COMUNE DI ROSATE

Provincia di Milano

Via Vittorio Veneto, 2 – 20088 Rosate (MI) – Tel. 02.90830.1 – Fax 02.908.48046

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 18 DEL 25/02/2016 COPIA

OGGETTO: APPROVAZIONE DEFINITIVA MANUALE PER LA GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

* *

Il giorno **25/02/2015** alle ore **17.30** presso questa sede comunale, convocati con avviso scritto del Sindaco, consegnato a norma di Legge, i Signori Assessori comunali si sono riuniti per deliberare sulle proposte di deliberazione iscritte all'ordine del giorno.

Assume la presidenza il Sindaco, **DANIELE DEL BEN**, assistito dal Segretario Comunale **DOTT.SSA MARIA BASELICE**.

Dei Signori componenti la Giunta comunale di questo Comune:

Presenti	Assenti
DEL BEN DANIELE	
VENGHI CLAUDIO	
ORENI MONICA	
CRESPI ALESSANDRO	
LIBERALI MARIO	

Membri ASSEGNATI 5 PRESENTI 5

Il Presidente, accertato il numero legale per poter deliberare validamente, invita la Giunta Comunale ad assumere le proprie determinazioni sulla proposta di deliberazione indicata in oggetto.

LA GIUNTA COMUNALE

Vista la seguente relazione-proposta:

VISTO il DPR 28/12/2000, n.445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" ed, in particolare, il terzo comma dell'art. 50 che prevede l'obbligo per le Pubbliche Amministrazioni di "realizzare ed revisionare sistemi informatici ed automatizzati finalizzati alla gestione del Protocollo informatico e dei procedimenti amministrativi" in conformità alle disposizioni contenute nello stesso Testo unico ed alle disposizioni di legge sulla riservatezza dei dati personali, nonché dell'art. 15 della Legge. 15/3/97, 'n. 59 e dei relativi regolamenti di attuazione;

VISTI:

- Visto il DPCM 31/10/2000 concernente "Regole tecniche per il protocollo informatico di cui al DPR 20/10/98, n.428 (sostituito dal sopracitato DPR 445/2000)", in particolare l'art.5 che prevede espressamente l'obbligo per le pubbliche amministrazioni di redigere un Manuale per la Gestione del protocollo informatico, dei flussi documentali e dell'archivio e ritenuto che questo manuale deve essere considerato come un valido strumento di lavoro per la gestione dei documenti e dei procedimenti amministrativi, in quanto descrive tutte le fasi operative del sistema per la gestione del protocollo informatico individuando, altresì, per ogni azione o processo i rispettivi livelli di esecuzione, responsabilità e controllo;
- la Direttiva del 9/12/2002 del Ministro per l'innovazione e le tecnologie recante "Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali";
- il DPCM 14/10/2003 pubblicato sulla G.U. del 25/10/2003, concernente l'"Approvazione delle Linee guida per l'adozione del Protocollo informatico e per il trattamento informatico dei procedimenti amministrativi";
- il Codice dell'Amministrazione Digitale – CAD – approvato con D. Lgs. n. 82/2005 nel testo coordinato e aggiornato con le modifiche ed integrazioni introdotte dal D.Lgs. 30/12/2010, n.235;
- il DPCM 03/12/2013 ad oggetto "Regole Tecniche per il protocollo informatico ai sensi degli articoli 40 – bis, 41, 47, 57 – bis e 71 del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005;
- il DPCM 13/11/2014 avente ad oggetto "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71 del Codice dell'amministrazione digitale di cui al D.Lgs. n. 82/2005;

RILEVATO CHE, ai sensi delle norme sopracitate, le Pubbliche Amministrazioni devono:

a) adottare il Protocollo informatico per la registrazione dei dati e documenti;
b) formare e conservare i documenti informatici sulla base delle deliberazioni dell'AIPA (ora Agenda Digitale per l'Italia) - Autorità informatica della Pubblica Amministrazione, n.51/2000 e n.42/2001;
c) realizzare la sottoscrizione elettronica dei documenti informatici;
d) gestire in forma informatica il sistema ed i flussi documentali sulla base delle Deliberazioni dell'AIPA n.51/2000 e n.42/2001 e del DPR 445/2000, artt. 64,65 e 66;
e) realizzare gli accessi telematici ai dati, ai sistemi ed alle banche dati sulla base delle indicazioni del DPR 445/2000, artt.58,59 e 60;
f) individuare le Aree Organizzative Omogenee (AOO) per la gestione del Protocollo informatico e dei flussi documentali e i relativi Uffici di riferimento;
g) nominare il Responsabile delle attività relative alla tenuta del Protocollo informatico, della gestione dei flussi documentali e degli Archivi;
h) adottare il Manuale di gestione dei documenti previsto dalle Regole tecniche di cui al DPCM 31/10/2000, che descrive il sistema di gestione e dì conservazione dei documenti e fornisce le istruzioni necessarie al corretto funzionamento del Protocollo informatico;
i) realizzare la sicurezza dei dati, dei documenti e delle tecnologie sulla base delle disposizioni del Codice in materia di dati personali (D.Lgs. 30/6/2003, n. 196);

j) ottemperare alla Direttiva sulla formazione del Ministro per la Funzione pubblica del 13/12/2001;
k) effettuare le comunicazioni di cui alla Direttiva del Ministero per l'innovazione e le tecnologie del 9/12/2002;

VISTA la deliberazione della Giunta Comunale n. 95 del 15/10/2015, esecutiva a tutti gli effetti di legge, con la quale:
- viene individuata un'unica Area Organizzativa Omogenea (AOO), per la gestione dei documenti e dei flussi documentali dell'amministrazione, denominata "Comune di Rosate" ai sensi dell'art.50 comma 4 del DPR 28/12/2000 n.445,
- viene individuato, ai sensi dell'art. 3 coma 1, lett.b) del DPCM 03/12/2013, nel Responsabile del Settore 1 – Area Servizi, Dott.ssa Adele Simonetta Panara, il Responsabile della Gestione Documentale e, quale vicario in sua sostituzione la posizione organizzativa a cui verranno delegate le funzioni sostitutive;

RICHIAMATA la deliberazione della Giunta Comunale nr. 96 del 15/10/2015, esecutiva a tutti gli effetti di legge, con la quale si è provveduto ad approvare il Manuale per la Gestione del Protocollo Informatico, dei Flussi Documentali e degli Archivi, composto da nr. 14 sezione e nr. 12 allegati regolarmente trasmesso a mezzo posta elettronica certificata alla Soprintendenza Archivistica della Lombardia in data 06/11/2015 – prot.nr. 8334;

DATO ATTO che la Soprintendenza Archivistica della Lombardia:
- con propria nota del 18/11/2015 – prot. nr. 8923 – ha invitato il Responsabile del servizio archivistico del Comune di Rosate a presenziare, in data 15/01/2016, ad un incontro formativo e di confronto sui contenuti del manuale di gestione,
- a seguito del suddetto incontro formativo, in data 08/02/2016, prot nr. 907, ha rilasciato la prescritta autorizzazione all'utilizzo del Manuale di gestione redatto ai sensi degli artt. 3 e 5 DPCM 03/12/2013

RAVVISATA, pertanto, la necessità di provvedere alla modifica del Manuale di Gestione del protocollo informatico in base alle indicazioni impartite durante l'incontro formativo presso la Soprintendenza Archivistica della Lombardia;

Visto il testo definitivo dell'allegato Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi, composto da nr. 15 sezione e nr. 12 allegati, che forma parte integrante e sostanziale del presente provvedimento;

Tenuto conto che il Manuale di Gestione del protocollo informatico dovrà essere periodicamente aggiornato e rivisto, in particolare in occasione di modifiche normative e di acquisizione di nuove tecnologie;

Ritenuto opportuno procedere all'approvazione del suddetto Manuale di Gestione del protocollo informatico;

Acquisito il parere favorevole espresso, ai sensi dell'art. 49, comma 1, del D. Lgs.n. 267/2000, del Responsabile del Settore, in ordine alla regolarità tecnica, atteso che il presente provvedimento non comporta di per sé spese a carico del bilancio;

Tutto ciò premesso,

Con voti unanimi, legalmente espressi,

DELIBERA

1) Di approvare in via definitiva, per le motivazioni di cui in premessa che qui si intendono integralmente riportate e trascritte il Manuale di Gestione del Protocollo informatico, dei

flussi documentali e degli archivi, composto da nr. 15 sezione e nr. 12 allegati, che forma parte integrante e sostanziale del presente provvedimento;

2) Di dare atto che il Manuale di Gestione è strumento di lavoro necessario alla corretta tenuta del protocollo ed alla gestione del flusso documentale e dell'archivio e, pertanto, dovrà essere aggiornato quando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiedano o, comunque, ogni qualvolta si renda necessario alla corretta gestione documentale;

3) Di confermare, ai sensi dell'art. 3, comma 1, lett. b) del DPCM 03/12/2013, la Dott.ssa Adele Panara Simonetta, Responsabile del Settore 1 – Area Servizi Amministrativi, quale Responsabile della Gestione Documentale, come da deliberazione GC nr. 95 del 15/10/2015 e di nominare, quale Vicario in sua sostituzione, la Dott.ssa Annalisa Fiori, Responsabile del Settore 3 – Area Servizi alla Persona;

4) Di provvedere alla pubblicazione del Manuale sul sito internet del Comune;

5) Di trasmettere copia della presente deliberazione alla Sovrintendenza Archivistica per la Lombardia;

6) Di disporre che il presente atto venga trasmesso ai Capigruppo Consiliari, ai sensi dell'art.125, comma 1, del D.Lgs. n.267/2000 e pubblicato contestualmente all'albo pretorio online.

Quindi, riconosciuta l'urgenza di provvedere all'approvazione del Manuale di Gestione del Protocollo Informatico, con voti unanimi, espressi nei modi e forme di legge

DELIBERA

di dichiarare la presente deliberazione immediatamente eseguibile ai sensi del comma 4 dell'art. 134, del D. Lgs. n. 267 del 18/08/2000.

Allegato delibera ~~C.C.~~/G.M.
n. 18 del 25/2/2016

Comune di Rosate

(Provincia di Milano)

Manuale di Gestione del Protocollo Informatico, dei Documenti e dell'Archivio

(DPCM 3/12/2013 e DPCM 13/11/2014)

Approvato con deliberazione di Giunta Comunale n. _____ del _____

SOMMARIO **pagina**

SEZIONE 1
DISPOSIZIONI GENERALI

1.1 - Ambito di applicazione

Il presente manuale è adottato ai sensi della normativa vigente (all. n.1) per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti del Comune di Rosate.

1.2 - Definizioni dei termini

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al glossario allegato al DPCM 3/12/2013 (all. n.2).

1.3 Area organizzativa omogenea (AOO)

Ai fini della gestione dei documenti, è individuata una sola **Area Organizzativa Omogenea (A.O.O.)** denominata "Comune di Rosate".
Ai sensi dell'art.50, comma 4 del DPR 445/00, per AOO si intende un insieme di uffici da considerare ai fini della gestione unica e coordinata dei documenti, che assicuri uniformità di classificazione, archiviazione e comunicazione interna.
Per il Comune di Rosate l'AOO è composta dall'insieme di tutte le sue unità organizzative, di cui all'elenco dell'allegato. n.3, alla quale è associato un unico registro di protocollo e una sola casella di posta elettronica certificata dedicata alla ricezione di flussi documentali in formato digitale. Il codice identificativo dell'area è c_h560.
Per qualsiasi informazione statistica relativa all'Amministrazione Comunale si rimanda alle pagine del sito www.comune.rosate.mi.it.

1.4 Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

Nell'ambito dell'AOO, ai sensi dell'art.61, comma 1 del DPR n.449/00, è istituito il Servizio per la tenuta del Protocollo Informatico, la Gestione dei flussi documentali e degli archivi. Con deliberazione di Giunta Comunale nr. 95 del 15/10/2015, è stato individuato, ai sensi dell'art. 3 coma 1, lett.b) del DPCM 03/12/2013, nella persona del Responsabile del Settore 1 – Area Servizi, la Dott.ssa Adele Simonetta Panara, il Responsabile della Gestione Documentale e, quale vicario in sua sostituzione la posizione organizzativa a cui verranno delegate le funzioni sostitutive;
Ai sensi della Deliberazione CNIPA numero 11/04, articolo 5, il responsabile del servizio archivistico svolge le funzioni di Responsabile della conservazione ed è specificamente considerato pubblico ufficiale. Durante l'assenza del responsabile ne svolge le funzioni un sostituto.
Al Responsabile della gestione documentale sono affidati i compiti di cui all'art.61 comma 3 del DPR 445/00 e all'art.4 del DPCM 3/12/2013 "Regole tecniche per il Protocollo Informatico", in particolare:

a) attribuisce i livelli di autorizzazione per l'accesso alle funzioni del Sistema di Gestione Informatica dei Documenti;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
c) cura, di concerto con il Servizio Informatico, che le funzionalità del sistema, in caso di guasti o anomalie, vengano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
d) autorizza l'utilizzo del registro di emergenza per le registrazioni di protocollo, nei casi e secondo le modalità previste dall'art.63 del DPR n.445/00;
e) autorizza l'annullamento delle registrazioni di protocollo secondo quanto disposto dall'art.54 del DPR n.445/00;
f) assicura la corretta produzione del registro giornaliero di protocollo e la sua trasmissione al sistema di conservazione entro la giornata lavorativa successiva

secondo quanto disposto dall'art.7, comma 5 del DPCM 3/12/2013 " Regole tecniche per il protocollo informatico"

f) predispone ed aggiorna, d'intesa con il Responsabile della sicurezza informatica ed il Responsabile per il trattamento dei dati personali, il Piano per la sicurezza informatica;
g) cura, di concerto con il Servizio Informatico, la conservazione delle copie di cui alla normativa vigente in luoghi sicuri differenti;
h) garantisce il buon funzionamento del Sistema di Gestione Informatica dei documenti, la formazione e la gestione dell'archivio digitale del'Ente, nonché la corretta conservazione degli archivi cartacei dell'Ente;
i) vigila sull'osservanza delle disposizioni del presente Manuale di gestione da parte del personale autorizzato e degli incaricati;
j) cura, ai sensi della normativa vigente4, il trasferimento dei documenti dagli uffici agli archivi e la conservazione degli archivi medesimi;
k) cura il costante aggiornamento del presente Manuale di gestione e di tutti i suoi allegati.
l) cura la pubblicazione del presente manuale sul sito istituzionale del Comune;

1.5 - Unicità del protocollo informatico

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette numeri, tuttavia a norma dell'art.53, comma 5 del decreto del Presidente della Repubblica n.445/2000, sono possibili registrazioni particolari (all. n.4). Il sistema informatico di gestione del protocollo è sincronizzato per il calcolo dell'ora con il server di sistema. L'Amministrazione non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (all. n.4). Ad ogni documento è attribuito un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

1.6 - Modello operativo adottato per la gestione dei documenti

Per la gestione dei documenti è adottato un modello operativo parzialmente decentrato che prevede la partecipazione attiva di più soggetti ed uffici abilitati a svolgere soltanto le operazioni di loro competenza di cui all'elenco allegato (all. n.3): infatti, solo il personale del Servizio Protocollo è abilitato a svolgere le operazioni di protocollazione in entrata; mentre, al fine di snellire lo svolgimento delle pratiche e delle procedure, la protocollazione in partenza viene demandata ai singoli servizi dei vari settori dell'Ente, sia per i documenti informatici che per i documenti cartacei; in quest'ultimo caso, il documento viene acquisto all'interno della procedura di protocollazione con i dati della segnatura di protocollo e, successivamente stampato dall'operatore per l'invio al destinatario. I dati in entrata e quelli in uscita sono gestiti dalle unità operative di cui all'all. n.3.

1.7 – Sistema di Gestione Informatica dei Documenti

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo del *server* che ospita i *file* utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al *server* del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato

1.8 - Titolario di classificazione

La classificazione è un'attività di organizzazione logica di tutti i documenti correnti, protocollati e non (spediti, ricevuti, interni), secondo uno schema di voci che identificano attività e materie specifiche del soggetto produttore.
Il sistema complessivo di organizzazione dei documenti è definito nel titolario di classificazione (All.5)
Lo scopo del titolario di classificazione è quello di guidare l'archiviazione dei documenti in base alle funzioni ed alle materie di competenza dell'ente e si suddivide in titoli, classi e sottoclassi. La classificazione collega ciascun documento in maniera univoca ad una precisa unità archivistica: il fascicolo.
Il DPR 445/2000, articolo 64, comma 4, individua nella classificazione il mezzo per consentire la corretta organizzazione dei documenti, presupposto per il corretto svolgimento dell'attività amministrativa e garanzia del diritto d'accesso ai documenti amministrativi riconosciuta dalla legge 241/1990.

SEZIONE 2
FORMAZIONE DEI DOCUMENTI

2.1 - Disposizioni generali sulla produzione dei documenti

Ai sensi dell'art.22 comma 1. lettera d) della L.241//90 per documento amministrativo si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, formati dalle pubbliche amministrazioni o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.
In base al tipo di supporto e di modalità di formazione, i documenti amministrativi possono essere analogici o informatici.
Per documento analogico si intende un documento amministrativo prodotto su supporto non informatico, di norma su supporto cartaceo.
L'originale è analogico, cartaceo e dotato di firma autografa.
Per versione informatica del documento analogico si intende copia del documento su supporto informatico.
Per versione analogica di documento informatico si intende la copia cartacea di un documento prodotto su supporto informatico.
Ai sensi dell'art.1 comma 1, lettera p), del D.Lgs n.82/05 per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Ai sensi dell'art.23-ter del D.Lgs n.82/05 per documenti amministrativi informatici si intendono, gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonchè i dati e i documenti informatici detenuti dalle stesse.
Il Comune, conformemente a quanto sancito dall'art.3 del D. Lgs n. 39/93, nello svolgimento delle proprie attività, predispone i propri atti utilizzando sistemi informativi automatizzati.
Il Comune di Rosate, nell'ottica di una progressiva dematerializzazione della propria attività amministrativa, procede ad una graduale riduzione dei documenti cartacei da esso prodotti, fino a giungere alla formazione degli originali dei propri documenti esclusivamente in modalità digitale, entro e non oltre l'11/08/2016.

I documenti prodotti dal Comune, i cui originali siano su supporto informatico, sono prodotti nel rispetto delle regole tecniche emanate ai sensi dell'art.71 del D.Lgs n.82/05 conformemente alle modalità previste dal presente manuale.

2.2 - Informazioni minime del documento cartaceo prodotto dal Comune

Le informazioni minime presenti nei documenti cartacei prodotti dal Comune di Rosate sono le seguenti:

- denominazione e stemma dell'amministrazione, *comprensiva del codice fiscale o partita IVA e del codice identificativo di cui all'articolo n. 1.3;*
- indicazione dell'AOO e del settore, servizio o ufficio che ha prodotto il documento;
- indirizzo completo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica certificata dell'ente);
- indicazione del luogo, giorno, mese, anno di formazione;
- destinatario, per i documenti in partenza;
- oggetto del documento, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- riferimenti ad eventuali documenti precedenti;
- indice di classificazione (categoria, classe e fascicolo);
- numero degli allegati, se presenti;
- numero di protocollo;
- testo;
- indicazione dello scrittore del documento (nome e cognome anche abbreviato);
- estremi identificativi del responsabile del procedimento (L. 241/90);
- sottoscrizione autografa o elettronico/digitale del responsabile, e/o del Responsabile di procedimento.

2.3 - Produzione documenti informatici

I documenti informatici sono prodotti dal Comune di Rosate attraverso l'utilizzo di appositi strumenti software o mediante estrazione e raggruppamento di dati provenienti dalle basi gestite dall'Ente.

I documenti informatici prodotti dal Comune contengono le informazioni minime elencate nel precedente articolo2.2, ad eccezione di quelli sottoscritti con firma digitale; questi ultimi non riportano visualizzati il numero e la data di protocollo in quanto il documento, al momento della registrazione, è già perfezionato e non è consentita la modifica attraverso l'inserimento successivo di dati; sarà il Sistema di Gestione Informatica di documenti SGID a mantenere il collegamento tra il documento ed il numero di protocollo assegnato.

I formati elettronici utilizzati dal Comune di Rosate per la produzione di documenti informatici, anche ai fini della conservazione:

- sono conformi a quanto disposto dall'allegato 2 al DPCM 3/12/2013;
- sono aperti, completamente documentati e preferibilmente riconosciuti come standard da organismi internazionali;
- sono indipendenti sa specifiche piattaforme tecnologiche hardware e software;
- non possono comunque contenere macroistruzioni o codice eseguibile;
- sono ampiamente adottati;
- sono preferibilmente stabili e non soggetti a continue modificazioni nel tempo;
- sono preferibilmente utilizzabili con versioni precedenti e successive dell'applicativo software che li ha prodotti;
- sono privi di meccanismi tecnici di protezione che possano impedirne la replica del contenuto su nuovi supporti o la possibilità di effettuare migrazioni pregiudicandone la fruibilità nel lungo periodo a causa dell'obsolescenza tecnologica;
- permettono la fruizione anche ad utenti diversamente abili;

Il documento informatico prodotto dal Comune presenta la caratteristica di immodificabilità in modo tale che forma e contenuto dello stesso non siano alterabili durante

2.4 - Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici prodotti dal Comune di Rosate avviene in conformità a quanto previsto dal D.lgs n.82/05 e dal DPCM 22/02/2013 " Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali";

Per **firma digitale** (cosiddetta "firma digitale forte" o "firma elettronica avanzata") si intende, a norma dell'art. 1 c.1, lett. N) del DPR 445/2000 e dell'art. 1, comma 1, lettera S del D. Lgs 82/2005, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le chiavi devono essere certificate con la procedura di cui all'art. 27 del D. Lgs 82/2005.

In particolare, la certificazione di una chiave pubblica da parte di una autorità di certificazione garantisce la corrispondenza della chiave con il soggetto che la espone.

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle suddette regole tecniche, emanate ai sensi dell'art.20 comma 3 e dell'art.71 del D.Ls n.82/05 che garantisca, pertanto, l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha efficacia della scrittura privata prevista dall'art. 2702 del Codice Civile;

I documenti informatici prodotti dal Comune di Rosate nello svolgimento della propria attività istituzionale sono sottoscritti dai Responsabili del procedimento con firma digitale conforme alla normativa vigente, acquistate da certificatore accreditato (all. n.6).

Il dispositivo per la generazione della firma digitale è usato esclusivamente dal titolare designato dal Comune; ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria;

Il titolare del dispositivo di firma digitale, conformemente a quanto previsto dall'art.8 comma 5 del DPCM 22/02/2013:

- assicura al custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal certificatore alfine di adempiere agli obblighi di cui all'art.32 comma 1 del D.lGS.82/05;
- conserva le informazioni di abilitazione all'uso delle chiave privata separatamene dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute nel dispositivo sicuro per la generazione della firma digitale inutilizzabile o di cui abbia perduto il possesso o il controllo esclusivo;
- richiede immediatamente la revoca del certificato qualificato relativo alle chiavi contenute nel dispositivo sicuro per la generazione della firma digitale qualora abbia il ragionevole dubbio che possa essere usato da altri.

Per **firma elettronica** (cosiddetta "firma digitale debole") si intende, ai sensi dell'art. 2, c. 1, lett. a) del D.Lgs.10/2002, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Essa assicura solo la provenienza del documento e non l'integrità del contenuto.

2.5 - Tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche

Le eventuali modifiche alle tipologie di documentazione sottoposta a trattamento specifico e a registrazione particolare sono evidenziate nell'allegato elenco (all. n.4).

Per quanto riguarda un quadro generale di casi che possono creare dubbi sull'opportunità della protocollazione, si rimanda alla Sezione 5 "Documentazione particolare".

SEZIONE 3
RICEZIONE DEI DOCUMENTI

3.1 - Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

a) il servizio postale;
b) la consegna diretta all'Ufficio Protocollo dell'Ente;
c) l'apparecchio telefax dell'ufficio protocollo.

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione. Quelli pervenuti via telefax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei.

In presenza di un sistema informatico che ne consente l'acquisizione in formato elettronico si applicano le procedure previste per la ricezione dei documenti informatici.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema ha già attribuito ad altri documenti, anche se questi sono strettamente correlati tra loro.

Non è pertanto consentito, in nessun caso, l'utilizzo di un unico numero di protocollo per il documento in arrivo e il documento in partenza. La documentazione che non è stata registrata in arrivo o in partenza viene considerata giuridicamente inesistente per l'Amministrazione.

3.2 - Ricezione dei documenti informatici

Ai sensi dell'art.45 comma 1 del D.Lgs 82/2005, i documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

Al fine di soddisfare il suddetto requisito, i documenti informatici sono, di norma, acquisiti dal Sistema di Gestione Informatica del Comune di Rosate, mediante:

- la casella di posta elettronica certificata (PEC) collegata al servizio protocollo e archivio;
- il fax server qualora utilizzato dall'AOO;
- la posta elettronica certificata garantisce la certezza della provenienza e l'integrità dei documenti ricevuti.

La casella PEC attivata dal comune di Rosate è comunicata all'agenzia per l'Italia Digitale (Agid) al fine di essere inserita nell'indice delle Pubbliche Amministrazioni (IPA) avendo cura di comunicare tempestivamente con cadenza semestrale le variazioni, secondo quanto previsto dall'art.57-bis del D.Lgs 82/05.

La suddetta casella di posta elettronica certificata è integrata funzionalmente con il Sistema di gestione Informatica dei documenti, in modo tale che si formi una "coda" della corrispondenza in arrivo che permetta la registrazione di protocollo e l'acquisizione sul Sistema di tutti i documenti ricevuti. Tale "coda" sarà accessibile al personale autorizzato dal responsabile della gestione documentale.

Qualora i documenti pervenuti tramite PEC siano le ricevute di avvenuta consegna rilasciate dal gestore del servizio di posta elettronica certificata relative a documenti spediti dall'AOO o i messaggi di ritorno generati automaticamente da sistemi di gestione documentale delle amministrazioni destinatarie di una spedizione,il Sistema procede automaticamente alla loro archiviazione, collegandoli alla registrazione di protocollo cui si riferiscono. Le ricevute di posta elettronica certificata che si riferiscano a situazioni di anomalia, come ad esempio, il mancato recapito di una spedizione, sono notificate dal SGID.

I documenti informatici provenienti da altre pubbliche amministrazioni possono essere recapitati al comune di Rosate sia attraverso la suddetta casella di PEC, sia utilizzando i meccanismi dell'interoperatività e della cooperazione applicata di cui al Sistema Pubblico di Connettività (SPC), utilizzando le informazioni contenute nella segnatura di protocollo, nel rispetto di quanto previsto dalla normativa vigente.

Il Comune di Rosate si avvale dell'utilizzo di dispositivo di fax server, funzionalmente integrato con il Sistema di Gestione Informatica dei documenti.

Qualora si verifichi il caso in cui un documento informatico, soggetto alla registrazione di protocollo, pervenga agli uffici del Comune utilizzando una modalità diversa da quelle esposte precedentemente, ad esempio la consegna diretta del documento memorizzato su un supporto removibile, o tramite l'inoltro di una casella di posta elettronica convenzionale, (quale, ad esempio, CD ROM, DVD, pen drive, etc,) il personale che riceve tale documento procede alla sua valutazione e, accertatane la provenienza, lo inoltra all'ufficio protocollo per la relativa registrazione.

3.3 - Ricevute attestanti la ricezione dei documenti

La ricevuta della consegna di un documento cartaceo può essere costituita dalla fotocopia del primo foglio del documento stesso con un timbro che attesti il giorno della consegna.
A chi ne fa domanda, compatibilmente con le esigenze del servizio, deve essere anche riportato il numero di protocollo assegnato al documento, in questo caso l'operatore deve provvedere immediatamente alla registrazione dell'atto.

3.4 - Apertura della posta

Il servizio Protocollo apre tutta la corrispondenza cartacea pervenuta all'ente salvo nei casi in cui sulla busta sia riportata la dicitura "personale" o "riservata", compresa la posta elettronica certificata.
La posta elettronica individuale è gestita dai singoli titolari.

3.5 Conservazione delle buste o altri contenitori di documentazione

Le buste dei documenti analogici pervenuti non si inoltrano agli uffici destinatari. Le buste delle assicurate, corrieri, espressi, raccomandate ecc. si inoltrano insieme ai documenti.

3.6 - Orari di apertura per il ricevimento della documentazione cartacea

L' Ufficio Protocollo riceve la documentazione negli orari di apertura al pubblico pubblicati sul sito internet comunale.

SEZIONE 4
REGISTRAZIONE DEI DOCUMENTI

4.1- Documenti soggetti a registrazione di protocollo

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.

4.2 - Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:

- gazzette ufficiali;
- bollettini ufficiali, notiziari della pubblica amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico e certificazioni anagrafiche;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti i documenti che per loro natura non rivestono alcuna rilevanza giuridico - amministrativa presente o futura;

Tutti quei documenti già soggetti a registrazione particolare da parte dell'ente, il cui elenco è allegato al presente manuale (all. n.4).

4.3 - Registrazione di protocollo dei documenti ricevuti e spediti

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e numero di protocollo dei documenti ricevuti, se disponibili;
f) impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
g) classificazione: categoria, classe, fascicolo (si veda titolario all. n.5);
h) assegnazione;

Inoltre possono essere aggiunti:
i) data di arrivo;
j) allegati (numero e descrizione);
k) estremi provvedimento differimento termini di registrazione;
l) mezzo di ricezione/spedizione (lettera ordinaria, prioritaria, raccomandata, corriere,fax ecc.);
m) ufficio di competenza;
n) tipo documento;
o) livello di riservatezza:
p) elementi identificativi del procedimento amministrativo, se necessario.

4. 4 - Registrazione dei documenti interni

Di norma i documenti prodotti dall'Ente a solo uso interno non vengono protocollati. Nel caso in cui sia necessario dare valenza giuridico-probatoria a documenti che costituiscono atti preparatori (pareri tecnico-legali), essi potranno essere protocollati.

4.5 - Segnatura di protocollo

La segnatura di protocollo è effettuata contemporaneamente all'operazione della registrazione di protocollo; essa consiste nell'apposizione o nell'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.
La segnatura di protocollo di un documento cartaceo avviene mediante l'apposizione su di esso di un timbro sul quale siano riportate le seguenti informazioni: codice identificativo dell'amministrazione;
a) denominazione e codice identificativo dell'AOO;
b) data e numero di protocollo del documento;
c) indice di classificazione.

L'operazione di segnatura di protocollo dei documenti informatici è effettuata contemporaneamente all'operazione di registrazione di protocollo e persegue il fine di favorire l'interoperabilità tra i diversi sistemi di gestione documentale, riportandole informazioni archivistiche fondamentali, in modo da facilitare il trattamento da parte del ricevente.
I dati relativi alla segnatura di protocollo di un documento trasmesso dal Comune sono associati al documenti stesso e contenuti in un file XML conforme alle specifiche di cui alla circolare AgiD n.60 del 23/01/2023 "Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni".
Tali dati sono specificati negli artt. 9 e 21 del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico" e sono i seguenti:

a) codice identificativo dell'amministrazione;
b) codice identificativo dell'AOO;
c) codice identificativo del registro;
d) data di protocollo;
e) numero di protocollo;

f) oggetto
g) mittente
h) destinatario o destinatari.

Per quanto riguarda i documenti protocollati in uscita, nella signatura di protocollo possono essere specificate altresì, una o più delle seguenti informazioni incluse anch'esse nello stesso file XML:
-indicazione della persona o dell'ufficio interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.
L'Amministrazione che riceve il suddetto file XML utilizzerà le informazioni in esso contenute per eseguire, eventualmente anche in forma autorizzata, la registrazione di protocollo del documento in entrata e per avviarlo alla UOR competente al trattamento.

4.6 - Annullamento delle registrazioni di protocollo

Ai sensi della normativa vigente l'eventuale annullamento e/o la modifica anche di uno solo dei dati obbligatori della registrazione di protocollo, devono essere autorizzate, su specifica nota motivata, dal Responsabile della gestione documentale.
Le informazioni relative alle registrazioni annullate e/o modificate rimangono memorizzate nella procedura di protocollo informatico unitamente alle informazioni relative all'ora, alla data, al nominativo dell'operatore che effettua l'operazione ed agli estremi del provvedimento di autorizzazione. Sui documenti cartacei è apposto un timbro che riporta gli estremi del verbale di annullamento. L'annullamento del numero di protocollo comporta l'annullamento di tutta la registrazione di protocollo.

4.7 - Differimento dei termini di protocollazione

Di norma la registrazione della documentazione pervenuta avviene nell'arco della giornata o nella successiva giornata lavorativa a quella di ricezione. Eccezionalmente, in presenza di situazioni che lo rendano necessario, come un imprevisto carico di lavoro che non permetta di effettuare le registrazioni di protocollo nella stessa giornata lavorativa e qualora, a causa di tale condizione, possa venir meno un diritto di terzi, il Responsabile della gestione documentale, con apposito provvedimento motivato, può autorizzare il differimento della registrazione di protocollo dei documenti ricevuti, fissando un limite di tempo entro cui le registrazioni dovranno essere effettuate e conferendo valore, nel caso di scadenze predeterminate, alla data di arrivo dei documenti. Tutte le registrazioni di protocollo che vengono differite devono riportare gli estremi del suddetto provvedimento di autorizzazione.

4.8 - Registro giornaliero e annuale di protocollo

Il Responsabile della Gestione documentale provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni, inserite dall'operatore di registrazione di protocollo nell'arco di uno stesso giorno, ivi comprese quelle modificate e annullate in quella medesima data. Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili, i quali sono conservati in luogo sicuro a cura di un soggetto diverso, ai sensi dell'art.7. comma 5, del DPCM 31 ottobre 2000, dal RSP ed appositamente nominato.

4.9- Registro di emergenza

Qualora si verificassero interruzioni, accidentali o programmate, nel funzionamento del sistema di protocollo informatico, l'AOO è tenuta, ai sensi della normativa vigente, ad effettuare le registrazioni di protocollo su un registro di emergenza (All.8) in forma cartacea oppure in forma digitale.
Le registrazioni in emergenza, in partenza, in arrivo o interne, vengono tutte eseguite dall'Ufficio Protocollo.

Le informazioni da inserire nel registro di emergenza, ovvero i campi obbligatori da compilare sono gli stessi previsti dal protocollo generale.
Le modalità con cui vengono eseguite le registrazioni di protocollo sul registro di emergenza sono quelle sancite dall'art.63 del DPR N.445/00, in particolare:
- sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema informatico di protocollo, nonché la data e l'ora del ripristino della funzionalità;
- qualora l'interruzione del funzionamento del sistema di protocollo informatico si prolunghi per più di ventiquattro ore, il Responsabile del Servizio Protocollo, ai sensi della normativa vigente, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle notizie di cui al precedente comma, vengono riportati gli estremi del provvedimento di autorizzazione (All.8.1);
- per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati.
Al ripristino della funzionalità del sistema di protocollo informatico tutte le registrazioni effettuate mediante i registri di emergenza vengono recuperate dal sistema, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.
La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

SEZIONE 5
DOCUMENTAZIONE PARTICOLARE

5.1 - Deliberazioni di Giunta e Consiglio, determinazioni dei responsabili di P.O., decreti, ordinanze, contratti, verbali di sanzioni amministrative della Polizia Locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, pubblicazioni all'albo on line e notifiche.

Le deliberazioni di Giunta e Consiglio, le determinazioni dei responsabili di P.O., i decreti, le ordinanze, i contratti, i verbali della Polizia Locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, se sono documenti già soggetti a registrazione particolare da parte dell'Ente possono non essere registrati al protocollo.
Per quanto riguarda le pubblicazioni all'albo *on line* e le notifiche si rimanda alle apposite Linee guida (all. n.9).

5.2 - Documentazione di gare d'appalto

La corrispondenza che riporta l'indicazione "offerta" - " gara d'appalto "- "preventivo" o simili, dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili e deve essere indirizzata all'ufficio competente.
In caso di gare nel mercato elettronico o acquisti effettuati mediante piattaforme informatiche, tutta la documentazione è ricevuta telematicamente direttamente nel sistema, che ne garantisce la sicurezza e la riservatezza.

5.3 Gestione delle fatture

La dotazione informatica del Comune di Rosate è stata adeguatamente integrata al fine ai garantire il puntuale rispetto della normativa vigente in materia di fatturazione elettronica.
Per quanto concerne la conservazione delle fatture elettroniche si rimanda alla sezione 11.

5.4 - Lettere anonime

La registrazione di un documento in arrivo deve rispondere a criteri di valutabilità. Il responsabile della protocollazione deve attestare che un determinato documento così come

si registra è pervenuto. Si tratta di una competenza di tipo notarile, attestante la certezza giuridica di data, forma e provenienza per ogni documento.
Le lettere anonime, pertanto vanno protocollate con indicazione di "anonimo" al mittente.
Non spetta a chi protocolla un documento in arrivo effettuare verifiche sulla veridicità del documento. Sarà, eventualmente, compito del responsabile del servizio, assegnatario del documento, valutare caso per caso, ai fini della sua efficacia riguardo ad un affare o procedimento amministrativo, se la lettera è da ritenersi valida.

5.5 Lettere prive di firma o con firma illeggibile

Le lettere prive di firma vanno protocollate. Si equiparano alle lettere prive di firma le lettere pervenute con firma illeggibile.
La funzione notarile del protocollo è quella di attestare data e provenienza certa di un documento senza interferire su di esso. Sarà poi compito del Responsabile del Servizio, assegnatario del documento, valutare, caso per caso ai fini della sua efficacia riguardo ad un affare o un determinato procedimento amministrativo, se la lettera priva di firma o con firma illeggibile è da ritenersi valida.

5.6 Corrispondenza Personale o Riservata

La corrispondenza personale è regolarmente aperta e registrata al protocollo, a meno che sulla busta non siano riportate le diciture "riservata", "personale", "riservata personale", "confidenziale": in questi casi, la corrispondenza è consegnata in busta chiusa al destinatario il quale, dopo averne preso visone, se ritiene, ne può richiedere la protocollazione.

5.7 - Documenti inviati via fax

Sulla base della normativa vigente, la corrispondenza tra pubbliche amministrazioni deve avvenire di norma tramite l'uso della posta elettronica (Art.5.13). Pertanto di norma non si spediscono documenti via fax.
In caso di necessità è consentito l'utilizzo del fax verso destinatari con i quali risulti impossibile comunicare in altro modo.
Tutti i documenti ricevuti e inviati via fax sono registrati al protocollo. Qualora successivamente al fax arrivasse anche l'originale del documento, a questo sarà attribuito lo stesso numero di protocollo. Il modello di trasmissione e l'originale del documento spedito via fax devono essere inseriti nel fascicolo.
Di norma al fax non segue mai l'originale; qualora l'originale sia spedito a seguito del fax deve essere apposta sul documento la dicitura "già inviato via fax". Al documento inviato successivamente al fax deve essere apposto lo stesso numero di protocollo attraverso un timbro di segnatura che riporta le seguenti informazioni: " *Già pervenuto via fax"* , numero di protocollo, data e classificazione.
Il timbro di segnatura di protocollo va posto sul documento (lettera) e non sulla copertina di trasmissione del fax.

5.8 - Corrispondenza con più destinatari e copie per conoscenza

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo. Se in uscita, i destinatari possono essere descritti in elenchi associati al documento. Dei documenti analogici prodotti/pervenuti, di cui necessita la distribuzione interna all'ente, si faranno copie informatiche.

5.9 - Integrazioni documentarie

Gli addetti al ricevimento della corrispondenza e alle registrazioni di protocollo non sono tenuti a verificare la completezza formale e sostanziale della documentazione pervenuta, ma unicamente a verificare la corrispondenza fra gli eventuali allegati dichiarati e gli allegati effettivamente presentati con la pratica.
La verifica di cui sopra spetta all'ufficio competente o al RPA che, qualora ritenga necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente con le comunicazioni del caso

5.10 - Documenti di competenza di altre amministrazioni

Qualora pervengano all'Ente documenti di competenza di altre amministrazioni, questi verranno restituiti al destinatario con la dicitura "Erroneamente pervenuto al Comune di Rosate" . Se il documento viene erroneamente protocollato, il numero di protocollo deve essere annullato e il documento inviato al destinatario. Nel caso in cui il destinatario non sia individuabile, il documento deve essere rimandato al mittente.

5.11- Oggetti plurimi

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi e pertanto, da assegnare a più fascicoli, si dovranno produrre copie autentiche dello stesso documento e successivamente registrarle, classificarle e fascicolarle indipendentemente una dall'altra. L'originale verrà inviato al destinatario indicato nel documento, oppure, nel caso di destinatari plurimi, al primo in indirizzo. Nel caso in cui l'individuazione di più oggetti venga effettuata successivamente da parte del destinatario, questi deve inviare al Servizio apposita comunicazione affinché si provveda nel medesimo modo. La documentazione in partenza deve avere un unico oggetto per ciascuna comunicazione.

5.12 - Modelli pubblicati

Tutti i modelli di documenti pubblicati sul sito internet o sulla rete intranet dell'Ente sono classificati secondo il piano di classificazione in uso. Non possono essere pubblicati modelli, formulari ecc. che non siano classificati.

5.13 - Gestione della posta elettronica certificata

La AOO è dotata della casella di Posta Elettronica Certificata istituzionale per la corrispondenza sia in ingresso che in uscita, pubblicata sull'indice della Pubbliche Amministrazioni (IPA) e sulla homepage del proprio sito Internet; questa casella costituisce l'indirizzo virtuale dell'AOO e di tutti gli uffici che ad essa fanno riferimento. La casella istituzionale di posta elettronica certificata, collegata con il sistema di protocollo informatico, è quindi l'indirizzo elettronico ufficiale atto a ricevere messaggi da altre pubbliche amministrazioni, cittadini, professionisti ed imprese dotati di analoghi strumenti di trasmissione (PEC).

La casella di Posta Elettronica Certificata è accessibile, per l'invio e la ricezione di documenti, solo dall'Ufficio Protocollo, che procede quindi alla registrazione di protocollo, previa verifica dell'integrità e leggibilità dei documenti stessi, mentre per la manutenzione e la gestione tecnica è accessibile al servizio Informatico.

La posta elettronica non certificata è utilizzata per l'invio di comunicazioni, informazioni e documenti.

In particolare è sufficiente ricorrere a un semplice messaggio di posta elettronica per convocare riunioni (interne all'ente), inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito a informazioni generali di organizzazione, diffondere circolari e ordini di servizio (gli originali si conservano nel fascicolo specifico), documenti informatici, copie di documenti cartacei. La posta elettronica è utilizzata per spedire copie dello stesso documento a più destinatari. A chi ne fa richiesta deve sempre essere data la risposta dell'avvenuto ricevimento. Non è possibile inviare messaggi dalla casella di posta elettronica personale quando il contenuto di questi impegni l'amministrazione verso terzi. La trasmissione di documenti che necessita di una ricevuta di invio e di consegna è effettuata tramite il sistema di posta elettronica certificata. Per quanto riguarda la gestione della posta elettronica nelle pubbliche amministrazioni vedi gli articoli 45-49 del CAD D.Lgs 82/05 come modificato dal D.Lgs 235/10.

Ogni Servizio, è dotato di mail istituzionale non certificata, le cui mail sono riportate nel sito istituzionale sezione "Trasparenza" secondo quanto stabilito dal D.L. 33/2013.

Qualora il messaggio pervenga a caselle di ufficio e si ritenga opportuno attribuire egualmente un'efficacia probatoria al messaggio stesso, dovrà essere rispettata la seguente procedura:

- il corpo del messaggio o il/i documento/i ad esso allegati dovranno essere inoltrati alla casella di posta certificata dell'ente e successivamente registrati a cura del servizio protocollo;

- il messaggio sarà successivamente assegnato dal servizio protocollo, attraverso il software di protocollo, al responsabile del procedimento amministrativo che ne ha precedentemente richiesto la protocollazione.

5.14 - Produzione di copie cartacee di documenti informatici

Nel caso della produzione di copie cartacee di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione di cui ai modelli dell'allegato n. 10.

5.15 - Trasmissioni telematiche

I dati di cui all'allegato n.11 sono trasmessi/ricevuti dall'Ente con immissione diretta dei dati sul server dell'Ente destinatario, senza la produzione e conservazione dell'originale cartaceo. I documenti sono trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate ed ad identificazione univoca attivati con i singoli Enti destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

5.16 - Sito Internet Istituzionale

Sul sito internet istituzionale (www.comune.rosate.mi.it) sono pubblicate le sezioni dedicate all'Albo online, gestito secondo le linee guida previste dall'allegato n.9, e la Sezione relativa all'Amministrazione Trasparente, in cui sono indicati i contenuti previsti nel D.Lgs. n.33/2013.

SEZIONE 6
ASSEGNAZIONE DEI DOCUMENTI

6.1- Assegnazione

L'assegnazione dei documenti agli uffici utenti o ai responsabili di procedimento è effettuata dal Servizio Protocollo sulla base dell'elenco allegato degli uffici e dei responsabili di procedimento (all. n.3).
I documenti ricevuti dall'Ente, al termine delle operazioni di registrazione, classificazione, segnatura ed assegnazione, sono fatti pervenire in originale agli uffici competenti.
La registrazione a protocollo sulla procedura informatica risulta in "carico" ad un determinato ufficio : è compito dell'ufficio protocollo procedere ad eventuale modifica di assegnazione.
Il sistema di gestione informatica dei documenti tiene traccia delle riassegnazioni.
Spettano al Responsabile del Procedimento amministrativo le incombenze relative alla gestione del documento: l'inserimento nel fascicolo di competenza preesistente o eventualmente in un nuovo fascicolo e l'invio delle copie per conoscenza.

6.2 - Consegna dei documenti informatici

I documenti informatici e/o le immagini digitali dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale (vedi anche Sezione 10 – Scansione dei documenti su supporto cartaceo).

6.3 - Consegna dei documenti analogici

I documenti analogici/cartacei protocollati e assegnati sono resi disponibili ai destinatari mediante l'uso di cassette per ogni servizio situate presso il Servizio Protocollo.

SEZIONE 7
CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

7.1- Classificazione dei documenti

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario di cui all'art.1.7. La classificazione è l'operazione finalizzata ad organizzare logicamente, in relazione alle funzioni dell'Ente, tutti i documenti ricevuti e prodotti dal comune di Rosate, siano essi cartacei o informatici, contestualmente alla loro registrazione nel sistema di gestione informatica dei documenti. Tale operazione consiste nell'assegnazione a ciascun documento di un codice, detto indice di classificazione che, in base all'oggetto del documento medesimo, lo associa alla voce del titolario relativa alla corrispondente funzione dell'Ente. sulla base dell'indice di classificazione risulta indicata la posizione logica del documento all'interno dell'archivio ed è così possibile l'inserimento nel fascicolo appropriato.

Nel caso siano riscontrati errori nell'indice di classificazione, il personale dell'ufficio che riceve il documento lo segnala all'Ufficio Protocollo che procede a correggere sul sistema, la classificazione errata. Il sistema di gestione informatica dei documenti mantiene traccia delle operazioni svolte, registrandone l'autore, la data e l'ora.

7.2 - Formazione e identificazione dei fascicoli

Tutti i documenti registrati al protocollo informatico e classificati, indipendentemente dal supporto sul quale sono forniti, devono essere riuniti in fascicoli attraverso l'opportuna funzione del sistema di protocollo informatico. La formazione di un nuovo fascicolo è effettuata dal Responsabile del procedimento ed avviene attraverso l'operazione di apertura, con richiesta scritta oppure, se informatica, regolata dal manuale operativo del sistema, che prevede la registrazione sul repertorio/elenco dei fascicoli o nel sistema informatico delle seguenti informazioni:

a) categoria e classe del titolario di classificazione;
b) numero del fascicolo (la numerazione dei fascicoli è annuale e indipendente per ogni classe);
c) oggetto del fascicolo;
d) data di apertura;
e) ufficio a cui è assegnato;
f) responsabile del procedimento;
g) livello di riservatezza eventualmente previsto.

Il sistema di protocollo informatico provvede automaticamente ad aggiornare il repertorio/elenco dei fascicoli.

7.3 - Processo di formazione dei fascicoli

In presenza di un documento da inserire in un fascicolo i Responsabili di Servizio stabiliscono, consultando le funzioni del protocollo informatico o il repertorio dei fascicoli, se esso si collochi nell'ambito di un affare o procedimento in corso, oppure se dà avvio ad un nuovo procedimento.

Se il documento deve essere inserito in un fascicolo già aperto, dopo la classificazione e protocollazione viene rimesso al responsabile del procedimento che ha cura di inserirlo fisicamente nel fascicolo; nel caso di documenti informatici il sistema provvede automaticamente, dopo l'assegnazione del numero di fascicolo, a inserire il documento nel fascicolo informatico stesso. Se invece dà avvio a un nuovo affare, I responsabili di procedimento aprono un nuovo fascicolo (con le procedure sopra descritte).

7.4 - Modifica delle assegnazioni dei fascicoli

La riassegnazione di un fascicolo è effettuata da chi ha in carico il fascicolo, provvedendo a correggere le informazioni del sistema informatico e del repertorio dei fascicoli e inoltrando successivamente il fascicolo al responsabile del procedimento di nuovo carico. Delle operazioni di riassegnazione, e degli estremi del provvedimento di autorizzazione, è lasciata traccia nel sistema informatico di gestione dei documenti o sul repertorio/elenco cartaceo dei fascicoli.

SEZIONE 8
SPEDIZIONE DEI DOCUMENTI DESTINATI ALL'ESTERNO

8.1 - Spedizione dei documenti cartacei

I documenti da spedire sono trasmessi direttamente dal responsabile del procedimento dopo le operazioni di registrazione al protocollo e di classificazione nonché delle eventuali indicazioni necessarie a individuare il procedimento amministrativo di cui fanno parte. I documenti devono essere in originale da inviare e la minuta è da conservare agli atti; nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate, posta celere, corriere o altro mezzo di spedizione), queste saranno compilate a cura del servizio interessato alla trasmissione. All'ufficio protocollo competono le operazioni di pesatura.
Spedizioni di grandi quantità di corrispondenza devono essere concordate con il servizio protocollo.

8.2 - Spedizioni documenti cartacei con destinatari multipli

Nel caso di spedizioni con destinatari multipli superiori a 10 si potrà inserire nel campo del destinatario la dicitura "destinatari diversi elenco nel fascicolo". L'elenco dei destinatari deve essere unito al documento e registrato come allegato nel sistema di protocollo. Sull'elenco si riporta la segnatura di protocollo.
In questo caso il materiale dovrà essere consegnato, dopo avvenuta assegnazione del protocollo in partenza, già imbustato a cura dell'Ufficio richiedente e su ogni busta dovrà, sempre a cura dell'Ufficio richiedente, essere apposto il destinatario.

8.3 - Spedizione dei documenti informatici

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti con le procedure adottate dal manuale operativo dello stesso, dopo essere stati classificati, fascicolati e protocollati e comunque secondo i seguenti criteri generali:

1) i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via elettronica, tramite casella di posta elettronica certificata;
2) per la spedizione l'amministrazione si avvale di una casella di posta elettronica certificata e dei servizi di autenticazione e marcatura (art.27, comma 3, DPR n.445/00);
3) l'ufficio protocollo/le postazioni decentrate di protocollo provvedono:
   - a effettuare l'invio elettronico utilizzando i servizi di autenticazione e marcatura temporale;
   - a verificare l'avvenuto recapito dei documenti spediti per via elettronica;
   - ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del CAD D.Lgs. 82/05 come modificato dal D.Lgs. n.235/10.
Per l'uso della posta elettronica si rimanda all'articolo n.5.13.
La spedizione di documenti informatici può avvenire anche attraverso canali telematici, previsti nell'allegato n.11
La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste l'amministrazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

SEZIONE 9
GESTIONE DEI FLUSSI DI DOCUMENTI COSIDDETTI INTERNI

9.1 Comunicazioni informali
Questo genere di informazioni possono essere trasmesse/ricevute per posta elettronica purché si tratti di scambio di informazioni e documenti che non impegnino l'amministrazione verso terzi.

9.2 Scambio di documenti fra gli uffici
Della comunicazione/scambio di informazioni, di documenti giuridicamente rilevanti all'interno dell'ente deve essere tenuta traccia nel sistema informatico di gestione dei documenti e degli archivi. Le modalità di trasmissione e registrazione sono descritte nel manuale operativo al capitolo "Registrazione dei documenti" alla voce Registrazione dei documenti interni.

SEZIONE 10
SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

10.1 - Documenti soggetti a scansione
I documenti su supporto cartaceo, di formato inferiore o uguale all'A4, dopo le operazioni di registrazione, classificazione e segnatura, possono essere acquisiti in formato immagine con l'ausilio di scanner.
La scansione degli altri documenti avviene secondo quanto previsto dal piano di conservazione.

10.2 - Processo di scansione
Il processo di scansione si articolerà di massima nelle seguenti fasi:

1) acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard abilitato alla conservazione;
2) verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
3) collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
4) memorizzazione delle immagini, in modo non modificabile.

I documenti analogici soggetti a riproduzione sostitutiva si conservano nell'archivio dell'ente fino a procedimento legale di scarto.

SEZIONE 11
CONSERVAZIONE E TENUTA DEI DOCUMENTI

11.1 - Conservazione e memorizzazione dei documenti cartacei, informatici e delle rappresentazioni digitali dei documenti cartacei.

I documenti dell'amministrazione, su qualsiasi formato prodotti, sono conservati a cura del Servizio archivistico che svolge anche le funzioni di Responsabile della conservazione.
La documentazione corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.
I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo, e conservati nell'archivio informatico.

Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.
Il Responsabile del servizio archivistico provvede, in collaborazione con il servizio di gestione dei servizi informativi e con il supporto della tecnologia disponibile, a conservare i documenti informatici e a controllare periodicamente a campione (almeno ogni sei mesi) la leggibilità dei documenti stessi. L'intervento del Responsabile del servizio archivistico deve svolgersi in modo che si provveda alla conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi. Il servizio archivistico, di concerto con i sistemi informativi dell'ente, provvede altresì alla conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti. Il sistema deve inoltre fornire la documentazione del software di gestione e conservazione, del sistema di sicurezza, delle responsabilità per tutte le fasi di gestione del sistema documentario, delle operazioni di conservazione dei documenti.
La documentazione prodotta nell'ambito del manuale di gestione e dei relativi aggiornamenti deve essere conservata integralmente e perennemente nell'archivio dell'ente

SEZIONE 12
ARCHIVIO CORRENTE, DI DEPOSITO E STORICO

12.1. L' archivio
L' Archivio dell'Ente è costituito dal complesso organico di documenti ricevuti e spediti dall'ente nell'esercizio delle proprie funzioni.
L' Archivio è da considerarsi unico indipendentemente dalle soluzioni organizzative. La suddivisione in archivio corrente, archivio di deposito e archivio storico risponde esclusivamente a necessità legate alla differente gestione delle carte in rapporto all'età.
I documenti conservati hanno un valore amministrativo, giuridico e storico fin dalla loro formazione.
Possono far parte dell'archivio anche fondi archivistici di enti e istituti cessati le cui funzioni siano state trasferite al Comune e gli archivi e i documenti acquisiti per dono, deposito, acquisto o a qualsiasi altro titolo.

12.2 Regime giuridico
Il D.Lgs. 42 del 22/01/2004 "Codice dei beni culturali e del paesaggio" stabilisce che sono beni culturali, assoggettati al regime proprio del demanio pubblico, gli archivi e i singoli documenti degli enti pubblici.
I singoli documenti (analogici ed informatici, ricevuti, spediti, interni) e l'archivio del Comune di Rosate nel complesso sono quindi beni culturali appartenenti al demanio pubblico, sin dal momento dell'inserimento di ciascun documento nell'archivio del Comune mediante l'attribuzione di un codice di classificazione.
In quanto appartenenti al demanio pubblico gli archivi e i singoli documenti del Comune di Rosate sono inalienabili. Devono essere conservati nella loro organicità. Lo scarto di documenti è subordinato all'autorizzazione della Soprintendenza Archivistica competente per territorio.
L'amministrazione potrà eventualmente, previa autorizzazione della Soprintendenza Archivistica competente, anche con affidamento in outsorcing, attivare un archivio ibrido composto da documenti informatici e cartacei. In tal caso l'archivio sarà strutturato su due livelli: archivio informatico e archivio fisico.

12.3 - L' archivio corrente: formazione e gestione dei fascicoli
L' Archivio corrente è costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi non ancora conclusi.
La responsabilità della gestione (classificazione, fascicolazione, organizzazione) e della custodia della documentazione dell'archivio corrente è del Responsabile del procedimento.

12.4 - L'Archivio di deposito

L' Archivio di Deposito è costituito dalla documentazione riferita ad affari e a procedimenti amministrativi che, sebbene conclusi, possono essere riassunti in esame o per un'eventuale ripresa o per un interesse sporadico, legato all'analogia o alla connessione con altre pratiche successive.

L' Archivio di Deposito raccoglie, ordina, seleziona ai fini della conservazione permanente e rende consultabile, nel rispetto delle leggi vigenti, tutta la documentazione di valore archivistico prodotta dal Comune di Rosate che, non essendo più strettamente necessaria per il disbrigo degli affari correnti, non è tuttavia ancora nelle condizioni di essere collocata, a norma di legge (cioè 40 anni trascorsi dalla conclusione della pratica), presso l'archivio storico.

All'inizio di ogni anno gli uffici, verificata l'effettiva conclusione ordinaria della pratica, individuano i fascicoli cartacei da versare all'archivio di deposito dandone comunicazione al Responsabile della Conservazione.

Per ragioni logistiche dal 1/01/2011 il servizio di deposito *in outsourcing* dell'archivio comunale è stato affidato alla ditta Microdisegno Srl di Lodi.

Il responsabile della Conservazione provvede al trasferimento dei fascicoli aggiornando il relativo elenco e rispettando l'organizzazione dell'archivio corrente.

I fascicoli informatici, mediante specifiche funzionalità di sistema, vengono trasferiti nel sistema di conservazione adottato.

12.5 Archivio storico

L' Archivio Storico è costituito dai documenti relativi ad affari esauriti da oltre quaranta anni (art. 40 del D. Lgs. 490/1999).

I documenti dell' Archivio Storico sono destinati alla conservazione permanente per finalità di tipo prevalentemente culturale-storico e di ricerca.

I locali dell'Archivio Storico si trovano presso il Municipio.

I registri dello stato civile italiano dal 1866 sono conservati presso l'Ufficio Anagrafe e Stato Civile.

Il Comune ha l'obbligo di ordinare ed inventariare il proprio archivio storico (art..40 del D.Lgs. 490/1999) e di garantirne la consultazione per finalità culturali storico-scientifiche.

12.6- Gestione archivio di deposito e storico

Per la gestione dell'archivio di deposito e dell'archivio storico, si rimanda alle linee guida dell'archivio (All.12).

SEZIONE 13
PIANO PER LA SICUREZZA INFORMATICA

13.1 Piano per la sicurezza informatica

Il Piano per la sicurezza informatica, redatto ai sensi della normativa vigente, è contenuto nel "Documento Programmatico sulla Sicurezza Informatica (DPS)", approvato dalla Giunta Comunale con proprio atto, cui si fa rinvio.

È messo in atto ai sensi della normativa vigente il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi.

13.2- Politiche di sicurezza

a) Politiche accettabili di uso del sistema informativo

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di

rete, le licenze di acquisto dei software applicativi, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.
Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.
Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati delle aziende *outsourcer* includendo tutto il personale affiliato con terze parti. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.
Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito. Le singole aree o settori sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Responsabile di Posizione Organizzativa.
Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.
Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password).
Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni sei mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

Non permettere ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le proprie credenziali.

b) Politiche – antivirus

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni. I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia. I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato. Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.

Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura. Non scaricare mai messaggi da siti o sorgenti sospette. Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus. Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste. Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone. Evitare collegamenti diretti ad Internet via modem.

Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura. Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura. Non utilizzare i server di rete come stazioni di lavoro. Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali. Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione. Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno. Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato. È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il Responsabile del Servizio Protocollo stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

c) Politiche per le azioni consuntive. Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza,

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.
Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

- Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
- Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
- È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
- Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
- Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
- Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedopornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
- Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
- Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
- Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione. Internet/Intranet/Extranet.

e) Attività di messaggistica e comunicazione.

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.
Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
Uso non autorizzato delle informazioni della testata delle e-mail, Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

SEZIONE 14
ACCESSO

14.1- Accessibilità da parte degli utenti appartenenti all'Amministrazione

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e *password,* o altre tecniche e dispositivi di autenticazione

sicura. L'operatore che effettua la registrazione di protocollo inserisce il livello di riservatezza richiesto per il documento in esame, altrimenti il sistema applica automaticamente l'inserimento di un livello standard predeterminato. In modo analogo, al momento dell'apertura di un nuovo fascicolo, deve esserne determinato il livello di riservatezza. Il livello di riservatezza applicato a un fascicolo si estende a tutti i documenti che ne fanno parte. In particolare, un documento con livello minore di quello del fascicolo assume il livello del fascicolo di inserimento, mentre mantiene l'eventuale livello maggiore. Per quanto riguarda i documenti riservati, si rimanda alle normative che regolano tutte le possibilità di accesso, consultazione e riproduzione dei documenti.
L'accessibilità e la riservatezza delle registrazioni di protocollo sono garantite dal sistema attraverso l'uso di profili utente e password.
I livelli di accesso interno sono i seguenti: visualizzazione, inserimento, modifica e annullamento.

14.2- Accesso esterno

L'accesso al sistema informatico da parte di utenti esterni può avvenire nei casi di particolari procedimenti amministrativi con credenziali di accesso rilasciate dall'Ente.
Come previsto dal D.Lgs. n.33/2013, è garantito a tutti i cittadini, mediante l'istituzione dell'Accesso Civico, l'accesso e la libera consultazione a tutti gli atti dell'Ente per i quali è prevista la pubblicazione. Sul sito istituzionale è consultabile l'apposita sezione "Amministrazione Trasparente" a cui il cittadino ha libero accesso e nella quale sono disponibili informazioni integre e conformi all'originale.
Per ogni altro obbligo inerente la pubblicazione di documenti e atti dell'Ente sul sito internet istituzionale, si fa riferimento al D.Lgs. n.33/2013 e per quanto riguarda il diritto di accesso, alle leggi specifiche in materia.

SEZIONE 15
APPROVAZIONE REVISIONE E PUBBLICAZIONE

15.1- Approvazione

Il presente manuale è adottato dalla Giunta Comunale con suo provvedimento proprio, su proposta del responsabile del Servizio della gestione documentale.

15.2 - Revisione

Il presente manuale sarà rivisto ogni qualvolta se ne presenti la necessità. La modifica o l'aggiornamento di uno o tutti i documenti allegati al presente manuale non comporta la revisione del manuale stesso.

15.3 Pubblicazione e divulgazione

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet dell'amministrazione e la pubblicazione all'albo pretorio.

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 1

NORMATIVA DI RIFERIMENTO IN AMBITO DI GESTIONE DOCUMENTALE

> D.P.C.M. 31/10/2000

> D.P.R. n.445 del 28/12/2000

> D.P.C.M. 03/12/2013 e relativi allegati

> Deliberazione CNIPA n.11/2004

> D.Lgvo n.82 del 7/03/2005 -CAD " Codice dell'Amministrazione Digitale"

> D.P.C.M. 13/11/2014

ALLEGATO 2

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

GLOSSARIO/DEFINIZIONI

Allegato n.1 D.P.C.M. 03-12-2013 "Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici"

Indice

1. INTRODUZIONE

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizione del citato decreto ed a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

2. DEFINIZIONI

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte **dell'Agenzia per l'Italia digitale,** del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, **dall' Agenzia per l'Italia digitale,** il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica, dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo

TERMINE	DEFINIZIONE
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, **dall'Agenzia per l'Italia digitale,** il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, **dall'Agenzia per l'Italia digitale**
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di *backup* degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni

TERMINE	DEFINIZIONE
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
Funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni

TERMINE	DEFINIZIONE
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità 1 previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

TERMINE	DEFINIZIONE
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma l delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse **storico** culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice

TERMINE	DEFINIZIONE
sistema di gestione informatica dei documenti	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
Testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
ufficio utente	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 3

ELENCO DEI SETTORI - UFFICI E SERVIZI - DELL'ENTE ED ELENCO ABILITAZIONI ALLA PROTOCOLLAZIONE

AREA ORGANIZZATIVA OMOGENEA

L'Amministrazione di Rosate ha istituito un'unica area organizzativa omogenea per la gestione dei documenti, denominata COMUNE DI ROSATE.

Denominazione dell'Ente:	**COMUNE DI ROSATE**
Indirizzo:	**Via Vittorio Veneto nr. 2**
Codice Identificativo:	**c_h560**
A.O.O.:	**COMUNE DI ROSATE**
Indirizzo posta elettronica certificata istituzionale:	**comune.rosate@pec.regione.lombardia.it**
Telefono:	**02/908301**
web:	www.comune.rosate.mi.it

SETTORE	SERVIZIO	N. POSTAZIONI IN ARRIVO	N. POSTAZIONI IN PARTENZA
Settore 1	Area Servizi Amministrativi	1	6
Settore 2	Area Servizi Finanziari	0	3
Settore 3	Area Servizi alla Persona	0	6
Settore 4	Area Servizi Tecnici	0	4
Settore 5	Area Servizi Polizia Locale	0	5

Attività dei singoli settori

SETTORE 1 – AREA SERVIZI AMMINISTRATIVI

Si occupa prevalentemente delle seguenti tematiche, materie e funzioni:
Segreteria del Sindaco e Segreteria Generale
Giunta e Consiglio Comunale
Commissioni Comunali
Gestione, verifica e controllo atti formali, Statuto, Regolamenti, Delibere, Determine, Ordinanze, Decreti e atti del Sindaco
Affari Generali
Protocollo

Albo Pretorio
Gestione Archivio
Centralino
Informazione Istituzionale e Sportello relazioni con il pubblico
Gestione sistema informatico e Sito web istituzionale
Assicurazioni Comunali
Comunicazione istituzionale
Gemellaggio, Ricorrenze ed eventi Istituzionali
Controllo e rapporti con società partecipate del Settore
Fiscalità comunale – pianificazione e acquisizione delle entrate tributarie e loro costante monitoraggio anche a sostegno e in affiancamento agli altri settori comunali
Accertamento e riscossione dei tributi, delle tasse , delle tariffe e dei canoni comunali riferite al settore
Attività di recupero della evasione tributaria e rimborso dei tributi
Tenuta e aggiornamento dell'anagrafe tributaria comunale
Rapporti con l'Agenzia delle Entrate e le altre Agenzia creditizie e finanziarie
Controllo di gestione con riferimento alla verifica di efficacia, di efficienza della gestione
Analisi relativa all'avanzamento dei progetti con riferimento agli obiettivi individuati dal Governo Comunale
Gestione, controllo, verifica e monitoraggio entrate e spese riferite al settore

SETTORE 2 – AREA SERVIZI FINANZIARI

Si occupa prevalentemente delle seguenti tematiche, materie e funzioni:
Programmazione finanziaria
Predisposizione e gestione Bilancio previsionale annuale e pluriennale compresi equilibrio – assestamento – consuntivo – variazioni
Verifica patto di stabilità
Controllo e monitoraggio delle spese e delle entrate
Mutui, investimenti e strumenti finanziari, adempimenti connessi alla contrazione di nuovo debito anche attraverso strumenti di finanza innovativa, anticipazioni di cassa e gestione attività del debito
Gestione contratto di Tesoreria e dei rapporti con la Tesoreria Regionale e Statale
Pagamenti e introiti
Gestione finanziaria del personale
Gestione finanziaria del patrimonio e del demanio comunale
Gestione, controllo, verifica e monitoraggio entrate e spese riferite al settore

SETTORE 3 – AREA SERVIZI ALLA PERSONA

Si occupa prevalentemente delle seguenti tematiche, materie e funzioni:
Attività scolastiche, formative ed educative, gestione mense scolastiche
Gestione trasporto scolastico
Asilo nido, infanzia, famiglia, anziani, consultorio
Gestione alloggi anziani e categorie protette
Assistenza sociale, domiciliare, rapporti con ASL, azienda ospedaliera, enti socio – sanitari – assistenziali
Attività sostegno persone in difficoltà
Gestione strutture socio-assistenziali
Gestione rapporti con Enti e Associazioni Socio – Assistenziali
Lavoro e occupazione
Attività culturali, del tempo libero e ricreative, fiere, manifestazioni ed eventi
Attività sportive e gestione degli impianti sportivi, culturali e ricreativi
Rapporti e controllo società partecipate del settore
Attività rivolte al mondo giovanile e adolescenziale
Gestione rapporti e attività inerenti i settori scolastici, educativi, formativi, culturali, del tempo libero e sportivi

Gestione rapporti con Enti e Associazioni educative, culturali, sportive e ricreative
Gestione, controllo, verifica e monitoraggio entrate e spese riferite al settore

SETTORE 4 – AREA SERVIZI TECNICI

Si occupa prevalentemente delle seguenti tematiche, materie e funzioni:
Gestione piano governo del territorio, programmi e piani urbanistici
Edilizia privata e residenziale pubblica
Permessi di costruire
Programmazione, valorizzazione e tutela territoriale
Piste ciclo pedonali
Parchi sovra comunali
Collegamenti viari sovra comunali
Trasporti e mobilità
Gestione programma opere pubbliche
Interventi edilizi pubblici e realizzazione opere, strutture e infrastrutture di pubblica utilità
Viabilità comunale
Manutenzione beni immobili comunali
Arredo urbano
Ecologia, ambiente e tutela del territorio, raccolta e smaltimento rifiuti – parte di competenza
Servizi tecnologici, energetici e di pubblica utilità: gas metano, ciclo integrato acque, fognatura, ecc.
Parchi comunali e verde pubblico
Controllo e rapporti con società partecipate del settore
Gestione, controllo, verifica e monitoraggio entrate e spese riferite al settore

SETTORE 5 – AREA SERVIZI DI POLIZIA LOCALE

Si occupa prevalentemente delle seguenti tematiche, materie e funzioni:
Polizia Locale
Attività produttive
Viabilità
Protezione civile
Sportello unico – insediamenti produttivi
Controllo e rapporti con società partecipate del settore
Gestione, controllo, verifica e monitoraggio entrate e spese riferite al settore

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 4

ELENCO DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Albo on-line

APR

Atti di cittadinanza

Atti di matrimonio

Atti di morte

Atti di nascita

Atti di pubblicazione di matrimonio

Atti di Polizia Giudiziaria

Autorizzazioni in materia paesaggistica

Autorizzazione al seppellimento

Autorizzazione alla cremazione

Autorizzazioni apertura medie e grandi strutture di vendita

Autorizzazioni commercio su aree pubbliche con posteggio e itinerante

Autorizzazioni manifestazioni

Autorizzazioni trasporti pubblici non di linea

Autorizzazioni di occupazione di suolo pubblico

Autorizzazioni al trasporto salma

Contratti pubblici in forma amministrativa

Contratti di lavoro individuali

Convenzioni

Decreti del Sindaco

Deliberazioni di Consiglio Comunale

Deliberazioni di Giunta Comunale

Accertamenti ICI – IMU

Accertamenti TIA – TARES

Determinazioni

Fatture emesse

Mandati di pagamento

Notifiche

Numeri di matricola degli ascensori

Ordinanze

Permessi Pass Disabili

Permessi Pass Veicoli

Permessi di costruire

Reversali

Segnalazioni Certificate inizio Attività Produttiva (S.C.I.A.)

Verbali accertamenti violazione Codice della Strada

Verbali della delegazione trattante per la contrattazione integrativa

Verbali della commissione consiliare per le garanzie statutarie

Verbali delle violazioni comunicazioni ospitalità stranieri

Verbali delle violazioni in materia di commercio su aree pubbliche e private

Verbali delle violazioni per ritardata/omessa denuncia di infortunio

Verbali delle violazioni pubblici esercizi

Verbali di fermo amministrativo e sequestro di veicoli

Verbali del Revisione dei Conti

Verbali Ufficio Elettorale Comunale

Verbali Commissione Elettorale Comunale

Allegato delibera ~~C.C.~~/G.M
n. 18 del 25/2/2016

Allegato n. 5

Titolario di classificazione

dic. 2005	Schema riassuntivo del piano di classificazione per l'archivio comunale
I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana 17. Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario *ad acta* 14. Organi di controllo interni 15. Organi consultivi 16. Consigli circoscrizionali 17. Presidente dei Consigli circoscrizionali 18. Organi esecutivi circoscrizionali 19. Commissioni dei Consigli circoscrizionali 20. Segretari delle circoscrizioni 21. Commissario *ad acta* delle circoscrizioni 22. Conferenza dei Presidenti di quartiere
III	Risorse umane 1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo

	8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari 14. Formazione e aggiornamento professionale 15. Collaboratori esterni
IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni
V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni 3. Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze
VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio 10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive

	7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale 2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio 3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri
XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi

Condizioni Generali di Contratto
- Firma Digitale -

Allegato delibera C.C./G.M. n. 18 del 25/2/2016

1. DEFINIZIONI
Ai fini delle presenti Condizioni Generali, si intende per:
Accordo: il documento redatto da Aruba Pec e sottoscritto dal Contraente, in cui sono descritte le caratteristiche tecniche ed economiche della Firma Digitale e delle relative condizioni di fornitura di cui possono usufruire i Clienti Business;
Aruba S.p.A.: soggetto che in forza di autonomo contratto stipulato con il Gestore è autorizzato a svolgere attività di rivendita della Firma Digitale ed è competente ad emettere fattura nei confronti del Cliente (di seguito, "Aruba");
Aruba Pec S.p.A.: soggetto iscritto nell'elenco pubblico dei certificatori predisposto, tenuto ed aggiornato dal Centro Nazionale per l'Informatica della Pubblica Amministrazione (CNIPA) ai sensi dell'art. 27 del D.P.R. 28 dicembre 2000, n. 445 e, come tale, legittimata ad emettere Certificati di Firma Digitale aventi valore legale, a norma del combinato disposto del D.P.R. 10 novembre 1997, n. 513 e del D.P.C.M. 13 gennaio 2004 e successive modifiche ed integrazioni (di seguito, "Aruba Pec" o "Certificatore");
Certificato: una rappresentazione digitale di dati informatici che deve contenere i dati identificativi del Certificatore e del richiedente/sottoscrittore del certificato, la Chiave pubblica del sottoscrittore, un numero seriale identificativo, la firma digitale del Certificatore e deve identificare il periodo di validità del certificato;
Chiave privata: la componente della coppia di chiavi asimmetriche destinato ad essere noto esclusivamente al soggetto che ne è titolare, mediante il quale quest'ultimo appone la Firma Digitale su un documento informatico oppure decifra il documento informatico in precedenza cifrato mediante la corrispondente Chiave pubblica;
Chiave pubblica: la componente della coppia di chiavi asimmetriche destinata ad essere resa pubblica, mediante la quale si verifica la Firma digitale apposta sul documento informatico del titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;
Cliente : il soggetto che, in qualità di Titolare richiede la fornitura della Firma Digitale alle condizioni tecniche e economiche pubblicate sul sito www.pec.it (di seguito cliente consumer) o che essendo iscritto/appartenente al Contraente, usufruisce delle condizioni stabilite nell'Accordo sottoscritto da quest'ultimo con Aruba Pec e richiede l'attivazione della Firma Digitale con le caratteristiche tecniche ed economiche ivi indicate (di seguito cliente business);
Contatto del Certificatore: il personale incaricato dal Certificatore per fornire ausilio agli Utenti nell'utilizzo della Firma Digitale ai recapiti indicati sul sito http://www.pec.it/Contacts.aspx;
Contraente: soggetto (Società, Ente, Ordine Professionale, etc.) che ha stipulato con Aruba Pec un Accordo e che assume, rispetto al soggetto richiedente l'emissione del certificato, il ruolo di Terzo Interessato;
Firma digitale: il risultato della procedura informatica (validazione), basato su un sistema di chiavi asimmetriche a coppia, una pubblica ed una privata, che consente al sottoscrittore, mediante la Chiave privata, ed al destinatario, mediante la Chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
Firma digitale remota: tipologia di Firma Digitale che non necessita del possesso fisico della chiave privata da parte del firmatario, poiché tale chiave è conservata, congiuntamente al certificato di firma, all'interno di un server remoto sicuro, accessibile via rete (Intranet e/o Internet);
Fornitori: Aruba Pec ed Aruba che, congiuntamente tra di loro, concludono con il Cliente il contratto di fornitura della Firma Digitale;
Kit di firma digitale: il kit distribuito dai Fornitori descritto in dettaglio nel Manuale Operativo ed avente ad oggetto l'emissione in favore del Cliente di un Certificato di Firma Digitale, in base alla tipologia di kit dal medesimo scelta tra quelle messe a sua disposizione e pubblicate sul sito istituzionale www.pec.it, conforme a quanto previsto nel D.P.R. 445/2000, nel D.P.C.M. 13 gennaio 2004 e successive modifiche ed integrazioni;
Manuale Operativo: il documento pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio del certificato digitale di sottoscrizione e del certificato digitale di autenticazione, nonché l'indicazione delle modalità operative per l'emissione e la gestione del servizio di certificazione di Aruba Pec nonché le istruzioni per l'uso del Servizio medesimo;
Modulo di Richiesta Firma Digitale: il modulo per la richiesta del Certificato compilato dal Cliente nel quale quest'ultimo indica le informazioni necessarie alla sua identificazione;
Terzo Interessato: soggetto che, in caso di rilascio di Certificati per firmare in funzione di un ruolo o di cariche rivestite per conto di organizzazioni terze che prevedono il conferimento di poteri, da parte di terzi, a colui che richiede il Certificato, unitamente al Titolare, avendo un interesse diretto nella gestione del Certificato, è legittimato alla revoca e/o sospensione del Certificato.
T.U.: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa approvato con il D.P.R. 445/2000.
Le definizioni qui non specificatamente richiamate mantengono il significato indicato nel Manuale Operativo.

2. OGGETTO DEL CONTRATTO
2.1 Le presenti Condizioni Generali di Contratto per la Fornitura della Firma Digitale (di seguito, "Condizioni Generali"), disciplinano le modalità ed i termini con cui le Società Aruba S.p.A. (P.Iva 01573850516), con sede in Piazza Garibaldi n. 8, 52010 Soci – Bibbiena (Arezzo), ed Aruba PEC S.p.A., (P.Iva 01879020517) con sede in Via Sergio Ramelli n. 8, 52100 Arezzo, forniscono al Cliente la Firma Digitale, nelle opzioni e con le caratteristiche tecniche e le condizioni economiche proprie della singola offerta commerciale prescelta dal Cliente, tra quelle messe a Sua disposizione, come individuata e descritta nel Contratto e nel sito www.pec.it.
2.2 La Firma Digitale è offerta e commercializzata dai Fornitori mediante la rete internet con le modalità descritte online, con le caratteristiche tecniche e nello stato di fatto e di diritto in cui si trova alla data della richiesta, così come pubblicati sul sito istituzionale, che il Cliente, accettando le seguenti Condizioni Generali, dichiara esplicitamente di conoscere ed accettare.
2.3 L'offerta della Firma Digitale è a tempo indeterminato, salva la facoltà dei Fornitori di sospenderla o revocarla in qualsiasi momento; in tal caso, i contratti conclusi prima della predetta sospensione e/o della revoca saranno onorati alle condizioni pattuite.

3. STRUTTURA DEL CONTRATTO
3.1 Il Contratto di fornitura della Firma Digitale è costituito da i seguenti documenti:
a) Modulo di Richiesta Firma Digitale (di seguito, "Modulo di Richiesta"), che integra una proposta contrattuale formulata dal Cliente;
b) Condizioni Generali di Contratto –Firma Digitale, redatte e predisposte in osservanza ed in conformità alle disposizioni contenute nel D.lgs. 206/2005 e nella L. 40/2007, hanno portata di carattere generale e potranno subire le modifiche rese necessarie da successive disposizioni di legge e/o regolamenti;
c) Manuale Operativo, nella versione pubblicata al momento della richiesta di fornitura della Firma Digitale, pubblicato a norma dell'art. 38, punto 2, del D.P.C.M. 13 gennaio 2004, che il Cliente è espressamente tenuto a consultare prima di inoltrare l'ordine della Firma Digitale.
Le pubblicazioni del Manuale sono disponibili in formato elettronico nel sito istituzionale del Certificatore, al link (http://www.pec.it/DocumentazioneFirmaDigitale.aspx, in formato elettronico e cartaceo presso il CNIPA (http://www.cnipa.it), in formato cartaceo presso ogni Centro di Registrazione Locale o Incaricato della Registrazione individuati al link http://www.pec.it/CDRLaccreditati.aspx.
3.2 Il Cliente prende atto ed accetta che l'invio online del Modulo di Richiesta, comporta l'accettazione delle presenti Condizioni Generali e del Manuale Operativo da esse richiamato, i quali avranno piena efficacia vincolante nei confronti del Cliente, indipendentemente dall'intervenuta conclusione del Contratto e successiva fornitura della Firma Digitale.

4. CONCLUSIONE DEL CONTRATTO
Il contratto si considera concluso con l'emissione del Certificato da parte del Certificatore.

5. CORRISPETTIVI, MODALITÀ DI PAGAMENTO E FATTURAZIONE
5.1 Il prezzo della Firma Digitale è individuato nell'offerta formulata dai Fornitori alla luce delle tariffe vigenti al momento dell'ordine ed indicata sul sito www.pec.it, e si differenzia in base alla tipologia diFirma Digitale scelta. A tutti gli importi fatturati sarà applicata l'Iva dovuta che, assieme a qualsiasi altro onere fiscale derivante dall'esecuzione del contratto, sarà a carico del Cliente. In ogni caso, il Cliente dichiara espressamente di sollevare ora per allora i Fornitori da ogni e qualsiasi responsabilità derivante dalle transazioni o dai pagamenti effettuati. Il Cliente non potrà far valere diritti o sollevare eccezioni di alcun tipo, se prima non avrà provveduto ad eseguire i pagamenti previsti dal contratto.
5.2 Il Cliente prende atto ed accetta che il pagamento della Firma Digitale deve essere eseguito a favore e nei confronti di Aruba con una delle le modalità indicate alla pagina http://www.aruba.it/recapiti.asp. In caso di pagamento con bollettino postale o bonifico bancario, il Cliente dovrà indicare nella relativa "causale" in maniera univoca e corretta il numero d'ordine e la tipologia diFirma Digitale acquistata; in assenza di una corretta ed univoca indicazione, i Fornitori non potranno essere ritenuti responsabili della mancata imputazione del pagamento all'ordine del Cliente e quest'ultimo non potrà avanzare alcuna pretesa o richiesta di risarcimento danni e/o indennizzo nei loro confronti, e comunque dichiara di rinunciarvi sin da ora. Il Cliente, tuttavia, potrà richiedere ai Fornitori di utilizzare tale credito per l'acquisto e/o il rinnovo di altri Servizi, con le modalità ed i termini indicati al successivo comma 4, al quale integralmente si rinvia anche in riferimento all'ipotesi di perdita credito.
5.3 Con l'accettazione delle presenti Condizioni Generali, il Cliente prende atto ed accetta che la fattura relativa alla Firma Digitale ordinata sia emessa esclusivamente da Aruba e che la medesima gli sia trasmessa e/o messa a disposizione in formato elettronico.
5.3 I Fornitori si riservano la facoltà di sospendere o disattivare, con effetto immediato, la Firma Digitale richiesto, nel caso in cui il pagamento del prezzo sia per qualsiasi motivo revocato o annullato dal Cliente oppure non sia eseguito, confermato o accreditato a beneficio della stessa Aruba.
5.4 I crediti eventualmente esistenti in favore del Cliente in forza della mancata fornitura della Firma Digitale, a qualsiasi causa dovuta, dovranno essere utilizzati da quest'ultimo per l'acquisto o il rinnovo di servizi erogati dai Fornitori entro e non oltre il periodo di dodici mesi dalla data del pagamento. Trascorso inutilmente il periodo di tempo sopra indicato, senza che il Cliente abbia utilizzato il predetto credito, questo si intenderà definitivamente acquisito ed incassato da parte dei Fornitori senza che il Cliente possa pretenderne la restituzione o l'utilizzazione.

6. RICHIESTA DI REGISTRAZIONE E RILASCIO DEL CERTIFICATO ED ATTIVAZIONE
6.1 La procedura di richiesta della Firma Digitale si differenzia per il Cliente Consumer ed il Cliente Business:
a) Il Cliente Consumer richiede la registrazione e l'emissione del Certificato di sottoscrizione mediante la procedura di ordine indicata sul sito www.pec.it, come precisato nel Manuale Operativo, compilando online l'apposito Modulo di Richiesta, inserendovi dati corretti e veritieri e trasmettendo ad Aruba la documentazione originale riepilogativa dell'Ordine costituita dal Modulo di Richiesta, appositamente sottoscritto dal Cliente, dai documenti dal medesimo richiamati, dalla documentazione attestante l'avvenuto pagamento del corrispettivo dovuto, dalla Dichiarazione Sostitutiva dell'Atto di Notorietà e dalla copia di un documento di identità del Cliente. Il riconoscimento de visu del Cliente Consumer sarà eseguito dal soggetto incaricato ai sensi del D.P.R. 445/2000 e la consegna della Firma Digitale avverrà nel luogo indicato in fase di ordine.
b) Il Cliente Business richiede la registrazione e l'emissione del Certificato di sottoscrizione mediante la procedura di ordine indicata sul sito www.pec.it, come precisato nel Manuale Operativo, accedendo online al form relativo all'Accordo di riferimento, mediante l'inserimento del codice identificativo della medesima a lui comunicato dal Contraente di proprio riferimento, e compilando l'apposito Modulo di Richiesta, inserendovi dati corretti e veritieri e trasmettendo ad Aruba la documentazione attestante l'avvenuto pagamento del corrispettivo dovuto. La documentazione originale riepilogativa dell'Ordine costituita dal Modulo di Richiesta, corredata di copia del documento di identità del Richiedente, dovrà essere da quest'ultimo sottoscritta presso il Contraente di riferimento che provvederà ad eseguire il riconoscimento de visu ed a curare la consegna della Firma Digitale.
6.2 Nello specifico, il Cliente si obbliga a comunicare ai Fornitori:
a) dati, documenti, informazioni corrette e veritiere, specificando tra le informazioni fornite quelle che intende escludere dal certificato;
b) l'esistenza di eventuali limitazioni nell'uso della coppia delle chiavi di certificazione (a titolo esemplificativo, poteri di rappresentanza, limitazioni di poteri, ecc.), comprovate da idonea documentazione;
c) tempestivamente ogni eventuale cambiamento delle informazioni o dei dati forniti.
Il Cliente, altresì, è tenuto a generare la coppia di chiavi di sottoscrizione in sicurezza e nel rispetto delle procedure indicate nel Manuale Operativo.
6.3 I Fornitori provvederanno al rilascio del Certificato, rispettando rigorosamente l'ordine cronologico delle richieste pervenute, purché assistite dal ricevimento della conferma circa l'avvenuto pagamento del corrispettivo della Firma Digitale rilasciata dall'Ente individuato come competente ad effettuare l'operazione, e dalla restante documentazione indicata al precedente comma. Il Certificato sarà rilasciato al Cliente solo in caso di esito positivo delle verifiche a tal fine necessarie; in caso di mancata emissione del Certificato, i Fornitori indicheranno al Cliente le ragioni che ne hanno determinato il mancato rilascio e provvederanno alla restituzione in favore del Cliente del 50% (cinquanta%) dell'importo dal medesimo versato a titolo di canone annuale per la Firma Digitale; resta inteso, e di ciò il Cliente prende atto ed accetta, che il residuo 50% (cinquanta%) sarà trattenuto dai Fornitori a titolo di indennità per le spese relative all'istruttoria di rilascio del Certificato.
6.4 I Fornitori comunicheranno al Cliente l'emissione del Certificato. Resta inteso che l'attivazione del Certificato sarà effettuata direttamente dal Cliente mediante l'apposita procedura di autenticazione.

7. DURATA E VALIDITÀ DEL CERTIFICATO
7.1 La durata del Certificato è indicata sul medesimo, nella sezione "validità (validity)".
7.2 All'approssimarsi della data di scadenza i Fornitori, a mero titolo di cortesia e quindi senza che così facendo si assumano alcuna obbligazione nei confronti del Cliente, avranno la facoltà di inviare alle caselle di posta elettronica indicate dal Cliente in fase di ordine avvisi di prossima scadenza del Certificato.

8. OBBLIGHI DEL CLIENTE
8.1 Gli obblighi del Cliente sono quelli indicati nel Manuale Operativo e nelle presenti Condizioni Generali.
8.2 Il Cliente, in considerazione della circostanza che l'utilizzo di una Firma digitale per cui sia stato emesso un Certificato di sottoscrizione, comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua

persona, è obbligato ad osservare la massima diligenza nell'utilizzo, conservazione e protezione della chiave privata, del dispositivo di firma e del codice di attivazione ad esso associato (PIN). In particolare, il Cliente è obbligato, ai sensi dell'art. 29 bis del T.U., ad adottare tutte le misure idonee ad evitare che, dall'utilizzo del sistema di chiavi asimmetriche o della Firma digitale, derivi danno ad altri. Il Cliente è tenuto, altresì, a proteggere la segretezza della Chiave privata non comunicando o divulgando a terzi il codice personale identificativo (PIN) di attivazione della stessa, provvedendo a digitarlo con modalità che non ne consentano la conoscenza da parte di altri soggetti e conservandolo in un luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente la chiave. La Chiave privata, per cui è stato rilasciato il certificato di sottoscrizione, è strettamente personale e non può essere per alcuna ragione ceduta o data in uso a terzi. Il Cliente prende atto di essere il responsabile esclusivo della protezione della propria Chiave privata da danni, perdite, divulgazioni, modifiche o usi non autorizzati. Il Cliente si impegna ad utilizzare la Firma Digitale in conformità a quanto indicato nel Contratto e nel sito istituzionale, nel rispetto della legge, della normativa vigente della morale e dell'ordine pubblico. A titolo esemplificativo ma non esaustivo, il Cliente si impegna a:

a) astenersi dal compiere ogni violazione dei sistemi e della sicurezza delle reti che possano dar luogo a responsabilità civile e/o penale;

b) non utilizzare la Firma Digitale in maniera tale da recare danno a se stesso o a terzi;

c) utilizzare la Firma Digitale per i soli usi consentiti dalla legge con divieto, a titolo meramente esemplificativo e non esaustivo, di inviare, trasmettere e/o condividere materiale:

c.1) che violi o trasgredisca diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti legali o consuetudinari;

c.2) che abbia contenuti contro la morale e l'ordine pubblico al fine di turbare la quiete pubblica e/o privata, di recare offesa o danno diretto o indiretto a chiunque;

c.3) a contenuto pedopornografico, pornografico o osceno e comunque contrario alla pubblica morale;

c.4) idoneo a violare o tentare di violare la riservatezza dei messaggi privati o finalizzato a danneggiare l'integrità delle risorse altrui o a provocare danno diretto o indiretto a chiunque (software pirata, cracks, keygenerators, serials, virus, worm, trojan Horse o altri componenti dannosi);

c.5) idoneo ad effettuare Spamming o azioni equivalenti;

d) garantire che i dati personali comunicati ai Fornitori per l'integrale esecuzione del contratto siano corretti, aggiornati e veritieri e permettano di individuare la sua vera identità. Il Cliente prende atto ed accetta che, qualora abbia fornito dati falsi, non attuali o incompleti, i Fornitori si riservano il diritto di sospendere/disattivare la Firma Digitale, trattenendo le somme pagate dal Cliente e riservandosi il diritto di chiedere il risarcimento del maggior danno; resta inteso che il Cliente non potrà avanzare ai Fornitori alcuna richiesta di rimborso, indennizzo e/o risarcimento danni per il tempo in cui non ha usufruito della Firma Digitale;

e) manlevare e tenere indenne i Fornitori, da qualunque responsabilità in caso di denunce, azioni legali, azioni amministrative o giudiziarie, perdite o danni (incluse spese legali ed onorari) scaturite dall'uso illegale della Firma Digitale da parte del Cliente stesso.

8.3 Il Cliente è altresì responsabile dei danni derivanti ai Fornitori e/o a terzi nel caso di ritardo di attivazione da parte sua delle procedure previste dal Manuale Operativo per la revoca e/o la sospensione del Certificato.

8.4 Qualora il Cliente, al momento dell'identificazione abbia, anche mediante l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto, o comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, Egli prende atto ed accetta che sarà ritenuto penalmente responsabile per le dichiarazioni mendaci e/o l'utilizzo di falsa documentazione e sarà altresì considerato esclusivamente responsabile di tutti i danni subiti e subendi dal Certificatore e/o da terzi dall'inesattezza e/o falsità delle informazioni contenute nel certificato, assumendo sin da ora l'obbligo di manlevare e mantenere indenne i Fornitori da ogni eventuale pretesa, azione e/o richiesta di indennizzo o risarcimento danni che dovesse essere avanzata da chiunque nei loro confronti.

8.5 In caso di violazione anche di uno soltanto dei suddetti obblighi/impegni, i Fornitori avranno facoltà di intervenire nelle forme e nei modi ritenuti opportuni per eliminare, ove possibile, la violazione ed i suoi effetti, e di sospendere/disattivare immediatamente e senza alcun preavviso la Firma Digitale. I Fornitori tratterranno le somme pagate dal Cliente a titolo di risarcimento, fatto salvo in ogni caso il risarcimento del maggior danno. Il Cliente prende atto ed accetta che nulla avrà da pretendere dai Fornitori a titolo di rimborso, indennizzo o risarcimento danni per i provvedimenti che gli stessi stessa avranno ritenuto opportuno adottare. In ogni caso, il Cliente si assume, ora per allora, ogni responsabilità in merito alle violazioni di cui sopra e si impegna a manlevare e tenere indenne i Fornitori da ogni e qualsiasi responsabilità, spesa, pregiudizio o danno, diretto o indiretto, derivanti da pretese o azioni da parte di terzi di cui i Fornitori siano chiamati a rispondere nei confronti dei terzi per fatto imputabile del Cliente, ivi incluse, a titolo esemplificativo e non esaustivo, le responsabilità e i danni derivanti dall'eventuale erroneità o non attualità delle informazioni o dei dati rilasciati ai Fornitori, dal non corretto utilizzo delle procedure descritte nel Manuale Operativo.

9. OBBLIGHI E LIMITAZIONI DI RESPONSABILITA' DEI FORNITORI

9.1 Gli obblighi del Certificatore sono quelli indicati nel Manuale Operativo. I Fornitori non assumono obblighi ulteriori a quelli previsti nelle presenti Condizioni Generali, nel Manuale Operativo, e nelle leggi vigenti in materia di attività di certificazione.

9.2 I Fornitori non prestano alcuna garanzia in caso di uso improprio e/o non corretto della Firma Digitale rispetto a quanto stabilito dalle norme italiane vigenti e dal Manuale Operativo. I Fornitori non prestano alcuna garanzia sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dall'Cliente, sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali, sulla validità e rilevanza, anche probatoria, del certificato di sottoscrizione o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il Certificato è riferito nei confronti di soggetti sottoposti a legislazioni differenti da quella italiana, sulla loro segretezza e/o integrità (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili dall'Cliente o dal destinatario attraverso l'apposita procedura di verifica).

9.3 Il Cliente dichiara di aver letto ed accettato le limitazioni di responsabilità di cui al Manuale Operativo. Salvo i casi di dolo o colpa grave, i Fornitori non saranno responsabili di alcun danno nei confronti del Cliente e/o comunque nei confronti di terzi. I Fornitori non rispondono per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informativo. In ogni caso i Fornitori non rispondono di danni cagionati al Cliente e/o a terzi, trascorso il termine di decadenza di 10 (dieci) giorni dall'evento dannoso, ovvero dalla sua scoperta comunicato nelle forme indicate nel Manuale Operativo.

9.4 In nessun caso i Fornitori potranno essere ritenuti responsabili per i danni diretti o indiretti da chiunque subiti, ivi compreso il Cliente:

a) causati per uso improprio della Firma Digitale o per mancato rispetto delle regole e degli obblighi descritti nelle presenti condizioni contrattuali, nel manuale operativo della società Aruba Pec e nel sito www.pec.it;

b) derivanti da impossibilità della prestazione, mancato funzionamento di reti o apparati tecnici, cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni ecc.);

c) di qualsiasi natura ed entità patiti dal Cliente e/o da terzi causati da manomissioni o interventi sulla Firma Digitale o sulle apparecchiature effettuati dal Cliente e/o da parte di terzi non autorizzati dai Fornitori.

10. HARDWARE E SOFTWARE PER IL FUNZIONAMENTO DEL CERTIFICATO

Qualora richiesto dal Cliente, il Certificatore, direttamente o a mezzo degli Operatori di Registrazione o Incaricati di Registrazione, consegnerà a questi, previa corresponsione del relativo costo, un dispositivo (hardware-Smart Card e/o lettore) di firma in grado di conservare e leggere la Chiave privata dello stesso e generare al proprio interno le firme digitali, nonché dispositivi software a valore aggiunto.

11. ASSISTENZA

Il servizio di assistenza clienti viene erogato con le modalità previste nel manuale operativo ed indicate sul sito www.pec.it, al quale integralmente si rinvia.

12. RINVIO AL MANUALE OPERATIVO

Per quanto non espressamente indicato negli articoli precedenti si rinvia a quanto stabilito nel manuale operativo predisposto da Aruba Pec e nel sito www.pec.it che costituiscono parte integrante e sostanziale del presente contratto.

13. COMUNICAZIONI.

13.1 Ogni comunicazione scritta dovrà essere inviata dal Cliente ai recapiti dei Fornitori indicati nelle presenti Condizioni.

13.2 Qualora nel Modulo di Richiesta il Cliente abbia indicato un indirizzo e-mail, questo sarà considerato indirizzo elettronico ai sensi dell'art. 14, 1° comma del T.U., e tutte le comunicazioni saranno a lui validamente inviate presso il medesimo. In caso di mancata indicazione dell'indirizzo di posta elettronica, le comunicazioni saranno inviate all'indirizzo indicato dal Cliente nel Modulo di Richiesta.

14. MODIFICHE DEI SERVIZI E VARIAZIONI ALLE CONDIZIONI DELL'OFFERTA

14.1 Il Cliente prende atto ed accetta che la Firma Digitale oggetto del presente contratto è caratterizzata da tecnologia in continua evoluzione, per questi motivi i Fornitori si riservano il diritto di inserire nuove offerte, di modificare e/o togliere quelle inizialmente presenti, di modificare le caratteristiche della Firma Digitale, di variare le condizioni, anche economiche, dell'offerta, in qualsiasi momento e senza preavviso, quando ciò sia reso necessario dall'evoluzione tecnologica.

14.2 I Fornitori si riservano la facoltà di modificare in qualsiasi momento e senza preavviso la tipologia e le caratteristiche della Firma Digitale ovvero qualsiasi altra condizione della fornitura. In ogni caso le Firme Digitali attivate o rinnovate precedentemente alla data della variazione saranno mantenute, fino alla loro prima scadenza, alle condizioni pattuite.

14.3 Qualora i Fornitori modifichino le presenti Condizioni Generali, dette modifiche saranno comunicate al Cliente mediante pubblicazione sul sito istituzionale. Le predette modifiche avranno effetto decorsi 30 (trenta) giorni dalla data della loro comunicazione. Nello stesso termine il Cliente, qualora usufruisca del servizio di Firma Digitale Remota, potrà esercitare la facoltà di recedere dal contratto con comunicazione scritta inviata a mezzo posta elettronica certificata (PEC) o tramite raccomandata a.r. provvedendo a richiedere la revoca del certificato emesso in suo favore e specificando la volontà di recedere. Dalla data del recesso il Cliente è obbligato a non utilizzare il il servizio di Firma Digitale Remota precedentemente attivato in Suo favore. In mancanza di esercizio della facoltà di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le variazioni si intenderanno da questi definitivamente conosciute ed accettate.

14.4 Il Certificatore si riserva il diritto di effettuare modifiche alle previsioni del Manuale Operativo per sopravvenute esigenze tecniche, legislative e gestionali, che saranno efficaci nei confronti del Cliente decorsi 30 (trenta) giorni dalla comunicazione mediante la sua pubblicazione sul sito istituzionale.

15. RISOLUZIONE DEL CONTRATTO, CLAUSOLA RISOLUTIVA ESPRESSA

Qualora il Cliente usufruisca del servizio di Firma Digitale Remota, il presente contratto si risolve automaticamente, con conseguente sospensione/disattivazione della Firma Digitale, in caso di revoca del certificato. I Fornitori altresì hanno facoltà, ai sensi e per gli effetti dell'Art. 1456 Cod. Civ., di risolvere il presente contratto, qualora il Cliente violi in tutto o in parte le disposizioni di cui agli artt. 6 e 8 del presente contratto. Nelle ipotesi sopra indicate, la risoluzione si verifica di diritto mediante dichiarazione unilaterale dei Fornitori, con lettera raccomandata a.r. inviata al Cliente, per effetto della quale gli stessi saranno autorizzati a revocare il certificato senza alcun preavviso. In tali ipotesi, il Cliente prende atto ed accetta che le somme pagate dal medesimo saranno trattenute dai Fornitori a titolo di penale, fatto salvo in ogni caso il risarcimento del maggior danno, senza che lo stesso possa avanzare alcuna richiesta di rimborso, indennizzo e/o risarcimento danni per il periodo in cui non ha usufruito del certificato. Resta inteso che la risoluzione di diritto sopra indicata opera senza pregiudizio per le altre ipotesi di risoluzione previste dalla legge.

16. RECESSO

16.1 Il Cliente prende atto ed accetta che la Firma Digitale acquistata nell'opzione del Kit di Firma Digitale, prevedendo la fornitura di un prodotto personalizzato, rientra nella previsione di cui all'art. 55 del D.lgs. 206/2005 e che, pertanto, non è ammesso l'esercizio del diritto di recesso. L'ordine può essere bloccato ed eventualmente disdetto qualora la produzione ad esso relativa non sia stata ancora in alcun modo avviata; in tal caso il Cliente avrà diritto ad ottenere esclusivamente la restituzione del corrispettivo versato.

16.2 Il Cliente prende atto ed accetta che nel caso in cui abbia acquistato la Firma Digitale nell'opzione della Firma Digitale Remota, e qualora sia qualificabile come "consumatore" ed identificato, ai sensi dell'Art. 3 del D.lgs. 206/2005 (cd. "Codice del Consumo"), nella persona fisica che agisce per scopi estranei alla propria attività imprenditoriale o professionale, avrà facoltà di recedere dal presente Contratto in qualsiasi momento, senza alcuna penalità e senza indicarne le ragioni, con comunicazione scritta inviata a mezzo raccomandata a.r. ai Fornitori, o ad uno di essi. Il recesso avrà efficacia decorsi 30 (trenta) giorni dalla data di ricevimento della predetta comunicazione ed i Fornitori provvederanno a disattivare il Servizio. Nel caso in cui il Cliente richieda, altresì, il rimborso del prezzo del servizio per i giorni non utilizzati fino alla successiva scadenza naturale del rapporto, i Fornitori provvederanno ad effettuare detto rimborso con esclusione dei costi già sostenuti, conformemente a quanto stabilito dall'art. 1 comma 3 del Legge 40/2007. Resta inteso, e di ciò il Cliente prende atto ed accetta, che la facoltà di recesso prevista al presente comma è riconosciuta, in conformità al D.lgs. 206/2005 ed alla L. 40/2007, solo ai Clienti che siano qualificabili come consumatori e solo a coloro che abbiano acquistato il servizio di Firma Digitale Remota.

16.3 È esclusa la disdetta anticipata del contratto, eccezion fatta per i casi ivi espressamente previsti. In caso di disdetta, recesso o risoluzione illegittimi da parte del Cliente, i Fornitori sono sin d'ora autorizzati a trattenere le somme pagate dal Cliente a titolo di penale salvo il risarcimento del maggior danno.

16.4 In caso di servizio di Firma Digitale Remota, i Fornitori avranno facoltà di recedere dal presente contratto in qualsiasi momento e senza obbligo di motivazione con preavviso di 10 (dieci) giorni inviato tramite comunicazione scritta. In caso di esercizio della facoltà di recesso, trascorso il termine di preavviso sopra indicato i Fornitori potranno in qualsiasi momento disattivare e/o disabilitare il certificato. In tale ipotesi i Fornitori restituiranno al Cliente il rateo del prezzo del servizio di Firma Digitale Remota corrispondente ai giorni non utilizzati fino alla successiva scadenza naturale del rapporto, detratte le spese sostenute per la fornitura del servizio di Firma Digitale Remota, restando esplicitamente escluso ogni e qualsiasi altro rimborso o indennizzo o responsabilità dei Fornitori stessi o di chi avrà avuto parte nella fornitura del servizio di Firma Digitale Remota per il mancato utilizzo da parte del Cliente dei certificati nel periodo residuo.

17. REVOCA E SOSPENSIONE DEL CERTIFICATO

17.1 I presupposti, le procedure e la tempistica per la revoca o la sospensione del Certificato di sottoscrizione sono stabiliti oltre che nel presente articolo, nel Manuale Operativo. Il Certificatore provvederà alla revoca ovvero alla sospensione del Certificato qualora si verifichi una delle seguenti circostanze:
a) richiesta esplicita formulata dal titolare del Certificato per iscritto;
b) richiesta da parte del "terzo interessato" (che deve essere inoltrata per iscritto ai sensi di quanto previsto all'art. 20 D.P.C.M.);
c) richiesta nei casi di urgenza (in tutti i casi di smarrimento e/o furto del dispositivo di firma) formulata telefonicamente dal titolare del Certificato o "terzo interessato", identificati mediante il codice riservato per l'autenticazione rilasciatogli al momento della emissione del Certificato;
d) riscontro che il Certificato non è stato rilasciato secondo le modalità previste dal Manuale Operativo ovvero in maniera non conforme alle modalità previste dalla normativa vigente;
e) riscontro di una avvenuta violazione degli obblighi incombenti sul richiedente e/o sul titolare del Certificato;
f) compromissione della segretezza e/o rottura della chiave privata;
g) smarrimento della chiave privata;
h) abusi e falsificazioni;
i) richiesta proveniente dall'Autorità Giudiziaria.
In riferimento all'art. 19, comma 4, del D.P.C.M., il Certificatore provvede ad inserire in stato di sospensione il Certificato (e quindi a sospenderne la validità) nel caso in cui non possa accertare in tempo utile l'autenticità della richiesta.

17.2 I Certificati relativi a chiavi di certificazione possono essere revocati o sospesi nei seguenti casi:
a) smarrimento, sottrazione, furto, compromissione della chiave segreta;
b) guasto del dispositivo di firma;
c) cessazione dell'attività.
In tale casi il Titolare è obbligato (anche nel proprio interesse) a darne tempestiva comunicazione al Certificatore il quale attiverà le procedure di revoca o sospensione del Certificato.

17.3 La revoca/sospensione del certificato può essere effettuata dal suo titolare mediante tre diverse modalità:
a) l'invio per iscritto di una esplicita richiesta formale inviata al Certificatore, la quale deve contenere le indicazioni relative agli elementi di identificazione del Titolare e del certificato, le ragioni per le quali si richiede la revoca/sospensione ed essere firmata dal Titolare del certificato;
b) il servizio disponibile presso il sito di Aruba Pec alla pagina del web server Firma Digitale esplicitamente dedicata alla revoca/sospensione evidenziata sulla pagina principale, utilizzando il codice riservato di emergenza inviato da Aruba Pec durante la fase di generazione del Certificato;
c) il servizio telefonico, disponibile ai recapiti indicati al link http://www.pec.it/Contacts.aspx, comunicando il codice riservato di emergenza inviato dai Fornitori durante la fase di invio del certificato a seguito della generazione. A detta richiesta dovrà comunque seguire comunicazione scritta con l'indicazione delle ragioni per le quali si richiede la revoca/sospensione, firmata dal Titolare del certificato.

17.4 La revoca/sospensione del certificato può essere effettuata ad insindacabile iniziativa del Certificatore, indipendentemente dalla volontà del Titolare, qualora se ne ravvisi la necessità o si verifichi una delle seguenti circostanze:
a) sopravvenuta modifica dei dati personali riportati sul Certificato o di altri dati riportati sul Certificato;
b) conoscenza dell'avvenuta compromissione o rottura della chiave privata;
c) inadempimento agli obblighi incombenti sul Titolare del Certificato e previsti dalla normativa vigente e/o dal Manuale Operativo;
d) uso improprio della Firma Digitale da parte del Titolare;
e) eventuale compromissione della chiave di certificazione o marcatura temporale relativa al Certificato;
f) eventuale richiesta motivata proveniente dall'Autorità Giudiziaria.
Il Certificatore provvederà a notificare al Titolare le ragioni della revoca, nonché la data e l'ora dalla quale il Certificato non è più valido.

17.5 La revoca/sospensione del certificato può essere effettuata a richiesta del Terzo interessato. In questo caso la richiesta di sospensione o revoca deve essere firmata e pervenire per iscritto a Aruba Pec. Ove espressamente previsto, la richiesta può anche essere inoltrata via e-mail purché debitamente sottoscritta con il certificato digitale del "terzo interessato" ove ne sia stato previsto il rilascio. Nei casi di particolare urgenza il "terzo interessato" potrà richiedere la revoca/sospensione del certificato mediante il servizio telefonico disponibile ai recapiti indicati al link http://www.pec.it/Contacts.aspx, comunicando il codice riservato di emergenza inviato da Aruba Pec durante la fase di invio del certificato a seguito della generazione. A detta richiesta dovrà comunque seguire comunicazione scritta a mezzo posta o e-mail - sottoscritta con firma digitale - con le ragioni per le quali si richiede la revoca/sospensione. A mero titolo esemplificativo, i casi più frequenti in cui un "terzo interessato" può richiedere la sospensione o la revoca di un certificato sono qualora il terzo sia una organizzazione (ente, società, associazione, ecc) che abbia acquistato una serie di certificati e li abbia destinati a suoi dipendenti e/o fornitori e/o clienti e/o a persone, in qualunque modo, ad essa afferenti e:
a) siano modificati o terminati i rapporti tra la organizzazione ed il Titolare del certificato per qualsiasi motivo;
b) si siano verificati casi di dolo e/o infedeltà del dipendente per il quale la organizzazione ha richiesto il Certificato;
c) si sia verificato il decadere del titolo o della carica o del ruolo inerente i poteri di rappresentanza o la qualifica professionale in virtù del quale il certificato è stato rilasciato.
Il Certificatore provvederà a comunicare al titolare del Certificato l'avvenuta richiesta di revoca e/o sospensione effettuata dal "terzo interessato". Aruba Pec può rigettare la richiesta nel caso la giudichi non autentica, inesatta o incompleta e provvederà alla notifica del rigetto al "terzo interessato" richiedente.

17.6 In ogni caso, è facoltà del Certificatore sospendere/disattivare il certificato in caso di manomissione delle chiavi di certificazione ovvero qualora ritenga che siano state violate le procedure del Manuale Operativo. In caso di revoca del Certificato, per qualsiasi motivo, nessuno escluso e/o eccettuato, il Cliente non ha diritto alla restituzione di quanto versato.

18. INFORMATIVE EX ART. 5, 52, 53, 64 E SS. DEL D.LGS. 206/2005 ED EX ART. 7 D.LGS. 70/2003

Ai sensi di quanto previsto dagli artt. 5, 52, 53 e 64 e ss. D.lgs. 206/2005 il Cliente prende atto che:
a) Fornitori sono Aruba Pec S.p.A. con sede in Via Sergio Ramelli n. 8, 52100 Arezzo, REA 145843, P.Iva. 01879020517, ed Aruba S.p.A. con sede in Piazza Garibaldi n. 8, 52010 Soci (Arezzo), REA 118045, P.Iva. 01573850516;
b) il Servizio, prevedendo la fornitura di un prodotto personalizzato, rientra nella previsione di cui all'art. 55 del D.lgs. 206/2005 e pertanto non è ammesso l'esercizio del diritto di recesso, come indicato al precedente Art. 16. L'ordine può essere bloccato ed eventualmente disdetto solo qualora la produzione ad esso relativa non sia stata ancora in alcun modo avviata; in tal caso il Cliente avrà diritto ad ottenere esclusivamente la restituzione del corrispettivo versato ai Fornitori;
c) eventuali reclami possono essere inviati a uno dei Fornitori, o a ciascuno di essi, tramite PEC o posta raccomandata a.r. inviata alle rispettive sedi legali;
d) il servizio di assistenza tecnica previsto per i singoli servizi è descritto al precedente art. 11;

19. DISPOSIZIONI FINALI E COMUNICAZIONI

19.1 I rapporti tra i Fornitori ed il Cliente stabiliti dalle presenti Condizioni Generali non possono essere intesi come rapporti di mandato società, rappresentanza, collaborazione o associazione o altri contratti simili o equivalenti.

19.2 Nessuna modifica, postilla o clausola comunque aggiunta al presente contratto sarà valida se non specificatamente approvata per iscritto da tutte le parti contrattuali.

19.3 Tutte le comunicazioni al Cliente relative al presente rapporto contrattuale potranno essere effettuate dai Fornitori a mano, tramite e-mail, a mezzo di lettera raccomandata a.r., posta ordinaria oppure a mezzo telefax agli indirizzi comunicati dal Cliente e, in conseguenza, le medesime si considereranno da questi conosciute. Eventuali variazioni degli indirizzi del Cliente non comunicate ai Fornitori non saranno a loro opponibili.

19.5 L'eventuale inefficacia e/o invalidità totale o parziale di uno o più articoli del contratto non comporterà l'invalidità degli altri articoli i quali dovranno ritenersi validi ed efficaci. La disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

19.6 Eventuali reclami in merito alla fornitura della Firma Digitale ordinata dal Cliente, dovranno essere inoltrati a uno dei Fornitori, o a ciascuno di essi, tramite PEC o tramite posta raccomandata a.r. inviata alle rispettive sedi legali, il Fornitore ricevente il reclamo lo esaminerà e fornirà risposta scritta entro 60 (sessanta) giorni dal ricevimento dello stesso. Nel caso di reclami per fatti di particolare complessità, che non consentano una risposta esauriente nei termini di cui sopra, il Fornitore informerà il Cliente entro i predetti termini sullo stato di avanzamento della pratica.

20. LEGGE APPLICABILE

Per quanto non espressamente previsto nelle presenti Condizioni Generali si rinvia, nei limiti in cui ciò sia compatibile, alle norme di legge italiane vigenti al momento della conclusione del contratto.

21. FORO COMPETENTE

Per ogni e qualsiasi controversia relativa all'interpretazione, esecuzione e risoluzione del presente contratto sarà esclusivamente competente il Foro di Arezzo, salvo il caso in cui il Cliente abbia agito e concluso il presente contratto in qualità di Consumatore per scopi estranei all'attività imprenditoriale o professionale svolta; in tal caso sarà esclusivamente competente il Foro del luogo dove il Cliente ha la propria residenza o domicilio, se ubicati sul territorio dello stato italiano.

Clausole vessatorie

Ai sensi e per gli effetti degli art. 1341 e 1342 c.c., il Cliente dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le clausole seguenti: 3) Struttura del contratto; 5) Corrispettivi, modalità di pagamento e fatturazione; 6) Richiesta di registrazione e rilascio del certificato ed attivazione; 7) Durata del contratto e validità del certificato; 8) Obblighi del Cliente; 9) Obblighi e limitazioni di responsabilità dei Fornitori; 14) Modifiche dei servizi e variazioni alle condizioni dell'offerta; 15) Risoluzione del contratto, clausola risolutiva espressa; 16) Recesso; 17) Revoca e sospensione del certificato; 21) Foro competente.

Informativa sul trattamento dei dati personali

Si informa il Cliente che il D.lgs. 196/2003 prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Secondo le leggi indicate, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza tutelando la riservatezza e i diritti del sottoscrittore. Le seguenti informazioni sono fornite ai sensi dell'Art. 13 del D.lgs. 196/2003.
Il trattamento che intendiamo effettuare:
a) ha la finalità di concludere, gestire ed eseguire i contratti di fornitura dei servizi richiesti; di organizzare, gestire ed eseguire la fornitura dei servizi anche mediante comunicazione dei dati a terzi Fornitori o a società del gruppo Aruba; di assolvere agli obblighi di legge o agli altri adempimenti richiesti dalle competenti Autorità;
b) sarà effettuato con le modalità informatizzato/manuale;
c) salvo quanto strettamente necessario per la corretta esecuzione del contratto di fornitura, i dati non saranno comunicati ad altri soggetti, se non chiedendo espressamente il Suo consenso.
Informiamo ancora che la comunicazione dei dati è indispensabile ma non obbligatoria e l'eventuale rifiuto non ha alcuna conseguenza, ma potrebbe comportare il mancato puntuale adempimento delle obbligazioni assunte da Aruba Pec S.p.A. e da Aruba S.p.A. per la fornitura della Firma Digitale da Lei richiesto. I titolari del trattamento sono Aruba Pec S.p.A. con sede in Via Sergio Ramelli n. 8, 52100 Arezzo ed Aruba S.p.A., con sede legale in Piazza Garibaldi 8, 52010 Soci (Arezzo), alle quali può rivolgersi per far valere i Suoi diritti così come previsto dall'Art. 7 del D.lgs. 196/2003, che riportiamo di seguito per esteso:
Art. 7 - Diritto di accesso ai dati personali ed altri diritti
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Formula di consenso

Il Cliente dichiara di aver preso visione dell'Informativa resa dai Fornitori ai sensi dell'Art. 13 D.lgs. 196/2003, e di rilasciare il proprio consenso al trattamento dei dati personali per le finalità e con le modalità ivi indicate. Il Cliente dichiara, altresì, di essere consapevole che in mancanza di rilascio del consenso a tale trattamento potranno trovare applicazione le disposizioni indicate nella predetta Informativa.

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

Direttore Generale

COMUNE DI ROSATE
01 SET. 2015
PROT. N. 6594
Cat. I Cl. 7

A
MAGGIOLI S.p.a
Via del Carpino n. 8
47822 Santarcangelo di Romagna (RN)
PEC: segreteria@maggioli.legalmail.it

Oggetto

Accreditamento a svolgere la conservazione dei documenti informatici di cui all'art. 44-bis comma 1 del decreto legislativo 7 marzo 2005, n. 82 e s.m.i e iscrizione nell'elenco dei conservatori accreditati di cui all'art.1 della Circolare AgID n. 65 del 10 aprile 2014.

Riferimenti:

a) Domanda del 30 giugno 2015, acquisita agli atti in pari data con prot. n. 5605.

b) Nota del 24 luglio 2015, acquisita agli atti in pari data con prot. n. 6343.

Si fa seguito alla domanda e alla nota in riferimento e si comunica che, in esito alla positiva conclusione della fase istruttoria, in data 27 luglio 2015 è stato deliberato l'accreditamento di codesta Società ai sensi delle disposizioni in oggetto e la conseguente iscrizione nell'elenco dei conservatori accreditati pubblicato sul sito dell'Agenzia per l'Italia Digitale.

Pertanto, a decorrere da tale data, codesta Società è accreditata a svolgere le attività di conservazione dei documenti informatici.

Si ricorda che i conservatori accreditati sono soggetti ad attività di vigilanza da parte dell'Agenzia per l'Italia Digitale volta a verificare il permanere dei requisiti dimostrati in fase di accreditamento. Si richiamano a tal fine gli obblighi a carico dei conservatori accreditati indicati al paragrafo 5 della Circolare AgID n. 65/2014.

Antonio Samaritani

Firmato digitalmente da ANTONIOMARIA SAMARITANI
ND: c=IT, o=Ministero della Difesa/97355240587, ou=Personale Civile, sn=SAMARITANI, givenName=ANTONIOMARIA, serialNumber=IT:SMRNTN63R08L219Z, cn=ANTONIOMARIA SAMARITANI, dnQualifier=ZZAA00131
Data: 2015.07.29 17:33:49 +02'00'

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t+39 06 85264.1
pec protocollo@pec.agid.gov.it
direzione.generale@agid.gov.it

Allegato delibera ~~C.C.~~/G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 8

Registro protocollo di emergenza

NUMERO REGISTRO EMERGENZA	DATA	TIPO	MITTENTE/DESTINATARIO	OGGETTO	CLASSIFICAZIONE			
					CATEGORIA	CLASSE	SOTTO CLASSE	FASCICOLO

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 8.1

AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO DI EMERGENZA

(art. 63 D.P.R. n.445/2000)

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445 preso atto che, per le cause sotto riportate:

DATA INTERRUZIONE	
ORA INTERRUZIONE	
CAUSA DI INTERRUZIONE	

non è possibile utilizzare la normale procedura informatica si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Il Responsabile del Settore

Allegato delibera C.C./G.M.
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 9

LINEE GUIDA PER LE PUBBLICAZIONI ALL'ALBO ONLINE

1 - Oggetto ed ambito di applicazione

1.1. La Legge n. 69/2009 (art.32, comma 5) così come modificata dalla legge n.25/2010, ha stabilito che le pubblicazioni effettuate in forma cartacea, dal 1° gennaio 2011, non hanno effetto di pubblicità legale; l'eventuale pubblicazione cartacea ha solo finalità integrativa. Pertanto gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione, da parte delle amministrazioni e degli enti pubblici obbligati, nei propri siti informatici.

1.2. - L'Albo on-line tiene conto anche delle ultime disposizioni, imposte dalle recenti modifiche al Codice dell'Amministrazione Digitale (D.Lgs "Modifiche e integrazioni al D.Lgs. n.82/05 a norma dell'art.33 della Legge n. 69/09") e dal vigente Codice Privacy.

1.3. - La pubblicazione all'albo on-line sostituisce ogni altra forma di pubblicazione legale, salvo i casi previsti da leggi o regolamenti.

1.4. - La responsabilità della redazione dei documenti da pubblicare all'albo on-line e del loro contenuto è in capo ai Responsabili di Settore o ai titolari di Posizione Organizzativa a ciò delegati.

1.5. - I documenti sono visualizzati dal sistema in ordine cronologico di pubblicazione.

1.6. - Limitatamente al periodo di pubblicazione, l'acquisizione da parte degli utenti del sito web dell'Ente avviene gratuitamente e senza formalità.

1.7. - E' possibile consultare l'albo on-line presso l'Ente.

1.8. - Il sistema garantisce il diritto all'oblio e la temporaneità delle pubblicazioni.

2 - Gestione del servizio

2.1 - La pubblicazione dei documenti avviene in forma integrale, per estratto, per omissis o mediante avviso.

2.2 - Il periodo di pubblicazione è di quindici giorni interi e consecutivi, salvo termini diversi previsti da leggi, da regolamenti o stabiliti dall'Ente stesso. La pubblicazione si intende soddisfatta se un documento è rimasto disponibile sul sito complessivamente per almeno 12 ore per ciascun giorno di pubblicazione. Il periodo di pubblicazione è prorogato di un giorno per ciascun giorno di pubblicazione inferiore a dodici ore, in base all'attestazione del Responsabile dei Sistemi informativi.

2.3 - Durante il periodo di pubblicazione il sistema impedisce l'indicizzazione dei documenti e la ricerca ubiquitaria da parte di motori di ricerca o altri sistemi informatici esterni all'Ente.

2.4 - Al termine della pubblicazione il sistema ritira automaticamente il documento pubblicato.

2.5 - Le modalità di conservazione del Registro dell'albo on-line e dei documenti allegati sono descritte nel Manuale di gestione; i tempi di conservazione dei documenti pubblicati sono quelli previsti dal Piano di conservazione (Massimario).

2.6 - Mediante affissioni all'albo, sono pubblicati:

- le deliberazioni di consiglio e di giunta e le ordinanze;
- le determinazioni;
- gli avvisi di convocazione del consiglio;
- gli avvisi di gara;
- i bandi di concorso;
- l'albo dei beneficiari di provvidenze di natura economica;
- gli atti destinati ai singoli cittadini, quando i destinatari risultino irreperibili al momento della consegna;

- tutti gli ulteriori atti o documenti che per disposizioni di legge, di regolamento o su richiesta devono essere pubblicati ufficialmente mediante affissione all'albo, per la durata stabilita nelle predette norme o richieste.

3 - Pubblicazione degli atti dell'Amministrazione

3.1 – I responsabili di settore e i responsabili di procedimento accedono al sistema informatico di gestione dell'albo pretorio online e provvedono alle pubblicazioni degli atti prodotti di cui sono pienamente responsabili e a redigere la relata di pubblicazione a propria firma. Tale funzione può essere delegata ad altro dipendente del proprio settore.

Le deliberazioni della Giunta Comunale e del Consiglio Comunale sono pubblicate all'albo pretorio online dal Messo Comunale e, su sua attestazione, il Segretario Comunale sottoscrive la relata di pubblicazione.

L'originale del documento con la relativa relata di pubblicazione deve essere conservato nel rispettivo fascicolo informatico. Nel caso in cui il documento sia in forma analogica, il responsabile di procedimento deve provvedere alla produzione di una copia informatica secondo le procedure previste dall'articolo 23 del CAD.

3.2 - Nel caso di pubblicazione di un estratto, il documento integrale deve essere conservato nel fascicolo originario.

3.3 - Di norma i formati per la pubblicazione sono PDF e PDF/a.

4 - Pubblicazioni per conto di pubbliche amministrazioni o altri soggetti

4.1 - L'ente provvede alla pubblicazione all'Albo dei documenti provenienti da pubbliche Amministrazioni o da altri soggetti. Il richiedente la pubblicazione deve fornire il documento informatico sottoscritto con firma digitale e nel formato PDF. Nel caso di pubblicazione di una copia di originale analogico, il richiedente dovrà fornire la copia informatica prodotta secondo le modalità descritte nell'articolo 3.1.3

4.2 - Di norma, salvo che non sia prevista da legge, o comunque espressamente richiesto, l'Ente non dà comunicazione scritta dell'avvenuta pubblicazione, che potrà però essere verificata tramite la consultazione del sito web, sul quale è anche pubblicato il documento con gli estremi temporali di pubblicazione.

5 - Elementi obbligatori per la registrazione

5.1 - Gli elementi obbligatori e immodificabili della registrazione sono quelli previsti per il registro di protocollo informatico di cui agli artt. 53-57 del DPR 445/2000 e dal Manuale di gestione; inoltre dovranno essere obbligatoriamente indicate le date iniziali e finali di pubblicazione.

5.2 - Le integrazioni o l'annullamento di una pubblicazione avvengono con le stesse modalità previste dall'art. 54 del DPR 445/2000 e dal Manuale di Gestione.

6 - Visione degli atti, rilascio copie

6.1 - Il diritto di accesso agli atti pubblicati all'Albo on-line si esercita qualora la loro integrale conoscenza non sia possibile attraverso la pubblicazione allo stesso Albo.

6.2 - Per i presupposti, i limiti e le modalità tendenti ad ottenere la copia dell'atto si applicano le disposizioni previste dalla Legge 241/1990 e s.m.i., dal D.P.R. 184/1996 e, per quanto non disciplinato nel- le predette fonti, dal Linee guida dell'Ente per l'accesso agli atti.

7 - Sicurezza e riservatezza delle pubblicazioni

7.1 - Le modalità di pubblicazione all'Albo on-line degli atti e dei dati personali in essi contenuti, devono avere caratteristiche di sicurezza ed inviolabilità conformi alle misure previste dagli articoli 31 e seguenti del D.Lgs. n.196/2003 e dall'art. 51 del D.Lgs. n. 82/2005;

7.2 - L'accesso agli atti pubblicati all'Albo on-line dovrà essere consentito in modalità di sola lettura. Gli stessi potranno essere scaricabili dall'Albo on-line, in un formato tale da impedire qualsiasi alterazione del medesimo;

7.3 La pubblicazione di atti all'Albo on-line, costituendo operazione di trattamento di dati personali, consistente, ai sensi dell'art. 4, lettera m) del D.Lgs. 30.06.2003, n.196, nella diffusione degli stessi dati, deve essere espletata nel rispetto delle specifiche norme previste dal citato decreto legislativo, di cui principalmente:

a) tutti i dati personali possono essere oggetto di una o più operazioni di trattamento purché finalizzate allo svolgimento di funzioni e nel rispetto dei presupposti e dei limiti previsti dal D.Lgs. 196/2003, da ogni altra disposizione di legge o di Linee guida, dai provvedimenti del Garante per la privacy, di cui principalmente la deliberazione n.17 del 19.04.2007 "Linee guida in materia di trattamento di dati per- sonali per finalità di pubblicazione e diffusione di atti e documenti di enti locali";
b) sono da rispettare i principi di necessità e di proporzionalità dei dati personali diffusi rispetto alla finalità della pubblicità - notizia che con la pubblicazione si persegue;
c) la diffusione dei dati sensibili e giudiziari è lecita se la stessa sia realmente indispensabile (art. 3, art. 4° comma 1, lettere d) ed e), art. 22, commi 3, 8 e 9 del D.Lgs. n.196/2003) e i dati pertinenti rispetto al contenuto del provvedimento e non eccedenti rispetto al fine che con esso si intende perseguire;
d) i dati sensibili possono essere oggetto di diffusione, soltanto se tale operazione di trattamento sia prevista da una norma di legge o dalle apposite Linee guida approvate dal Consiglio di questo Ente;
e) i dati idonei a rivelare lo stato di salute non possono mai essere diffusi (ex art. 22, comma 8 D.Lgs. n.196/2003);
f) i dati giudiziari possono essere oggetto di diffusione, soltanto se siffatta operazione di trattamento sia prevista da una norma di legge o da un provvedimento del Garante della privacy (ex art. 20 D. Lgs. n.196/2003);
g) i dati personali diversi dai dati sensibili e giudiziari possono essere oggetto di diffusione se siffatta operazione di trattamento sia prevista da una norma di legge o di Linee guida.

7.4 - Al contenuto integrale degli atti sarà comunque consentito l'accesso da parte dei soggetti titolari di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso come previsto dall'art.22 della legge n.241/1990 e dall'art.2 del D.P.R. n.184/2006;

7.5 - All'Albo on-line è sempre affisso un apposito avviso con cui si fornisce informazione dei diritti del soggetto interessato di cui rispettivamente agli articoli 13 e 7 del D,Lgs. 196/2003 nonché il riferimento alle modalità dell'esercizio degli stessi diritti a norma degli articoli 8, 9 e 10 del D.Lgs. 196/2003;

7.6 - Il rispetto dei principi e delle disposizioni in materia di riservatezza dei dati personali, anche in relazione alla pubblicazione obbligatoria all'Albo online, è assicurato con idonee misure o accorgimenti tecnici da attuare in sede di redazione dell'atto stesso da parte del soggetto competente, come indicato nel prece- dente articolo 5;

7.7 - Del contenuto degli atti pubblicati, in relazione al rispetto delle norme per la protezione dei dati personali, anche con riguardo alla loro diffusione per mezzo della pubblicazione dei rispettivi atti all'Albo on-line, è responsabile il soggetto, l'ufficio o l'organo che propone e/o adotta l'atto da pubblicare e/o il soggetto (esterno o interno) che richiede la pubblicazione.

8 - Disposizioni finali

Le presenti linee guida entrano in vigore dalla data di esecutività della deliberazione di approvazione delle stesse, sono pubblicate nella pagina iniziale dell'albo on-line e allegate al Manuale di Gestione.

Allegato delibera C.C./G.M
n. 18 del 25/2/2016

COMUNE DI ROSATE

ALLEGATO 10

MODELLI PER RIPRODUZIONE CARTACEA DI DOCUMENTI INFORMATICI

Nel caso della produzione di copie cartacee conformi di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 20, 21, e 23 del Dlgs.82/2005.

La presente copia, composta di n._____ pagine è conforme all'originale depositata agli atti del Comune di Rosate.

Il sottoscritto _____

Responsabile del Settore _____ Data _____

Firma _____

Nel caso della produzione di copie cartacee semplici di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 20, 21, e 23 del Dlgs.82/2005.

F.to <dati_firma>
Firma autografa sostituita dall'indicazione del nome ai sensi dell'art. 3, c. 2, del Dlgs n.39/1993.

Allegato delibera ~~G.C.~~/G.M.
n. 18 del 25/2/2016 ALLEGATO 11

ELENCO TRASMISSIONI TELEMATICHE

descrizione	formato	riferimento normativo
AciPRA	Gestione pratiche automobilistiche	Servizi Polizia Locale
Acquisti in rete PA	Acquisizione beni/servizi	Tutti i Settori
Agenzia delle Entrate - SISTER	Dati catastali	Settore Tributario/Settore Tecnico
	Portale dei Comuni	Settore Finanziario/Settore Tributario/Settore Tecnico
	Visure - estratti	Settore Tributario/Settore Tecnico
ANCITEL/SGATE (Sistema gestione agevolazioni tariffe energetiche)	Richieste ammissione bonus luce e bonus gas	Settore Sociale
	Banca dati assicurazione	Settore Polizia Locale
	Banca dati veicoli rubati	
	Proprietà veicoli	
ARAN	Trasmissione contratto decentrato	Settore Personale
	Trasmissione deleghe sindacali	
AVCP - Autorità di vigilanza sui contratti pubblici di lavori, servizi e forniture	Richiesta cod.CIG (SIMOG e semplificato) - certificati esecuzione lavori - riscossione contributi - AVCPass - contributo AVCP -	Tutti i Settori
Camera di Commercio	Interrogazioni per visure camerali	Settore Tecnico
Casellario Giudiziale	Comunicazione decessi	Settore Demografico
CIPE	CUP	Settore Tecnico
CNSD - INA SAIA	Nascite - Decessi - Variazione stato civile - Variazione residenza motorizzazione - Codice Fiscale	Settore Demografico
Corte dei Conti	Conto Consuntivo	Settore Finanziario
ENTRATEL	F24EP - 770s -770o -ricezione mod. 730/4 - contratti - anagrafe tributaria	Settore Finanziario/Settore Tributario/Settore Tecnico
Equitalia / esatri / risconet	Provvedimenti scarico e ruoli	Settori Tributario/Polizia Locale
GUCE/SIMAP	Pubblicazione atti, avvisi e concorsi	Settore tecnico
IFEL	Dati contributo 0.8 per mille ICI	Settore Tributario
INAIL	Denucia annuale/Denuncia infortuni/Comunicazioni obbligatorie	Settore Finanziario/Settore Personale
Infocamere	Verifica autocertificazioni	Settori Ammistrativo/Tecnico
INPS	Mutui, piccoli prestiti, cessione stipendi, cartolarizzazione crediti, variazioni anagrafiche, durc on line	Settori Finanziario/Demografico
ISTAT	Rilevazione permessi a costruire, DIA, SCIA, rilevazioni settore sociale, statistiche demografiche, rilevazione cancellati dall'anagrafe per decesso	Settori Tecnico/Demografico/Sociale
Ministero Economie e Finanze	Dichiarazioni aliquote IMU/Addizionali e regolamenti/ rilevazioni partecipate e concessioni	Settori Tributario/Amministrativo

ELENCO TRASMISSIONI TELEMATICHE

descrizione	formato	riferimento normativo
Ministero dell'Interno	ANAGAIRE - statistiche elettorali/SICEANT	Settori: Amministrativo/Demografico/Tecnico/ Polizia Locale
Motorizzazione Civile	Dati veicoli, patenti, proprietari	Settore Polizia Locale
PerlaPA	GEDAP/CONSOC/GEPAS/Legge 104-92/Monitoraggi lavoro/Anagrafe delle prestazioni/Assenze del personale	Settore Personale
Prefettura di Milano	dati e statistiche/incidenti	Settori Demografico/Polizia Locale
Questura di Milano	Cessione Fabbricati	Settore Polizia Locale
Ragioneria dello Stato	Monitoraggio trimestrale del personale/conto del personale e relazione allegata/Rilevazione spesa sociale dei comuni/patto di stabilità	Settori Amministrativo/Finanziario/Sociale
Regione Lombardia	Comunicazioni osservatorio regionale/bandi di gara ed esiti/graduatorie ERP ed assegnazioni/rendicondo f.do sostegno affitti/Contributi diversi/Protezione Civile/Dote Scuola/Accesso ai finanziamenti/VAS/PGT/MAPEL/MUTA/Gestione impianti sportivi/Gestione anagrafica scolastica/Rendicontazione finanziamenti regionali	Tutti i Settori
Regione Lombardia - BURL	Pubblicazione atti, avvisi e concorsi	Settore Tecnico
SIATEL	Accertamenti anagrafici vari/Codici Fiscali	Settore Tributario/Demografico
SINTEL - ARCA Regione Lombardia	Acquisizione beni/servizi	Tutti i Settori
SINTESI	Comunicazioni obbligatorie	Settore Personale
SISTER	Visure / Portale Comuni - servizi catastali / Conservatoria	Settori Tributario/Tecnico
SIVES	Gestione veicoli sequestrati	Settore Polizia Locale
Tesoreria Comunale	Flussi stipendi/ Flussi mandati e reversali/ modelli pagamento	Settore Finanziario

COMUNE DI ROSATE

Allegato delibera ~~C.C.~~/G.M
n. 18 del 25/2/2016

ALLEGATO 12

LINEE GUIDA PER LA GESTIONE DELL'ARCHIVIO DI DEPOSITO E STORICO

1. Movimentazione fascicoli dall'archivio

I fascicoli cartacei dell'archivio corrente sono conservati presso i settori. In seguito, gli uffici redigeranno apposito piano di versamento (di norma una volta all'anno), costituito dall'elenco dei fascicoli relativi ad affari e a procedimenti conclusi, a seguito del quale consegneranno al Responsabile del protocollo/archivio i fascicoli da depositare nell'archivio di deposito.
Periodicamente e secondo un apposito piano di versamento (di norma una volta all'anno), il Responsabile del procedimento deve consegnare all'archivio i fascicoli relativi ad affari e a procedimenti amministrativi non più necessari ad una trattazione corrente corredati dal relativo elenco di versamento.
Le serie Archivistiche e i relativi registri o repertori sono conservati per cinque anni presso la struttura che cura i rispettivi procedimenti; trascorso tale termine vengono versati all'Archivio di deposito della sede centrale.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli avevano nell'archivio corrente.

Prima di effettuare il conferimento di cui sopra, il Responsabile del procedimento verifica:

a) l'effettiva conclusione ordinaria della pratica;
b) l'effettiva trascrizione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
c) il corretto aggiornamento della data di chiusura sulla camicia del fascicolo;
d) lo scarto di eventuali copie e fotocopie di documentazione passibile di scarto al fine di garantire la presenza di tutti e soli documenti pertinenti alla pratica;

Dell'avvenuto conferimento dei documenti viene predisposto un elenco di versamento con le modalità previste dal testo unico, copia del quale viene conservata dall'utente che ha versato la documentazione.
Il materiale viene archiviato con lo stesso ordine di classificazione dell'archivio corrente e per ordine cronologico.

2. Procedura di scarto ed archivio storico

Ogni anno, in base al massimario di scarto, viene effettuata la procedura di selezione della documentazione da proporre allo scarto e attivato il procedimento amministrativo di scarto documentale con l'invio della proposta alla competente Soprintendenza archivistica. Per effettuare lo scarto dei documenti, infatti, occorre sempre l'autorizzazione del ministero dei beni e le Attività culturali, ai sensi dell'art.21 comma 1, lettera d) del Codice dei Beni culturali e del paesaggio (D.Lvs n.52 del 22/01/2004) I fascicoli non soggetti a operazioni di scarto sono trasferiti nell'archivio storico per la conservazione permanente.

ELENCO DOCUMENTI ALLEGATI

Allegato n.1	Normativa di riferimento in ambito di gestione documentale
Allegato n.2	Glossario - Definizioni
Allegato n.3	Area Organizzativa Omogenea - Elenco dei settori dell'ente – elenco abilitazioni alla protocollazione
Allegato n.4	Elenco documenti soggetti a registrazione particolare
Allegato n.5	Titolario di classificazione
Allegato n.6	Condizioni generali di contratto – firma digitale
Allegato n.7	Certificazione di accreditamento
Allegato n.8	Registro Protocollo di Emergenza
Allegato n. 8.1	Autorizzazione all'utilizzo del protocollo di emergenza
Allegato n.9	Linee guida Albo Pretorio
Allegato n.10	Modelli per riproduzione cartacea di documenti informatici
Allegato n. 11	Elenco trasmissioni telematiche
Allegato n. 12	Linee guida gestione dell'archivio

COMUNE DI ROSATE (MI)
UFFICIO SERVIZI AMMINISTRATIVI

DELIBERAZIONE G.C. N° 18 DEL 25/2/2016

OGGETTO: APPROVAZIONE DEFINITIVA MANUALE PER LA GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

PARERE DI REGOLARITA' TECNICA

Visto con parere favorevole

Li 25/2/2016

IL RESPONSABILE DEL SETTORE
f.to Dr.ssa A. Simonetta Panara

PARERE DI REGOLARITA' CONTABILE

Visto con parere favorevole

Li_____

IL RESPONSABILE DI RAGIONERIA
Dr.ssa Giulia Mangiagalli

Si esprime parere favorevole alla citata.....di Bilancio

L'UFFICIO DEL REVISORE DEL CONTO

Li_____

IL REVISORE DEL CONTO

DGC NR 18 DEL 25/02/2016

Il presente verbale è stato letto, approvato e sottoscritto.

IL SINDACO
F.to Daniele Del Ben

IL SEGRETARIO COMUNALE
F.to Dott.ssa Maria Baselice

PUBBLICAZIONE / COMUNICAZIONE

La presente deliberazione viene pubblicata nelle forme di Legge all'Albo Pretorio del Comune per 15 giorni consecutivi e cioè dal 11/3/2016 al 26/3/2016

Rosate, 11/3/2016

IL SEGRETARIO COMUNALE
F.to Dott.ssa Maria Baselice

COPIA CONFORME

Copia conforme all'originale, per uso amministrativo.

Rosate, 11/3/2016

COMUNE DI ROSATE - Prov. di Milano

IL SEGRETARIO COMUNALE
Dott.ssa Maria Baselice

ESECUTIVITA'

Si certifica che la presente deliberazione è divenuta esecutiva dopo il decimo giorno dalla sua pubblicazione, insussistenti iniziativa, denunce di vizi di illegittimità o di incompetenza, di cui all'articolo 134 comma 3° del testo unico D.Lgs. n. 267/2000.

Rosate,

IL SEGRETARIO COMUNALE
Dott.ssa Maria Baselice