono rilevanti finalita' di interesse pubblico, ai sensi del d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

PRESO ATTO delle linee guida in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, dettati dal Garante per la Privacy con deliberazione del 14 giugno 2007;

VISTA la deliberazione di G.C. n. 33/2010 avente ad oggetto "Revisione del documento programmatico sulla sicurezza adeguamento delle misure minime di sicurezza nel trattamento dei dati

personali ai sensi del d.lgs. n. 196 del 2003";

RITENUTO di procedere alla revisione del documento programmatico sulla sicurezza, come da allegato sub A) alla presente per formarne parte integrante e sostanziale;

DELIBERA

1 – di approvare la revisione del documento programmatico sulla sicurezza contenuto nell'allegato sub A) alla presente per formarne parte integrante e sostanziale;

2 – di assicurare l'adeguamento al suddetto documento da parte di ogni Responsabile di Area, cui spetterà la nomina dei dipendenti incaricati al trattamento dei dati sensibili e/o particolari tramite propria determinazione.

* * * * * * * * * * *

Sulla suestesa proposta di deliberazione sono stati acquisiti i seguenti pareri ai sensi dell'art. 49, comma 1,del D. Lgs. 18.08.2000 n. 267;

- VISTO, si esprime parere favorevole in ordine alla regolarità tecnica.

Fto *IL RESPONSABILE SERV. TECNICO*
Dott. Paolo ORSO

COMUNE DI ROSSANO VENETO

SERVIZI INFORMATICI

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI INFORMATICI

Allegato A)

INDICE

1 – INTRODUZIONE

Il presente documento è adottato dal Comune di Rossano Veneto allo scopo di descrivere e pianificare, attraverso la rilevazione delle risorse attinenti il patrimonio informatico ed una analisi dei rischi cui lo stesso è soggetto, le misure di sicurezza fisiche, logiche ed organizzative adottate o da adottare per la sicurezza e integrità dei trattamenti effettuati mediante strumenti automatizzati, individuati come necessari per l'attività e che contengono dati personali soggetti all'applicazione del Dlgs 30/06/2003 n. 196 "Codice in materia di protezione dei dati personali".
Le misure individuate sono tali da soddisfare i requisiti generali del Dlgs 196/2003 e le misure minime di sicurezza descritte nell'allegato B del medesimo decreto legislativo.

2 – ASPETTI GENERALI

2.1 – Contenuti

Secondo quanto disposto dall'allegato B) del Dlgs 196/2003 il presente documento definisce, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità:

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 la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
e. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
f. la previsione di interventi formativi degli incaricati del trattamento, per renderli competenti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
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.

2.2 – Responsabilità

Il Titolare del trattamento dei dati personali (di seguiti Titolare) ed il Responsabile del trattamento dei dati informatici (di seguito Responsabile) assicureranno che il programma di sicurezza sia adeguatamente sviluppato, realizzato e gestito secondo quanto indicato nel presente documento con lo scopo di:

a. minimizzare le possibilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali o comunque critici per le funzioni istituzionali;
b. minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali.

2.3 – Applicabilità

Le norme indicate nel presente documento si applicano a tutti i trattamenti eseguiti nell'ambito dell'Ente e sono da considerarsi vincolanti anche nei rapporti contrattuali relativi a trattamenti eseguiti da altri soggetti esterni cui vengano conferiti incarichi in materia di informatizzazione.

2.4 – Validità
Il presente documento è valido per un anno dalla data della sua emissione o dalla sua ultima revisione e comunque non oltre il 31 marzo di ogni anno.
Entro tale data dovrà essere effettuato quanto previsto dal successivo punto 2.5.

2.5 – Revisione
La revisione del documento avviene obbligatoriamente:

a. alla scadenza del periodo di validità, allo scopo di valutare l'adeguatezza del documento anche in considerazione dell'evoluzione tecnologica;
b. ogni qualvolta dovessero cambiare le strutture dei dati o le apparecchiature oggetto delle misure di sicurezza;
c. ad ogni modifica della struttura organizzativa cui è demandata la responsabilità della sicurezza;
d. ad ogni controllo periodico cui le misure di sicurezza sono sottoposte per verificarne la validità ed efficacia. In tal caso la revisione del documento riporterà gli esiti di tale controllo ed eventuali riferimenti alla documentazione prodotta.

La nuova versione del documento riporterà, in modo sintetico, un verbale del processo di revisione che ha portato alla sua emissione con l'indicazione delle motivazioni.

3 - STRUTTURA ORGANIZZATIVA

3.1 – Identificazione dei trattamenti
Presso il Comune di Rossano Veneto vengono eseguiti trattamenti dei dati previsti dalla Legge 196/2003 e cioè operazioni o complesso di operazioni, svolte con l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la diffusione, la cancellazione di dati personali, trattamenti tutti finalizzati all'attività istituzionale dell'Ente.
L'elenco completo dei trattamenti, le unità organizzative coinvolte e i relativi incaricati sono riportati nell'allegato A) al presente documento.

3.2 – Titolare del trattamento dei dati personali
Titolare del trattamento dei dati oggetto del presente documento è il Comune di Rossano Veneto nella persona del Sindaco.
Il Titolare identifica i trattamenti necessari allo svolgimento dei processi dell'Ente, definisce le modalità e le finalità degli stessi e la natura dei dati trattati. Il Titolare è inoltre responsabile dell'osservanza di tutte le normative di legge in materia di dati personali.
Il Titolare emana il Documento Programmatico sulla sicurezza e vigila sulla sua applicazione.

3.3 – Responsabile del trattamento dei dati informatici
Il Responsabile del trattamento dei dati informatici è individuato nella persona del Responsabile del Servizio Informatico dell'Ente.
Il Responsabile ha il compito di attuare le normative di legge e le prescrizioni di sicurezza indicate nel presente documento per quanto attiene il trattamento dei dati personali definiti dal Titolare come funzionali allo svolgimento dei processi dell'Ente, ivi incluso quanto attiene alla gestione tecnica delle risorse informatiche ed allo sviluppo e manutenzione delle funzionalità applicative degli stessi.
Il Responsabile rileva e propone al Titolare le esigenze di atti formali nei confronti dell'Autorità Garante della Privacy.
Egli nomina incaricati di trattamento le persone fisiche che accedono ai dati, assegnando loro, ove lo ritenga opportuno, anche delle responsabilità specifiche in relazione ai diversi trattamenti effettuati.

Il Responsabile viene nominato mediante comunicazione scritta da parte del Titolare e la comunicazione dovrà essere controfirmata per accettazione.

3.4 – Amministratore della sicurezza, del sistema e delle password

L'amministratore della sicurezza e delle password (di seguito custode delle password) è nominato dal Titolare e nel Comune di Rossano Veneto viene identificato con la figura del Responsabile.
Il custode delle password ha il compito di assicurare la disponibilità dei dati e degli strumenti informatici in caso di prolungata assenza dell'incaricato che renda indispensabile od indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema. La custodia delle copie delle password è organizzata garantendo la relativa segretezza mediante conservazione presso cassaforte.
L'amministratore del Sistema è nominato dal Responsabile e nel Comune di Rossano Veneto viene identificato nella persona del Titolare della ditta ACTS Informatica, Via Ponchielli 5 -36030 Caldogno (VI), ditta incaricata dal Responsabile per l'attività di assistenza tecnico sistemistica hardware e software del Comune di Rossano Veneto.
L'operato dell'amministratore di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento o del Responsabile, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

3.5 – Incaricato del trattamento dei dati

L'incaricato del trattamento dei dati (di seguito incaricato) opera in accordo con le mansioni ed istruzioni affidate, eseguendo le operazioni necessarie per l'esecuzione dei trattamenti specificati.
L'incaricato viene nominato mediante comunicazione scritta dal Responsabile e la comunicazione dovrà essere controfirmata per presa visione. Nella lettera di nomina dovranno essere indicati in dettaglio i trattamenti e gli archivi cui l'incaricato è autorizzato ad accedere.

4 – SICUREZZA DEI DATI

4.1 - Analisi dei rischi

Per ciascun tipo di trattamento dei dati vengono adottate misure di sicurezza adeguate.
I singoli rischi sono raggruppati come segue:

- **rischi per la riservatezza dei dati**
  le informazioni devono essere accessibili ed utilizzate solo da persone autorizzate e per fini conformi all'attività istituzionale dell'Ente;
- **rischi per l'integrità dei dati**
  i dati devono essere esatti, aggiornati e corrispondenti alla realtà proteggendoli da qualsiasi forma di alterazione non controllata;
- **rischi per la disponibilità**
  l'accesso ai dati deve poter avvenire ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;
- **rischi di uso improprio**
  l'accesso ai dati deve avvenire esclusivamente per i fini definiti dal Titolare da parte di soggetti adeguatamente autorizzati e istruiti.

4.2 – Misure di sicurezza

In considerazione dei rischi individuati vengono indicate le misure di sicurezza adottate nel rispetto degli obblighi di legge.
Le misure di sicurezza sono divise in:

• **misure di sicurezza fisiche**
riguardano la sicurezza passiva e il controllo degli accessi ai locali contenenti le apparecchiature ed i supporti di memorizzazione informatici;

• **misure di sicurezza logiche**
riguardano il controllo dell'accesso alle piattaforme, agli archivi, ai database e alle applicazioni con il compito di segnalare una intrusione in atto e di richiedere l'intervento del Responsabile e/o di un tecnico in grado di bloccare l'intrusione;

• **misure di sicurezza organizzative**
riguardano le modalità per garantire la corretta funzionalità delle misure fisiche e logiche e di assicurare in tempi brevi l'intervento del Responsabile e/o dei tecnici.

4.3 – Misure di sicurezza fisiche

Le macchine server del Comune di Rossano Veneto, (vedi all. A), sono:
- server IBM (per gestione software contabilità finanziaria, personale, anagrafe della popolazione, stato civile, servizio elettorale, servizio di leva);
- server HP (per Terminal Services);
- server HP (per gestione dati);
- server HP (server primario per gestione di tutta la rete informatica).

Le stesse sono collocate in un locale esclusivamente destinato allo scopo posto al piano interrato dell'edificio comunale.
Questo locale è dotato di

• impianto elettrico a norma;
• un gruppo di continuità che permette il salvataggio dei dati e il mantenimento in funzione per un periodo di tempo limitato anche in caso di black out;
• impianto di condizionamento;
• idonee metodologie antincendio;
• impianto antifurto.

Il locale è accessibile esclusivamente al Titolare, al Responsabile del trattamento dei dati informatici, all'Amministratore della sicurezza, del sistema e delle password, all'incaricato dell'esecuzione dei back-up nonché ai tecnici di società esterne che operano per l'Ente esclusivamente per la necessaria manutenzione ed installazione delle componenti hardware e software di loro competenza.
In assenza del personale la sala viene mantenuta chiusa a chiave.
I supporti di back up vengono conservati in una cassetta di sicurezza antincendio e blindata, munita di serratura di sicurezza, posto nell'Ufficio Ragioneria.
Le chiavi dell'armadio vengono custodite dal Responsabile e dagli addetti all'Ufficio Ragioneria.
Non esistono armadi che contengono gli apparati di rete.
Le singole apparecchiature sono date in dotazione agli uffici e ai servizi secondo quanto indicato nell' all. A).

4.4 – Misure di sicurezza logiche

a) sicurezza del software

Presso ciascun ufficio e su ogni postazione di lavoro è consentita esclusivamente l'installazione delle seguenti categorie di software:

• software commerciale, ancorché gratuito, dotato di apposita licenza d'uso;
• software gestionale realizzato specificatamente per l'Amministrazione Comunale da ditte specializzate nel settore della Pubblica Amministrazione;
• software realizzato internamente per soddisfare eventuali esigenze particolari del singolo servizio;

• software scaricato via internet o posta elettronica, realizzato e trasmesso da altri Enti della Pubblica Amministrazione (Regione, Provincia, Prefettura, Ministeri, Agenzia della Entrate, ecc.) per la trasmissione on-line delle relative informazioni.

L'eventuale installazione di software diversi da quelli citati deve essere preventivamente valutata ed autorizzata dal Responsabile e dall'Amministratore di sistema.
Il software installato sulla rete e sulle singole postazioni è in dotazione ai servizi e agli uffici secondo quanto indicato nell'allegato A).
Al fine di prevenire ed evitare la diffusione di virus informatici il software deve venir installato solo da supporti fisici originari, dei quali sia nota la provenienza o scaricato, se nel caso, dai siti ufficiali degli Enti e delle società titolari dei diritti.
La rete informatica e le singole postazioni sono protette dal programma antivirus G Data gestito dal server con aggiornamenti giornalieri.
Le postazioni ubicate presso la Biblioteca Comunale protette con antivirus AVAST con aggiornamento giornaliero e da un firewall.
Per quanto riguarda la gestione della sicurezza della posta elettronica, dei servizi accessori, quali dominio, hosting, aggiornamenti e gestione del servizio e mail illimitate è garantita direttamente dalla Ditta affidataria della creazione e della gestione del sito Internet Comunale che provvede ad un controllo della posta in arrivo, mentre l'accesso ad internet è garantito da un firewall, interposto tra la rete interna e quella esterna, in grado di filtrare e prevenire gli accessi non autorizzati ed indesiderati alla rete comunale. Tra il firewall e il server esiste un'ulteriore password per garantire in maniera ottimale la protezione della Intranet.
Periodicamente viene effettuato uno scandisk del server.

b) integrità dei dati
Il Responsabile mantiene l'elenco (all. A) di tutte le attrezzature informatiche dei singoli uffici, dello scopo a cui sono destinati, della loro locazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate. Tale elenco viene aggiornato in caso di necessità o in occasione di consistenti modifiche nella dotazione delle attrezzature stesse.
In fase di installazione e configurazione del sistema di archiviazione dei file sono stati definiti i volumi logici o le aree di disco da sottoporre ai backup sui vari server.
Ogni incaricato deve collocare i propri documenti nelle apposite cartelle mappate su server.
Le operazioni di backup su n. 3 server windows e n. 1 server linux vengono effettuate giornalmente su nastro, e con cadenza settimanale viene effettuato un ulteriore backup automatico; i relativi nastri vengono depositati in una cassetta di sicurezza blindata antincendio presente nell'Ufficio Ragioneria;
Nella Biblioteca Comunale, esterna alla rete informatica comunale, le operazioni di backup vengono effettuate settimanalmente con procedura manuale.
Qualora l'incaricato non provveda a collocare i documenti nelle cartelle su server ma sul proprio Personal computer sarà responsabile dell'eventuale perdita dei dati dovuta a malfunzionamento o rottura della macchina.

c) sistema di monitoraggio
Attraverso appositi file di log presenti sul server è stato realizzato un sistema di controllo e verifica della sicurezza del sistema informatico. Tali file raccolgono le informazioni relative al funzionamento del Sistema Operativo del server, su eventuali virus e sull'invio e ricezione della posta elettronica.
Il sistema di controllo è in grado di registrare:

- gli accessi riusciti e falliti;
- gli accessi in lettura e scrittura;
- gli accessi in lettura e scrittura sui singoli archivi.

Attraverso apposito applicativo hardware/software viene implementato un sistema di log management per registrare gli accessi logici degli Amministratori di sistema ai sistemi stessi, permettendo che le registrazioni abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro

integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

d) controllo degli accessi
L'accesso diretto ai server è consentito esclusivamente al Responsabile, all'Amministratore di sistema, ai soggetti incaricati dallo stesso quali sostituti in caso di assenza, ai tecnici di società esterne che operano per l'Ente esclusivamente per il software di propria competenza.
L'accesso al server da parte dei tecnici di società esterne è consentito, esclusivamente per software di propria competenza o per interventi sulla rete informatica anche tramite collegamento diretto in teleassistenza previo accordi stipulati tra le parti e identificazione dei soggetti tramite apposite credenziali.
L'accesso alla rete informatica avviene esclusivamente attraverso un profilo di abilitazione che prevede per ciascun soggetto abilitato (di seguito utente) una propria identificazione tramite un nome utente (user-id) ed una password.
Per ciascun utente vengono definiti:

- il trattamento e/o gli archivi presenti sul server per cui viene data abilitazione di accesso;
- gli eventuali diritti di detta abilitazione (sola lettura, lettura e scrittura, ecc.).

A ciascun profilo di abilitazione è associato un gruppo di utenti che condividono gli stessi privilegi di accesso e di utilizzo.
Il custode delle password custodisce un elenco aggiornato contenente i nomi e le qualifiche degli utenti autorizzati.
Il Responsabile della ditta esterna incaricata dell'assistenza tecnica e sistemistica, hardware e software del Comune di Rossano Veneto, in qualità di Amministratore del sistema provvede:

- a definire il nome utente e la password per il primo accesso;
- a consegnare agli utenti il nome utente e la password assegnati;
- a definire i gruppi necessari per rispettare i privilegi di utilizzo.

Le password devono essere sostituite, non potendo più utilizzare le precedenti, con una frequenza non superiore a tre mesi mediante comunicazione all'utente in busta chiusa.

La definizione della password deve tener conto delle seguenti regole minime:

- deve essere alfanumerica, di non meno di otto caratteri;
- non deve essere composta utilizzando il nome utente;
- non deve essere ottenuta anagrammando la precedente.

Il nome utente e la password sono strettamente personali. L'utente è tenuto a non annotare la password stessa su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

La busta contenente le password verrà conservata in cassaforte blindata antincendio posta nell'Ufficio Ragioneria.
La violazione della segretezza della password costituisce infrazione grave alle disposizioni di sicurezza.

4.5 – Misure di sicurezza organizzative

a) controllo dei back up
Il Responsabile della ditta esterna incaricata dell'assistenza tecnica e sistemistica, hardware e software del Comune di Rossano Veneto, in qualità di Amministratore del sistema è chiamato a verificare la corretta esecuzione dei backup, a mantenere un elenco dei back up effettuati.

b) nomina degli incaricati
Il Responsabile provvede alla nomina degli incaricati per il trattamento dei dati informatici.
Qualora si faccia ricorso a soggetti esterni all'Ente per l'assistenza alla rete informatica con accesso a trattamento dei dati, il Responsabile provvede al relativo incarico definendo compiti e limiti dell'accesso.

c) individuazione dei rischi e prevenzione dei danni
Il Responsabile provvede ad informare tempestivamente gli incaricati:

- della presenza di virus nei personal computers in dotazione agli uffici;
- dell'utilizzo, da parte del personale, di procedure non conformi alle disposizioni sulla sicurezza;
- della periodica necessità di variazione della password;
- della disponibilità di programmi di aggiornamento relativi ad antivirus;
- del mancato rispetto di quanto previsto dalle norme contenute nel predetto documento.

In caso di continua inadempienza da parte degli incaricati il Responsabile provvederà a darne comunicazione scritta al Titolare.
Il Responsabile provvede ad organizzare iniziative per illustrare e diffondere gli accorgimenti da adottare in tema di sicurezza.

d) verifica ed aggiornamento del Documento sulla sicurezza
Il Responsabile provvede periodicamente:

- a presentare al Titolare una relazione sull'andamento dei processi relativi alla sicurezza;
- alla verifica delle norme contenute nel presente documento in rapporto all'efficacia delle contromisure adottate.

In particolare provvederà periodicamente a verificare:

- gli accessi fisici ai locali dove sono poste le apparecchiature server e/o dove si svolgono trattamenti informatici di qualsiasi genere;
- la corretta gestione dei codici identificativi personali e delle password;
- la corretta gestione dei profili di accesso degli incaricati;
- le procedure relative al controllo dell'integrità dei dati e al loro aggiornamento;
- la sicurezza delle trasmissioni in rete di dati personali;
- le modalità di conservazione dei back up;
- le modalità di ripristino dei back up;
- le modalità di reimpiego dei supporti di memorizzazione;
- il livello di formazione e il grado di apprendimento degli incaricati.
- l'operato dell'Amministratore del sistema con cadenza almeno annuale in modo da controllare la sua rispondenza alle misure organizzative tecniche e di sicurezza riguardanti i trattamenti dei dati personali.

Il Responsabile provvede ad aggiornare il presente documento a cadenza annuale e comunque ogni qualvolta si apportino consistenti variazioni al Sistema Informatico, alle strutture o a qualunque altro elemento o se ne dovesse ravvisare l'opportunità e/o la necessità in dipendenza di eventi non considerati nel documento stesso.

AREA FINANZIARIA

RESPONSABILE	PAN ZELIA

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
FINANZIARIA	contribuenti ici	C
	contribuenti pubblicità	C
	deliberazioni e determinazioni	C/S
	dichiarazioni e versamenti ici	C
	elenchi contribuenti tia	C
	elenco contribuenti tosap	C
	elenco clienti/fornitori	C
	elenco professionisti incaricati	C
	espositori fiera e manifestazioni diverse	C
	gestione economica personale	C/S
	ruoli fognatura e acqua	C
	versamenti ici esattoria	C

hardware	
PC	7
STAMPANTI	4

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
PROTOCOLLO	server / pc	Sesa Informatica	si	si
CONTABILITA' STIPENDI INVENTARIO	server	Kibernetes	si	si
PERSONALE - GESTIONE ACCESSI E CONTROLLO PRESENZE	server	Franco e Zoppello	no	si
ICI	pc	Gam Informatica	si	si
PERSONALE - E MENS	pc	Inps	no	si
PERSONALE - ENTRATEL - F24EP - UNICO ON LINE	pc	Agenzia Entrate	no	si
GESTIONE PRATICHE EDILIZIE	pc	Regione Veneto	no	si

PAGAMENTI F24	pc	Agenzia Entrate	no	no
PE - CATASTO	pc	Kibernetes	si	si

AREA AFFARI GENERALI - SERV. DEMOGRAFICI

RESPONSABILE	ORSO PAOLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
SERVIZI DEMOGRAFICI E STATISTICI	anagrafe e aire	C
	albo presidenti di seggio	C
	albo scrutatori	C
	deliberazioni e determinazioni	C / S
	elenco carte d'identità	C
	elenco giudici popolari	C
	elenco pensionati	C
	elenco titolari invalidi civili di provvid. econom. dal Ministero dell'Interno	C / S
	liste e tessere elettorali	C
	liste leva militare	C / S
	registri di stato civile	C / S
	registri libretti di lavoro	C
	ruoli matricolari	C / S
	stradario comunale	C

hardware	
PC	5
STAMPANTI	4

software

SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
ALBO WEB	server / pc	Grafice E. Gaspari	si	si
PROTOCOLLO	server / pc	Sesa Informatica	si	si
ANAG - AIRE	pc	Ministero Interno	no	si
ANAGRAFE POPOLAZIONE, STATO CIVILE, SERV. ELETTORALE, SERV. LEVA	server	Kibernetes	si	si
CNSD	pc	Ministero Interno	no	si
INA - SAIA	pc	Ministero Interno	no	si
PEC	pc	Regione Veneto	no	si

ISI - ISTATEL	pc	Istat	no	si

AREA AFFARI GENERALI - CENTRALINO - PROTOCOLLO - AMMINISTRAZIONE E SERV. SOCIALI

RESPONSABILE	ORSO PAOLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
AMMINISTRAZIONE SERVIZI SOCIALI	componenti commissioni comunali e amministratori	C
	ADI e SAD	C / S
	albo associazioni	C
	assegnatari aree ERP	C / S
	borse di studio	C
	elenco contributi regionali o statali scuola, affitti,canone telefonico, pasti caldi a domicilio	C / S
	elenco richiedenti contributi bonus elettrico/gas	C / S
	deliberazioni e determinazioni	C / S
	elenchi assegnatari assegno nucleo famigliare numeroso e maternità	C / S
	elenchi assegnatari provv. economiche non autosufficienti a domicilio	C / S
	elenco assegnatari contributi per malati di Alzheimer/assegno di cura	C / S
	scritture private concessioni cimiteriali	C
	elenco richiedenti alloggi Ater	C / S
	elenco soggiorni climatici portatori di handicap	C / S
	elenco utenti biblioteca	C
	elenco utenti telesoccorso e telecontrollo	C / S
	elenco utenti trasporto scolastico	C
	gestione giuridica personale	C / S
	registro di protocollo	C
	registro ditte camera di commercio	C
	registro per T.S.O.	C / S
	elenco bambini iscritti alle Scuole Materne paritarie Maria Bambina e Mottinello	C
	elenco bambini frequentanti centro infanzia/Sez. Primavera/scuola d'Infanzia	C / S

	elenco anziani cui si integra retta	C / S
	elenco minori in struttura	C / S
	contratti vari	C
	elenco utenti contributi straordinari e a sostegno minimum vitae	C / S
	elenco utenti contributo Regionale per abitazioni in locazione	C / S

hardware	
PC	12
STAMPANTI	7
FAX	1

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
PROTOCOLLO	server / pc	Sesa Informatica	si	si
PEC	pc	Provincia di Vicenza	no	si
CONTABILITA' ANAGRAFE	server	Kibernetes	si	si

AREA URBANISTICA EDILIZIA PRIVATA

RESPONSABILE	FARESIN GIANCARLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
URBANISTICA EDILIZIA PRIVATA	titolari licenze e concessioni edilizie, agibilità e abitabilità, ordinanze, abusivismo e cert. dest. urb., anagrafe tributaria, statistiche Istat	C
	catasto urbano e terreni	C
	deliberazioni e determinazioni	C / S
	PRG, piani urbanistici attuativi	C
	spotello unico	C

hardware	
PC	4
STAMPANTI	2
FAX	1

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD

OFFICE	server / pc	Microsoft	no	no
PROTOCOLLO	server / pc	Sesa Informatica	si	si
GEOMEDIA	pc	Regione Veneto	no	si
GESTIONE PRATICHE EDILIZIE	pc	Regione Veneto	no	si
AUTOCAD	pc	Computer e Uffici	no	no
ENTRATEL	pc	Agenzia Entrate	no	si
COLLAUDATORI	pc	Regione Veneto	no	si
PEC	pc	Regione Veneto	no	si
CONTABILITA' ANAGRAFE	server	Kibernetes	si	si

AREA GESTIONE TECNICA DEL TERRITORIO

RESPONSABILE	BONANNO CORRADO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
LAVORI PUBBLICI ECOLOGIA	ditte appaltatrici lavori pubblici	C
	deliberazioni e determinazioni	C / S
	professionisti incaricati	C
	proprietario immobili, allacciamento acquedotto	C
	registro autorizzazioni scarico	C

hardware	
PC	5
STAMPANTI	2
PLOTTER	1

software

SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
PROTOCOLLO	server / pc	Sesa Informatica	si	si
PROGETTAZIONE LAVORI PUBBLICI	pc	Acca	no	si
AUTOCAD	pc	Xteam	no	no
HI PROG 3	pc	Regione Veneto	no	no
CONTABILITA' ANAGRAFE	server	Kibernetes	si	si

AREA VIGILANZA

RESPONSABILE	ORSO PAOLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
VIGILANZA	autorizzazioni e licenze polizia amministrativa e temporanee	C
	contravvenzioni, rilevazioni incidenti, accertamento concessioni, ordinanze codice stradale	C / S
	registro cessioni fabbricati	C
	registro denunce stranieri art. 7 L. 286	C

hardware	
PC	4
STAMPANTI	4
FAX	1

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
GESTIONE CONTRAVVENZIONI	pc	Open Software	si	si
CESSIONE FABBRICATI	server / pc	Questura di Vicenza	no	no
CONTABILITA' ANAGRAFE	server	Kibernetes	si	si

ATTIVITA' ECONOMICHE

RESPONSABILE	FARESIN GIANCARLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
ATTIVITA' ECONOMICHE	autorizzazioni noleggio autoveicoli con conducente	C

	elenco autorizzazioni commercio areee pubbliche	C
	elenco autorizzazioni commercio fisso	C
	intestatari pubblici esercizi	C
	registro diploma esercizio professioni sanitarie	C
	registri acconciatori/estetisti	C
	registro tesserini invalidi	C/S
	registro forme speciali di vendita: dia distributori automatici, agenzie di affari, commercio di cose antiche usate, commercio elettronico, vendita al domicilio del consumatore, affittacamere	C
	registro matricole ascensori montacarichi	C
	registrio impianti privati e pubblici di distribuzione carburante	C

hardware	
PC	1
STAMPANTI	1

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
PROTOCOLLO	server / pc	Sesa Informatica	si	si
CESSIONE FABBRICATI	server / pc	Questura di Vicenza	no	no
ENTRATEL	pc	Agenzia Entrate	no	si
CONTABILITA' ANAGRAFE	server	Kibernetes	si	si

BIBLIOTECA

RESPONSABILE	ORSO PAOLO

FUNZIONE	BANCA DATI	DATI PERSONALI C= comuni S= sensibili
BIBLIOTECA	elenco utenti biblioteca	C

hardware	
PC	6

FOTOCOPIATORI E STAMPANTI	2

software				
SOFTWARE	SERVER/ PC	DITTA FORNITRICE	CONTRATTO MANUTENZIONE	PASSWORD
OFFICE	server / pc	Microsoft	no	no
ANTIVIRUS AVAST	pc	AVAST	no	si
FIREWALL GATEPROTECT - HARDWARE/SOFTWARE	pc	ACTS INFORMATICA	no	si

SERVER

SERVER HP	ML 350T G4, n. 2 processori Intel Xeon Processor 3.0 GHz/800-2 MB L2 , 512 MB MB PC2 – 3200 DDR2 SDRAM (400MHz), 6 slot disponibili, integrate d 2 MB Level 2 cache, hard disk 2 x 250GB, standard controller + 4 x 250GB, SATA aray controller opzionale, scheda di rete Embedded NC7761 PCI 10/100/1000T Gigabit network adapter, scheda grafica Integrated ATI RAGE XL Video Controller con 8 – MB SDRAM Video Memory VGA connector, floppy disk da 1.44 MB e cd – rom 48x IDE integrati. Sistema operativo Microsoft OEM windows 2003 server STD IT + 5 cal; Espansione memoria Hewlett Packard 2 x 512 MB PC2700 DDR 333;Controller ADAPTEC 1210SA Raid 0,1 SATA;Hewlett Packard Hard Disk Hot Plug SATA 160Gb 7200k/Rpm; Controller SCSI LSI Logic U80LVD 68 Pin per connessione DAT; Hewlett Packard DAT SURESTORE 72 GB Int SCSI, Storage works Ultrium tape drive 920 SCSI 400/800 Gb, controller SCSI.
SERVER HP	PL ML350TG4 XEON 3.2/1MBL2 512MB, ML350 G4 Redundant Fan Upgrade Kit, 2GB (1 x 2GB) ML350 G4 Only, 36.4 GB U320 15KRPM Univers. HotPlug, HP DAT 72H HOT PLUG for Proliant, ML350G4 XEON EM64T 3.2GHz/1MB L2, Microsoft OEM Windows 2003 Server Standard IT (Server + 5 CAL), Microsoft OEM Windows Server 2003 OEM ITA (5 CAL User), Microsoft ML-WIN TS CAL 2003 ITA EASY US, TREND MICRO CSS SMB ITA USER 10, Microsoft OEM Office 2003 PRO ITA OEM, n. 10 D-LINK Print Server Centronics-10/100 MBps. N. 1 ATLANTIS LAND Gigabit Switch Layer 2 with 5 10/100/1000Mbps ports, Standard, NWAY, Autopolarity, Autonegotiation, Flow control, Desktop design, Metal case.

SERVER HP	ML350T G6, processore Intel Xeon QC E5520 2.26 GHz, 2 processori base, disco fisso SATA/SAS da 2,5" (SFF), Memoria RAM base 3x 2GB 6GB, Controller on board HP Smart Array P410i/256MB controller (RAID 0,1,5),controller on board SAS / SATA con RAID, memoria RAM max up to 192GB, using PC3-8500R DDR3 Registered (RDIMM) memory, operating at 800MHz when fully populated at 2 DIMMs per Channel in 12 slots, alloggiamenti RAM (totali/disponibilità) 18/15, cache di secondo livello interna 4 MB (1 x 4 MB) di cache L3 (E5506/E5504/E5502/L5506), cache di secondo livello interna 4MB, 6 slot di espansione in totale, 1 PCI-Express x16 Gen2 (velocità x8), 1 PCI-Express x8 Gen2 (velocità x8), 4 PCI-Express x8 Gen2 (velocità x4), modulo di espansione opzionale PCI-X con 2 slot aggiuntivi PCI-X a 64 bit/100-MHz con 1 slot PCI Express singolo, scheda di rete, scheda Server a due porte Gigabit NC326i PCI Express integrata, unità ottica DVD-ROM SATA half-height HP, 1 porta seriale, 1 dispositivo di puntamento (mouse), 1 scheda grafica, 1 tastiera, 3 connettori di rete RJ-45 (1 dedicato per ProLiant Onboard Administrator), 6 porte USB 2.0 (2 posteriori, 2 frontali, 2 interne), alimentatore (1) 750 Watt Hot-Plug (Redundancy enabled) power supply, software certificato Windows, RHEL, SLES, NetWare, Oracle Enterprise Linux, VMware, and Citrix, gestione del sistema con password di avvio, password di setup, controllo interfaccia seriale, blocco configurazione disco, sicurezza interruttore di alimentazione, dimensioni (HxWxD) 21.7 x 44.5 x 55.7cm.
SERVER IBM	Processore fino a due Intel Pentium con bus a 800 MHz; cache di secondo livello integrata nel processore da 1 MB con a bordo 1 processore XEON da 3,2 GHz Alloggiamenti di espansione: sei slot PCI, Int. Video: controller video ATI Rage XL integrato 1024x768, 64K colori a 75Hz,Memoria: ECC quattro zoccoli DIMM PC-133 DIMM con capacità massimi di 4 GB con 1,5 GB installati, Ctrl. SCSI: Adaptec AHA-7899 Wide Ultra 320 SCSI controller dual channel integrato, Ctrl. SCSI: IBM ServerRAID Adapter, Ctrl. SCSI: Adaptec U320 per unità di backup, Alloggiamenti dischi fissi: tre vani disponibili ad alloggiamento comune per supporti rimovibili adatti per dispositivi di backup su nastro o per unità disco fisso, sei vani per mass storage hot-swap, con a bordo 3 dischi U320 da 36 GB U3 hot-swap in RAID 5 per una capacità totale disponibile di 70 GB, Unità di Backup: DAT SCSI 36/72 GB DDS5, Alimentazione: alloggiamento per alimentatore ridondante con 2 alimentatori installati, Collegamenti I/O: porta video, porta mouse, porta tastiera, due porte USB, una LAN 10/100/1000, una porta seriale. Sistema Operativo Linux RedHat ES 3Y, Runtime Cobol per 20 utenti codice PRM-1858.

hardware	
FOTOCOPIATORI DI RETE CON FUNZIONE DI STAMPANTE E SCANNER	3

	PROGRAMMI SU SERVER
DITTA/FORNITORE	
FRANCO E ZOPPELLO	GESTIONE ACCESSI E CONTROLLO PRESENZE

GRAFICHE E. GASPARI	ALBO WEB
ACTS INFORMATICA	MICROSOFT OFFICE
SE SA INFORMATICA	GESTIONE PROTOCOLLO
KIBERNETES	CONTABILITA', STIPENDI, INVENTARIO
KIBERNETES	ANAGRAFE POPOLAZIONE, STATO CIVILE, SERV. ELETTORALE, SERV. LEVA
ACTS INFORMATICA	FIREWALL GATEPROTECT - HARDWARE/SOFTWARE
ACTS INFORMATICA	ANTIVIRUS G DATA
QUESTURA DI VICENZA	CESSIONE FABBRICATI
ACTS INFORMATICA	LOG AMMINISTRATORI DI SISTEMA - HARDWARE/SOFTWARE

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

IL PRESIDENTE	IL SEGRETARIO COMUNALE
F.TO TREVISAN Gilberto	F.TO ORSO Dott. Paolo

N. 280 Reg. Pubbl.

REFERTO DI PUBBLICAZIONE
(Art. 124 D.Lgs. 267/2000)

Certifico io sottoscritto Segretario Comunale su conforme dichiarazione del messo che copia del presente verbale viene pubblicata il giorno **05/04/2011** all'albo pretorio ove rimarrà esposto per quindici giorni consecutivi.

Lì **05/04/2011**

IL SEGRETARIO COMUNALE
F.TO ORSO Dott. Paolo

CERTIFICATO DI ESECUTIVITÀ

☐ Si certifica che la presente deliberazione è stata pubblicata nelle forme di legge all'Albo Pretorio del Comune senza riportare nei primi dieci giorni di pubblicazione denunce di vizi di legittimità o competenza, per cui la stessa **É DIVENUTA ESECUTIVA il ..... ai sensi del 3° comma dell'art. 134 del D.Lgs. 18 agosto 2000, n. 267.**

– nei suoi confronti è intervenuto, nei termini prescritti, un provvedimento di sospensione/annullamento per cui la stessa **É DIVENUTA ESECUTIVA il** ..... ai sensi dell'art. 134 del D.Lgs 267/2000.

Lì .....

IL SEGRETARIO COMUNALE
.....
