

Allegato 5

ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

Nominativo	Titolo/Ruolo nell'AOO	Estremi e descrizione della delega ricevuta
PARODI Cav. Antonio	Sindaco pro tempore	Sino a scadenza mandato elettorale
SALVATICO dr. Fabrizio	Segretario Comunale	Sino a scadenza mandato elettorale del Sindaco – Decreti Sindacali n. 6 del 6 giugno 2011 – n. 1 del 31 gennaio 2012 – n. 3 del 1° febbraio 2012 – n. 5 del 1° febbraio 2012
ABBA' Elisa	Istruttore amministrativo UFFICIO TECNICO	Responsabile del Procedimento con da atto di organizzazione Area Tecnica Urbanistica ed Edilizia Privata datata 1° ottobre 2015
ALASIA Giorgio	RESPONSABILE DEL SERVIZIO LL.PP	Decreto Sindacale n. 11 del 6 giugno 2011 Attribuzione responsabilità Servizio di UTC-LLPP sino a scadenza mandato del Sindaco
ALTINA Caterina	RESPONSABILE DEL SERVIZIO FINANZIARIO	Decreto Sindacale n. 7 del 6 giugno 2011 Attribuzione responsabilità Servizio Finanziario sino a scadenza mandato del Sindaco
BERNARDI Mara	RESPONSABILE DEL SERVIZIO SEGRETERIA/COMMERCIO/CULTURA	Decreto Sindacale n. 9 del 6 giugno 2011 Attribuzione responsabilità Servizio Segreteria/Commercio/Cultura sino a scadenza mandato del Sindaco
BONINO Mauro	RESPONSABILE DEL SERVIZIO URBANISTICA – EDILIZIA PRIVATA	Decreto Sindacale n. 12 del 6 giugno 2011 Attribuzione responsabilità Servizio Urbanistica/Edilizia Privata sino a scadenza mandato del Sindaco
BONO Giuliana	Istruttore amministrativo DEMOGRAFICI	Ufficiale di Anagrafe e Stato Civile Responsabile del Procedimento come atto di organizzazione dell'Area Servizi Demografici, Scolastici ed Assistenza datato 7 aprile 2009
CHIAVAZZA Antonio	RESPONSABILE DEL SERVIZIO DI POLIZIA MUNICIPALE	Decreto Sindacale n. 13 del 6 giugno 2011 Attribuzione responsabilità Servizio DI Polizia Municipale sino a scadenza mandato del Sindaco
GARELLO Fulvio	Vigile Urbano	Responsabile del Procedimento come da atto di organizzazione dell'Area di Vigilanza e Custodia datato 7 aprile 2009
LERDA Ornella	RESPONSABILE DEI SERVIZI DEMOGRAFICI E DI ASSISTENZA	Decreto Sindacale n. 10 del 6 giugno 2011 Attribuzione responsabilità Servizi Demografici/Assistenza sino a scadenza mandato del Sindaco
MIGLIETTA Rosaria	Istruttore amministrativo ANAGRAFE	Ufficiale di Anagrafe e Stato Civile
TESIO Graziella	RESPONSABILE SERVIZI TRIBUTI/ECONOMATO	Decreto Sindacale n. 8 del 6 giugno 2011 Attribuzione responsabilità Servizi Tributi/Economato sino a scadenza mandato del Sindaco

Allegato 6

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI**ASPETTI FONDAMENTALI DELLA SICUREZZA**

Gli aspetti fondamentali del sistema di sicurezza sono:

- protezione fisica delle risorse
- protezione logica delle informazioni
- norme per il personale.

PROTEZIONE FISICA DELLE RISORSE

L'obiettivo della protezione fisica delle risorse è quello di proteggere le aree e le componenti del sistema informativo.

Generalmente le contromisure di sicurezza fisica possono essere ricondotte a sicurezza di area e sicurezza delle apparecchiature.

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi informatici. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle sale computer rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

La sicurezza delle apparecchiature e' riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in quest'area, come anche la protezione da manomissione o furti.

Le contromisure adottate sono le seguenti:

- I locali dove trovano alloggio i server sono chiusi, dotati di impianto di condizionamento e di sensori per l'antifurto.
- Le chiavi di accesso ai locali sono distribuite ai soli dipendenti degli Uffici Comunali ed agli Amministratori autorizzati.
- Le apparecchiature sono altresì protette da sbalzi di tensione elettrica tramite UPS.

PROTEZIONE LOGICA DELLE INFORMAZIONI

Gli obiettivi della protezione logica delle informazioni sono:

- il controllo degli accessi alle informazioni;
- il mantenimento della loro integrità e riservatezza;
- la sicurezza nella trasmissione e nelle comunicazioni all'interno dell'Amministrazione e con l'esterno (Internet, altre Amministrazioni etc.);
- la sicurezza delle stazioni di lavoro e dei personal computer;
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.

Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere.

Le contromisure adottate sono le seguenti:

- Sistema operativo del PdP utilizzato dall'Amministrazione, conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza);

- uso di sistemi RAID (si tratta di hard disk multipli visti però dal sistema operativo come un singolo disco). La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi;
- protezione dei sistemi di accesso e conservazione delle informazioni con assegnazione ad ogni utente del sistema di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno *bimestrale* durante la fase di esercizio;
- sistemi di backup giornalieri;
- conservazione, a cura di Ditta esterna incaricata, delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP oltre alle copie delocalizzate fuori della sede comunale;
- firewall perimetrale che protegge la LAN da intrusioni esterne e web/mail server collocato in DMZ per non compromettere la sicurezza della LAN;
- server accessibili dall'esterno solo tramite vpn o tramite attivazione all'interno della LAN di software per il controllo remoto;
- software anti-virus, con gestione diffusa, su ogni PC e server;
- manutenzione dei gestionali in uso e gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo costituito dal personale in dotazione all'ufficio Sistemi Informatici e da risorse esterne qualificate;
- Piano di Continuità Operativa necessario a garantire la continuità del servizio informatico e la disponibilità delle informazioni (aggiornate), evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. Il sistema informativo deve essere ripristinato entro sette giorni.

NORME PER IL PERSONALE

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO

<p>Premessa</p>	<p>E' necessario stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale.</p> <p>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, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc.</p> <p>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.</p> <p>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.</p>
<p>Scopo</p>	<p>Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.</p> <p>Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.</p> <p>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.</p>
<p>Ambito di applicazione</p>	<p>Queste politiche si applicano a tutti gli impiegati dell'Amministrazione e al personale esterno (interinali, stagisti, consulenti, ...) e a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.</p>

Politiche – Uso generale e proprietà

- 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.
- 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.

Politiche - Sicurezza e proprietà dell'informazione

- 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 quattro 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.
- Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
- 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 permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali, in quanto risultate voi autori di qualunque azione.

POLITICHE - ANTIVIRUS

Premessa	<p>I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.</p> <p>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.</p> <p>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.</p>
Scopo	<p>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.</p>
Ambito di applicazione	<p>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.</p>

Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile dal sito del suo produttore.
- 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.
- Evitare 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 copiati 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.
- I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).
- Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico ... [omissis]... che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".
- 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 RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

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, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

POLITICHE - USO NON ACCETTABILE DEL SISTEMA INFORMATIVO

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

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.

Attività di rete e di sistema

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 pedo-pornografico 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.
- Realizzare brecche nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecche della sicurezza si intendono, in modo riduttivo:
 - a) accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione;
 - b) attività di "sniffing";
 - c) disturbo della trasmissione;
 - d) spoofing dei pacchetti;
 - e) negazione del servizio;
 - f) le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
 - g) attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
- 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 Internet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

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 o collezionare copie.
- Uso di messaggi non sollecitati originati dall'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).

POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

Premessa	Lo scopo di queste politiche è prevenire rivelazioni non autorizzate o involontarie di informazioni confidenziali o sensitive dell'Amministrazione
Scopo	Lo scopo di queste politiche è prevenire rivelazioni non autorizzate o involontarie di informazioni confidenziali o sensitive dell'Amministrazione.
Ambito di applicazione	Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

Politiche

Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione.

Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

Scopo	Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.
Ambito di applicazione	Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

Politiche

Il personale dell'Amministrazione e le persone terze autorizzate possono utilizzare la linea commutata per guadagnare l'ingresso all'Intranet dell'Amministrazione. Tale accesso deve avvenire o tramite l'uso di VPN o tramite l'uso di sistemi di autenticazione forte quali per esempio password da usare una sola volta (one time password). È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente all'Intranet dell'Amministrazione ed alle sue informazioni.

Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" un'estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.

Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

Scopo	Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.
Ambito di applicazione	La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa..

Politiche – Usi proibiti

Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

Politiche – Uso personale

Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

ASPETTI DI SICUREZZA INFORMATICA

PER LA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

FORMAZIONE DEI DOCUMENTI

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

Si adottano preferibilmente i formati PDF, XML e TIFF. I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno dell'AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 (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 artt. 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al Decreto Legislativo n. 82/2005.).

I documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'Amministrazione.

GESTIONE DEI DOCUMENTI

Il sistema di protocollo informatico assicura:

- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

Il sistema di protocollo informatico consente:

- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (firewall);
- dalle registrazioni del PdP.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RGD e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre Pubbliche Amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Lo scambio per via telematica di messaggi protocollati tra AOO di Amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal Decreto Legislativo del 30 giugno 2003, n. 196.

Scambio dei documenti all'esterno dell'Amministrazione (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.).

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica certificata ai sensi del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. Tali informazioni sono incluse nella segnatura informatica di ciascun messaggio protocollato e sono codificate in formato XML.

Con provvedimento dell'Agenzia per l'Italia Digitale, vengono indicati le modalità di trasmissione dei documenti informatici, il tipo ed il formato delle informazioni archivistiche di protocollo minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai messaggi protocollati.

Scambio dei documenti all'interno dell'amministrazione

Gli Uffici dell'Amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'Innovazione e le Tecnologie concernente l'"impiego della posta elettronica nelle Pubbliche Amministrazioni".

ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Il PdP adottato dall'Amministrazione:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;
- assicura il tracciamento di qualsiasi evento di modifica dell'informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Accesso al registro di protocollo per utenti interni all'Amministrazione

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Un utente può avere la visibilità completa sul registro di protocollo solo a seguito di abilitazione.

Il personale dell'ufficio protocollo generale è abilitato alla visualizzazione completa sul registro protocollo. I Servizi Demografici sono abilitati solo il giorno settimanale del sabato e nel corso di consultazioni elettorali alla visualizzazione completa sul registro protocollo.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'Amministrazione. Nel caso in cui sia effettuata la registrazione di un documento riservato, la visibilità completa sul documento stesso è possibile solo alla persona destinataria del documento.

Di norma tutti gli utenti che devono protocollare sono abilitati alla consultazione, inserimento e modifica, ma è possibile abilitare un utente anche alla sola consultazione.

Solo il personale dell'ufficio protocollo - assistito dalla Ditta fornitrice del programma - è invece abilitato all'annullamento.

CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Per la conservazione dei documenti informatici si applicano le regole di cui al Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'Amministrazione Digitale di cui al Decreto Legislativo n. 82/2005.).

Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti o affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

L'Amministrazione ha optato per la seconda soluzione ed ha richiesto alla Soprintendenza Archivistica territorialmente competente, il nulla-osta preventivo alla sottoscrizione di un Accordo di collaborazione con il Servizio Polo Archivistico Regionale dell'Emilia-Romagna ai fini della conservazione dei documenti informatici su piattaforma digitale.

Per le modalità operative di trasmissione del contenuto del pacchetto di versamento al sistema di conservazione si rimanda al manuale di conservazione.

Il manuale di conservazione inoltre illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Allegato 7

ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del Decreto del Presidente della Repubblica 20 dicembre 2000, n. 445 e s.m.i.:

- Gazzette ufficiali
- Bollettini ufficiali e notiziari della Pubblica Amministrazione
- Note di ricezione delle circolari e altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Giornali e riviste
- Libri
- Materiali pubblicitari
- Inviti a manifestazioni
- Tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

Sono altresì esclusi dalla protocollazione, in ambito comunale, le seguenti tipologie documentarie:

- Offerte o preventivi di terzi non richiesti
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Richieste ferie
- Richieste permessi
- Richieste di rimborso spese e missioni
- Ricevute di ritorno delle raccomandate A.R.
- Pubblicità conoscitiva di convegni /corsi di aggiornamento
- Convocazioni ad incontri o riunioni e corsi di formazione interni
- Certificati e affini
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura.

I documenti che sono invece soggetti a particolare registrazione dell'Amministrazione e che, ai sensi dell'art. 53, com. 5 del D.P.R. n. 445/2000 e s.m.i., sono esclusi dalla protocollazione sono:

Area	Registrazione particolare	Modalità di trattamento
	Atti di organizzazione – Deliberazioni/Verbali della Giunta Comunale e del Consiglio Comunale – Determinazioni del Responsabile	Uso dell'applicativo Delibere – Determinazioni evol-x (Dedagroup)
	Contratti rogati dal Segretario Comunale	Uso dell'applicativo UNIMOND CLIENT Agenzia delle Entrate e dell'Applicativo Protocollo (GISMASTER)
	Contratti non rogati in forma pubblica dal Segretario Comunale	

Area	Registrazione particolare	Modalità di trattamento
	Decreti sindacali (repertorio atti)	
	Ordinanze dirigenziali (repertorio atti)	
	Ordinanze sindacali (repertorio atti)	
FINANZIARIA	Atti di liquidazione	Uso dell'applicativo CONTABILITA' FINANZIARIA evol-x (DEDAGROUP)
	Fatture emesse	
	Mandati di pagamento	Uso dell'applicativo CONTABILITA' FINANZIARIA evol-x (DEDAGROUP)
	Registri IVA	
	Reversali di incasso	Uso dell'applicativo CONTABILITA' FINANZIARIA evol-x (DEDAGROUP)
	Patrimonio ed Inventario	Uso dell'applicativo PATRIMONIO ED INVENTARIO evol-x (DEDAGROUP)
Demografici	Atti di stato civile (registrazione informatica)	Uso dell'applicativo Stato Civile evol-x (DEDAGROUP)
	Carte d'identità (registrazione informatica)	Uso dell'applicativo Anagrafe Demografici evol-x (DEDAGROUP)
	Certificati anagrafici	Uso dell'applicativo Anagrafe Demografici evol-x (DEDAGROUP)
	Pubblicazioni di matrimonio (registrazione informatica)	Uso dell'applicativo Stato Civile evol-x (DEDAGROUP)
	Tessere elettorali (registrazione informatica)	Uso dell'applicativo Anagrafe Demografici evol-x (DEDAGROUP)
Polizia Locale	Concessione contrassegno parcheggi invalidi	
	Documenti informatici ricevuti o inviati nell'ambito di sistemi dedicati allo scambio o alla consultazione di dati (ACI-PRA/MOTORIZZAZIONE)	Uso del Portale Motorizzazione Sistema ANCI/PRA
	Notizie di reato	
	Rapporti incidenti	
	Verbali CdS (registrazione informatica)	Uso dell'applicativo PM (SAPIDATA)
	Verbali oggetti smarriti	
	Verbali violazioni amministrative	
	Registro veicoli rimossi	
	Albo pretorio	Uso dell'applicativo Albo Web (DEDAGROUP)
	Notifiche	



COMUNE DI CAVALLERMAGGIORE
(Provincia di Cuneo)

MANUALE DI
GESTIONE E CONSERVAZIONE
DEI DOCUMENTI

ALLEGATO 8

PIANO CONSERVAZIONE
PRONTUARIO



CATEGORIA I – AMMINISTRAZIONE

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

CLASSE 1
COMUNE - ATTIVITA' ISTITUZIONALE
UFFICI COMUNALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>DENOMINAZIONE, TERRITORIO E CONFINI, CIRCOSCRIZIONI DI DECENTRAMENTO</u> a) Denominazione Comune b) Attribuzione del titolo di Città c) Confini del Comune	Permanente Permanente Permanente	
2) <u>STATUTO</u> : Redazione, modifiche e interpretazioni dello Statuto	Permanente, dopo lo sfolgimento del materiale informativo relativo ad altri Comuni	
3) <u>REGOLAMENTI</u> a) Regolamenti emessi dal Comune: repertorio annuale b) Redazione di Regolamenti: un fascicolo per ciascun affare	Permanente Permanente, previo sfolgimento dei documenti di carattere transitorio	Tenere un solo esemplare, scartare gli altri
4) <u>STEMMA, GONFALONE, SIGILLO</u> a) Definizione, modifica, riconoscimento dello stemma b) Definizione, modifica, riconoscimento del gonfalone c) Definizione, modifica, riconoscimento del sigillo d) Concessione del patrocinio gratuito e del connesso uso dello stemma del Comune: fascicolo annuale per attività	Permanente Permanente Permanente Permanente	Perché documenta attività che si svolgono nel territorio
5) <u>ATTIVITA' NORMATIVA - LEGISLAZIONE E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su leggi specifiche b) Circolari pervenute: repertorio annuale c) Circolari emanate dal Comune: repertorio annuale	Permanente Permanente Permanente	
6) <u>ESPOSIZIONE BANDIERA</u>	1 anno	
7) <u>ATTIVITA' E ORDINAMENTO DEGLI UFFICI E DEI SERVIZI</u> a) Attribuzione di competenze agli uffici b) Organigramma: un fasc. per ciascuna definizione dell'organigramma c) Organizzazione degli uffici: un fasc. per ciascun affare d) Orari di apertura degli uffici comunali e altre attività esistenti sul territorio e) Materiale preparatorio per i provvedimenti in materia di politica del personale	Permanente Permanente Permanente Permanente 10 nni	
8) <u>ATTIVITA' ISTITUZIONALE</u> a) Richieste di pubblicazione all'Albo Pretorio b) Registro all'Albo Pretorio c) Richieste di notifica presso la casa comunale (con allegati) d) Registro delle notifiche	1 anno 20 anni 2 anni 20 anni	

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
5) <u>CONCORSI, SELEZIONI, COLLOQUI</u> a) Criteri generali e normativa per il reclutamento del personale: un fasc. con eventuali sottofascicoli b) Procedimenti per il reclutamento del personale: un fasc. per ciascun procedimento (fasc. per affare), con i seguenti sottofascicoli: - Bando e manifesto - Domande - Allegati alle domande (ove previsti dal bando) - Verbali - Prove d'esame - Copie bando restituite al Comune c) Curricula inviati per richieste di assunzione d) Domande di assunzione pervenute senza indizione di concorso o selezione	Permanente Permanente 1 anno dopo la scadenza dei termini per i ricorsi Da restituire dopo la scadenza dei termini dei ricorsi agli interessati Permanente 1 anno dopo la scadenza dei termini per i ricorsi 1 anno dopo la scadenza dei termini per i ricorsi 2 anni 1 anno	
6) <u>ASSUNZIONI E CESSAZIONI</u> a) Criteri generali e normativa per le assunzioni e cessazioni b) Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente Permanente	
7) <u>COMANDI E DISTACCHI, MOBILITA'</u> a) Criteri generali e normativa per comandi, distacchi, mobilità b) Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente Permanente	
8) <u>ATTRIBUZIONI DI FUNZIONI, ORDINI DI SERVIZIO E MISSIONI</u> a) Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni b) Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali c) Determinazioni di missioni inserite nei singoli fascicoli personali d) Determinazioni di ordini di servizio inserite nei singoli fascicoli personali e) Ordini di servizio collettivi f) Autorizzazione allo svolgimento di incarichi esterni	Permanente Permanente 10 anni Permanente Permanente 2 anni	
9) <u>INQUADRAMENTI E APPLICAZIONE CONTRATTI COLLETTIVI DI LAVORO</u> a) Criteri generali e normativa per gli inquadramenti e le applicazioni dei contratti collettivi di lavoro b) Determinazione dei ruoli e contratti collettivi c) Determinazioni relative ai singoli	Permanente Permanente Permanente	NB: i contratti con il singolo confluiscono nel fasc. personale
10) <u>RETRIBUZIONI E COMPENSI</u> a) Criteri generali e normativa per le retribuzioni e compensi b) Anagrafe delle prestazioni: schede c) Determinazioni inserite nei singoli fascicoli personali d) Ruoli degli stipendi: base di dati/tabulati e) Provvedimenti giudiziari di requisizione dello stipendio	Permanente 5 anni 5 anni dalla cessazione dal servizio Permanente 5 anni	

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
11) <u>TRATTAMENTO FISCALE, CONTRIBUTIVO, ASSICURATIVO</u> a) Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi b) Trattamento assicurativo inserito nei singoli fascicoli personali c) Trattamento contributivo inserito nei singoli fascicoli personali d) Trattamento fiscale inserito nei singoli fascicoli personali e) Assicurazione obbligatoria	Permanente 5 anni dalla chiusura del fascicolo 5 anni dalla chiusura del fascicolo 5 anni dalla chiusura del fascicolo 5 anni dalla chiusura del fascicolo	
12) <u>TUTELA DELLA SALUTE E SICUREZZA SUL LUOGO DI LAVORO</u> a) Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro b) Rilevazione dei rischi, ai sensi della L. 626/94: un fasc. per sede c) Prevenzione infortuni d) Registro infortuni e) Verbali delle rappresentanze dei lavoratori per la sicurezza f) Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali g) Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro)	Permanente Tenere l'ultima e scartare le precedenti Permanente Permanente Permanente Permanente 10 anni	Per Legge 626/94
13) <u>DICHIARAZIONE DI INFERMITA' ED EQUO INDENNIZZO</u> a) Criteri generali e normativa per le dichiarazioni di infermità b) Dichiarazioni di infermità e calcolo dell'indennizzo inserite nel singolo fascicolo personale	Permanente Permanente	
14) <u>INDENNITA' PREMIO DI SERVIZIO E TRATTAMENTO DI FINE RAPPORTO QUIESCENZA</u> a) Criteri generali e normativa per il trattamento di fine rapporto b) Trattamento pensionistico e di fine rapporto inserito nel singolo fascicolo personale	Permanente Permanente	
15) <u>SERVIZI AL PERSONALE SU RICHIESTA</u> a) Criteri generali e normativa per i servizi su richiesta b) Domande di servizi su richiesta (mensa, asili nido, colonie estive, soggiorni climatici, etc)	Permanente 2 anni	

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
<p>16) <u>ORARIO DI LAVORO, PRESENZE E ASSENZE</u></p> <p>a) Criteri generali e normativa per le assenze</p> <p>b) Domande e dichiarazioni dei dipendenti sull'orario inserite nel singolo fascicolo personale:</p> <ul style="list-style-type: none"> - 150 ore - permessi d'uscita per motivi personali - permessi per allattamento - permessi per donazione sangue - permessi per motivi sindacali - opzione per orario particolare e part-time <p>c) Domande e dichiarazioni dei dipendenti sulle assenze (con allegati) inserite nel singolo fascicolo personale:</p> <ul style="list-style-type: none"> - congedo ordinario - congedo straordinario per motivi di salute - congedo straordinario per motivi personali e familiari - aspettativa per infermità - aspettativa per mandato parlamentare o altre cariche elettive - aspettativa obbligatoria per maternità e puerperio - aspettativa facoltativa per maternità e puerperio - aspettativa per motivi di famiglia - aspettativa sindacale - certificati medici <p>d) Referti delle visite di controllo inseriti nel singolo fascicolo personale</p> <p>e) Fogli firma; cartellini presenze, tabulati elettronici di rilevazione presenze</p> <p>f) Rilevazioni delle assenze per sciopero:</p> <ul style="list-style-type: none"> - singole schede - prospetti riassuntivi 	<p>Permanente</p> <p>2 anni</p> <p>2 anni</p> <p>2 anni</p> <p>2 anni</p> <p>2 anni</p> <p>Permanente</p> <p>2 anni</p> <p>2 anni</p> <p>Alla cessazione del servizio</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Permanente</p> <p>Alla cessazione del servizio</p> <p>Alla cessazione del servizio</p> <p>2 anni</p> <p>1 anno dopo la redazione dei prospetti riassuntivi</p> <p>Permanente</p>	<p>In assenza di pendenze disciplinari o giudiziarie</p>
<p>17) <u>GIUDIZI, RESPONSABILITA' E PROVVEDIMENTI DISCIPLINARI</u></p> <p>a) Criteri generali e normativa per i provvedimenti disciplinari</p> <p>b) Provvedimenti disciplinari inseriti nel singolo fascicolo personale</p>	<p>Permanente</p> <p>Permanente</p>	
<p>18) <u>FORMAZIONE E AGGIORNAMENTO PROFESSIONALE</u></p> <p>a) Criteri generali e normativa per la formazione e l'aggiornamento professionale</p> <p>b) Organizzazione di corsi di formazione e aggiornamento: un fasc. per ciascun corso</p> <p>c) Domande/Invio dei dipendenti a corsi inseriti nel singolo fascicolo personale</p>	<p>Permanente</p> <p>Permanente previo sfoltimento dopo 5 anni</p> <p>Permanente previo sfoltimento dopo 5 anni</p>	
<p>19) <u>COLLABORATORI ESTERNI</u></p> <p>a) Criteri generali e normativa per il trattamento dei collaboratori esterni</p> <p>b) Elenco degli incarichi conferiti: repertorio</p>	<p>Permanente</p> <p>Permanente</p>	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 9
AFFARI LEGALI E CONSULENZE VARIE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>CONTENZIOSO</u> a) Fascicoli di causa	Permanente	Concentrare quelli c/o gli studi professionali esterni
2) <u>PARERI E CONSULENZE</u>	Permanente	
3) <u>RICORSI</u> a) Fascicoli di causa	Permanente	
4) <u>ESPOSTI</u> (vedi anche in RELAZIONI ESTERNE)	Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 10
ISTITUZIONI - ENTI DIVERSI - COMMISSIONI COMUNALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>COMMISSIONI COMUNALI</u> a) Verbali della Commissione b) Fascicolo costituzione che dura quanto il mandato del Sindaco pro-tempore e/o alle disposizioni vigenti c) Convocazione	Permanente Permanente 1 anno	 Purchè riportata nel verbale

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 11
PALAZZO MUNICIPALE - LOCALI COMUNALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LOCALI COMUNALI</u> (inteso come locali siti nel Palazzo Comunale e/o pertinenze) a) Concessioni uso	5 anni dalla dismissione	
2) <u>VIGILANZA</u>	Permanente salvo sfoltimento	
3) <u>ANTIFURTO</u>	Permanente salvo sfoltimento	
4) <u>PULIZIA LOCALI</u>	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 12
CIRCOLARI, NORME, STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEGISLAZIONE E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su Leggi specifiche b) Circolari pervenute c) Circolari emanate dal Comune	Permanente Permanente Permanente	
2) <u>STATISTICHE CAT. I</u>	Permanente	



CATEGORIA II
ASSISTENZA E BENEFICIENZA/
SERVIZI SOCIALI

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 3
ASSISTENZA E TUTELA DELL'INFANZIA,
DELL'ADOLESCENZA E DELLA FAMIGLIA

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ATTIVITA' RICREATIVA E DI SOCIALIZZAZIONE</u> a) Funzionamento e attività delle strutture (colonie, centri ricreativi, etc): un fasc. annuale per ciascuna struttura b) Iniziative specifiche: un fasc. per ciascuna iniziativa (es. tutela minorenni, assistenza alle famiglie, iniziative varie per l'infanzia)	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 4
ASSISTENZA PER L'AVVIAMENTO AL LAVORO -
INFORMAGIOVANI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>INFORMAZIONE, CONSULENZA ED EDUCAZIONE CIVICA</u> a) Funzionamento e attività delle strutture (consultori, informagiovani, centri di iniziativa locale per l'occupazione, cantieri di lavoro, scuola, lavoro etc) un fasc. per struttura b) Iniziative di vario tipo: un fasc. per iniziativa (per disoccupati, etc)	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 5
ASSISTENZA SANITARIA GENERALE
A PORTATORI DI HANDICAP E/O INVALIDI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>TUTELA E CURATELA DI INCAPACI</u> a) Interventi per le persone sottoposte a tutela e curatela: un fasc. per intervento b) Residenze per portatori di handicap (costituzione, gestione)	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni Permanente	

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
2) <u>ASSISTENZA DIRETTA E INDIRETTA, BENEFICI ECONOMICI</u> a) Funzionamento e attività delle strutture: un fasc. annuale per ciascuna struttura b) Iniziative specifiche: un fasc. per ciascuna iniziativa (esenzione ticket sanitario per indigenza, rilascio tessere trasporto urbano ad invalidi a basso reddito, assistenza vittime delitti)	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 6 ASSISTENZA TOSSICODIPENDENTI/SCARCERATI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>PREVENZIONE, RECUPERO E REINTEGRAZIONE DEI SOGGETTI A RISCHIO</u> a) Campagne di prevenzione: un fasc. per campagna b) Interventi di recupero e reintegrazione dei soggetti a rischio: un fasc. per intervento c) Ricognizione dei rischi: un fasc. per affare	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 5 anni Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 5 anni Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 5 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 7 ASSISTENZA EXTRACOMUNITARI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ATTIVITA' DI INTEGRAZIONE E SOCIALIZZAZIONE</u> a) Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfolgimento del carteggio temporaneo e strumentale dopo 5 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 8 ISTITUTI NAZIONALI DI ASSISTENZA E PREVIDENZA

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
==	==	==

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 9
ASSOCIAZIONI DI VOLONTARIATO
 (es. Croce Rossa, SOA, Consulta Giovanile, etc)

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
a) ASSOCIAZIONISMO E PARTECIPAZIONE DI VOLONTARIATO		
b) Politica di incoraggiamento e appoggio alle associazioni	Permanente	
c) Albo dell'associazionismo: elenco delle associazioni accreditate	Permanente	
d) Fascicoli delle associazioni che chiedono l'iscrizione all'albo	Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 10
CIRCOLARI - NORME - STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) LEGISLAZIONE E CIRCOLARI ESPLICATIVE		
a) Pareri chiesti dal Comune su Leggi specifiche	Permanente	
b) Circolari pervenute	Permanente	
c) Circolari emanate dal Comune	Permanente	
2) STATISTICHE CAT. II	Permanente	



CATEGORIA III
POLIZIA URBANA/RURALE

**N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria —▶ 5 anni**

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 1 POLIZIA MUNICIPALE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>POLIZIA MUNICIPALE</u> a) Direttive e disposizioni: un fasc. annuale b) Organizzazione del servizio di pattugliamento: un fasc. annuale c) Verbali di accertamento di violazioni al Codice della Strada: repertorio annuale d) Accertamento di violazioni al Codice della Strada e conseguente erogazione di sanzioni: un fasc. per accertamento e) Verbali di rilevazione incidenti: repertorio annuale f) Statistiche delle violazioni e degli incidenti: un fasc. annuale g) Gestione veicoli rimossi: un fasc. per ciascun veicolo h) Bollettari per riscossione contravvenzioni	Permanente 3 anni Permanente solo il registro; i verbali 10 anni 10 anni Permanente solo il repertorio; i verbali 20 anni Permanente 2 anni 10 anni	In assenza di contenzioso (ai sensi dell'art. 157 del Codice Penale)
2) <u>INFORMATIVE</u> a) Informative su persone residenti nel Comune: un fasc. per ciascuna persona	5 anni	
3) <u>OGGETTI SMARRITI E RECU- PERATI</u> a) Verbali di rinvenimento: serie annuale repertoriata b) Ricevute di riconsegna ai proprietari: serie annuale repertoriata c) Vendita o devoluzione: un fasc. periodico (per attività)	2 anni 2 anni 2 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 2 CIRCOLAZIONE, SEGNALETICA, SICUREZZA STRADALE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>PREVENZIONE ED EDUCAZIONE STRADALE</u> a) Iniziative specifiche di prevenzione: un fasc. per iniziativa b) Corsi di educazione stradale nelle scuole: un fasc. per corso	5 anni 5 anni	
2) <u>VIABILITA'</u> a) Piano Urbano del Traffico: un fasc. per ciascun affare b) Piano Urbano della Mobilità: un fasc. per ciascun affare c) Autorizzazioni in deroga: serie annuale repertoriata (es. Rilascio autorizzazioni traffico limitato, passi carrai, rilascio autorizzazioni, sosta portatori di handicap) d) Appalto segnaletica	Permanente con sfoltimento Permanente con sfoltimento 2 anni dal cessato (conservare eventualmente i registri) Permanente con sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^



CATEGORIA IV
IGIENE E SANITA'

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 3
SALUTE PUBBLICA - PROVVEDIMENTI D'URGENZA -
VACCINAZIONI - EPIDEMIE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>SALUTE PUBBLICA</u> a) Emergenze sanitarie: un fasc. per ciascun evento b) Misure di igiene pubblica: un fasc. per ciascun affare (sequestro alimenti, medicinali) c) Interventi di derattizzazione, dezanarizzazione etc: un fasc. per ciascun intervento d) Trattamenti fitosanitari e di disinfestazione: un fasc. per ciascun intervento e) Copie lettere trasmissione denunce malattie infettive	Permanente Permanente 1 anno 5 anni 5 anni	
2) <u>TRATTAMENTI SANITARI</u> <u>OBBLIGATORI</u> a) TSO: un fasc. per ciascun procedimento b) ASO: un fasc. per ciascun procedimento c) Fascicoli personali dei soggetti a trattamenti: un fasc. per ciascuna persona	Permanente Permanente Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 4
IGIENE PUBBLICA

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>IGIENE PUBBLICA</u> a) Autorizzazioni sanitarie: repertorio annuale b) Fascicoli dei richiedenti autorizzazioni sanitarie: un fasc. per ciascuna persona/ditta	Permanente 5 anni dalla cessazione dell'attività	
2) <u>AMBIENTE: AUTORIZZAZIONI,</u> <u>MONITORAGGIO E CONTROLLO</u> a) Valutazioni e pareri di impatto ambientale: un fasc. per ciascun parere b) Monitoraggi della qualità delle acque: fasc. annuale per attività c) Monitoraggi della qualità dell'aria: fasc. annuale per attività d) Monitoraggi della qualità dell'etere: un fasc. annuale per attività e) Altri eventuali monitoraggi: fasc. annuale per attività f) Fascicoli relativi alle irregolarità g) Controlli a campione sugli impianti termici dei privati: fasc. annuale (e/o per attività) h) Fascicoli relativi alle irregolarità in materia ambientale i) Contravvenzioni sanitarie	Permanente 10 anni 10 anni 10 anni 10 anni 10 anni 2 anni 10 anni	Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare Conservazione campioni a scadenza regolare

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 5
PROFILASSI E VIGILANZA VETERINARIA
PROTEZIONE ANIMALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ZOOPROFILASSI VETERINARIA</u> a) Fasc. relativi a epizootie (epidemie animali): un fasc. per ciascun evento b) Verbali di interrimento animali indotti all'alimentazione (se esiste un repertorio)	Permanente 10 anni	
2) <u>RANDAGISMO ANIMALI E RICOVERI</u> a) Gestione dei ricoveri e degli eventi connessi: un fasc. per ciascun procedimento	3 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 6
POLIZIA MORTUARIA

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>POLIZIA MORTUARIA E CIMITERI</u> a) Registro di seppellimento b) Registri di tumulazione c) Registri di esumazione d) Registri di estumulazione e) Registri di cremazione f) Registri della distribuzione topografica delle tombe g) Trasferimento delle salme: un fasc. per ciascun trasporto fuori comune h) Copie di avvisi per esumazione di salme nei Cimiteri i) Concessioni Cimiteriali: repertorio j) Fascicoli personali dei concessionari: un fasc. per ciascun concessionario k) Lampade votive l) Camera mortuaria	Permanente Permanente Permanente Permanente Permanente Permanente 50 anni 10 anni Permanente 5 anni dalla cessazione del rapporto Permanente (previo sfoltimento conservando solo offerta ditta appaltatrice, verbale gara, contratti) Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 7
CIRCOLARI - NORME - STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEGISLAZIONE E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su Leggi specifiche b) Circolari pervenute c) Circolari emanate dal Comune	Permanente Permanente Permanente	
2) <u>STATISTICHE CAT. IV</u>	Permanente	



CATEGORIA V
FINANZE E CONTABILITA'

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria —▶ 5 anni

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
3) <u>GESTIONE DELLA SPESA: IMPEGNO, LIQUIDAZIONE, ORDINANZA E PAGAMENTO</u> a) Impegni di Spesa (determinazioni dei dirigenti delle UOR): copie inviate alle UOR alla Ragioneria: repertorio annuale b) Fatture ricevute: repertorio annuale c) Atti di liquidazione con allegati trasmessi da ciascuna UOR: repertorio annuale d) Mandati e Reversali di pagamento con allegati emessi dalla Ragioneria e inviati alla Tesoreria: repertorio annuale e) Eventuali copie di mandati (scatoloni) f) Libri mastri mandati e reversali g) Verbali chiusura dell'esercizio finanziario h) Copia delibere pagamento gettoni presenza i) Libri contabili obbligatori in base alle leggi fiscali j) Solleciti pagamento fatture pervenute al Comune k) Proventi da affitti e locazioni: un fasc. annuale per ciascun immobile locato l) Diritti di segreteria: registri annuali m) Ricevute dei versamenti in banca delle somme riscosse nelle differenti UOR per diritti di segreteria n) Fatture emesse: repertorio annuale o) Bollettari vari p) Ricevute di pagamenti vari	2 anni 10 anni 2 anni 10 anni dall'approvazione del Bilancio 2 anni Permanente Permanente 5 anni Permanente 5 anni 5 anni dal termine del contratto 5 anni 5 anni 10 anni 5 anni 5 anni	Purchè registrati in scritture contabili di sintesi Purchè verificati con gli originali
4) <u>PARTECIPAZIONI FINANZIARIE</u> (Es. Azioni) a) Gestione delle partecipazioni finanziarie: un fasc. per ciascuna partecipazione	Permanente, previo sfolgimento	
5) <u>RENDICONTO DELLA GESTIONE; ADEMPIMENTI E VERIFICHE CONTABILI</u> a) Rendiconto della Gestione articolato in Conto del Bilancio, Conto del Patrimonio e Conto Economico	Permanente	
6) <u>ADEMPIMENTI FISCALI CONTRIBUTIVI E ASSICURATIVI</u> a) Mod. 770 b) Ricevute dei versamenti (IVA, IRPEF, etc) c) Pagamento dei premi dei contratti assicurativi	10 anni 10 anni 5 anni dall'estinzione del contratto	Più se si ritiene opportuno
7) <u>REVISORI DEI CONTI</u> a) Fascicolo personale	Permanente	
8) <u>AGENTI CONTABILI</u> a) Registri delle riscossioni dei diritti comunali b) Atti relativi al riparto dei diritti comunali c) Verbali Agenti Contabili	10 anni 10 anni 10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 3
IMPOSTE E TASSE ERARIALI E REGIONALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>AVVISI DI PAGAMENTO PER COMPARTICIPAZIONE DI IMPOSTE ERARIALI A FAVORE DEL COMUNALI</u>	10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 4
IMPOSTE E TASSE COMUNALI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>GESTIONE DELLE ENTRATE; ACCERTAMENTO, RISCOSSIONE, VERSAMENTO</u>		
a) Fascicoli personali dei contribuenti comunali: un fasc. per ciascun contribuente per ciascun tipo di imposte (TARSU, COSAP, etc), con eventuali sottofascicoli (variazioni, ricorsi, etc)	10 anni dopo la cancellazione del contribuente dai ruoli	
b) Dichiarazioni ICI	10 anni dopo la cancellazione del contribuente dai ruoli Illimitato	
c) Ruoli tributi: base di dati	10 anni	Prevedere una stampa periodica
2) <u>PUBBLICITA' E PUBBLICHE AFFISSIONI</u>		
a) Autorizzazione alla pubblicità stabile: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	Salvo non si rilevi qualche necessità particolare di conservazione a campione
b) Autorizzazione alla pubblicità circoscritta: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	
c) Richieste di affissione: un fasc. per richiesta	5 anni dalla scadenza dell'autorizzazione	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 5
FINANZE, MONOPOLI, DOGANE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
==	==	==

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 6
MUTUI/CONTRIBUTI EROGATI DAL COMUNE
E ALTRI ENTI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>CONTRATTI DI MUTUO</u> : un fasc. per ciascun mutuo	5 anni dall'estinzione del mutuo	
2) <u>CONTRIBUTI COMUNALI</u> : a) Albo Beneficiari b) Un fasc. per ciascun contributo	Permanente 5 anni dall'erogazione	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 7
ESATTORIA - TESORERIA

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>TESORERIA</u> a) Giornale di cassa b) Mandati quietanzati, repertorio periodico (nello scatolone)	Permanente 10 anni	
2) <u>CONCESSIONARI ED ALTRI INCARICATI DELLA RISCOSSIONE DELLE ENTRATE</u> a) Concessionari: un fascicolo per ciascuno dei concessionari	10 anni dalla cessazione del rapporto	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 8
CIRCOLARI - NORME - STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEGISLAZIONI E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su Leggi specifiche b) Circolari pervenute c) Circolari emanate dal Comune	Permanente Permanente Permanente	
2) <u>STATISTICHE CAT. V</u>	Permanente	



CATEGORIA VI
GOVERNO

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 1

LEGGI E DECRETI/ RAPPORTI CON ORGANI DELLO STATO

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
a) RAPPORTI CON ORGANI DELLO STATO: (es. Prefettura)	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 2

FESTE NAZIONALI/COMMEMORAZIONE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
a) FESTE NAZIONALI / COMMEMORAZIONI	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 3

SERVIZIO ELETTORALE - ELEZIONI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ALBI ELETTORALI</u> a) Albo dei Presidenti di seggio: un elenco per ciascuna elezione b) Albo degli Scrutatori: un elenco per ciascuna elezione	5 anni 5 anni	
2) <u>LISTE ELETTORALI</u> a) Liste generali b) Liste sezionali c) Verbali della commissione elettorale comunale d) Copia dei verbali della Commissione elettorale mandamentale in ordine alle operazioni e deliberazioni adottate dalla Commissione Elettorale Comunale e) Schede dello schedario f) Fasc. personali degli elettori: un fasc. per ciascun elettore g) Elenchi recanti le proposte di variazione delle liste elettorali h) Carteggio concernente la tenuta e la revisione delle liste elettorali i) Corrispondenza generica fine a se stessa che non genera suo procedimento	1 anno dopo la redazione della successiva 1 anno dopo la redazione della successiva Permanente 5 anni 5 anni dopo la redazione della successiva 5 anni dopo la cancellazione dalla lista 5 anni dopo la redazione della lista successiva 5 anni dopo la redazione della lista successiva 5 anni	

3) <u>ELEZIONI</u>		
a) Convocazione dei comizi elettorali: un fasc. per ciascuna elezione	Permanente	
b) Presentazione delle liste: manifesto	Permanente	
c) Presentazione delle liste: carteggio	5 anni	
d) Atti relativi alla costituzione e arredamento dei seggi (es. verbali di consegna del materiale elettorale) e alla propaganda	5 anni	
e) Verbali dei presidenti di seggio		Trasmessi al Ministero dell'Interno
f) Schede		Trasmessi al Ministero dell'Interno
g) Pacchi scorta elezioni	2 anni	
h) Certificati elettorali non ritirati	2 anni	
i) Istruzioni elettorali a stampa	2 anni	
4) <u>REFERENDUM</u>		
a) <u>Atti preparatori</u>	5 anni	
b) <u>Verbali sezionali</u>	5 anni	
c) <u>Atti relativi alla costituzione e arredamento dei seggi</u>	5 anni	
d) <u>Verbali dei Presidenti di seggio</u>		Trasmessi al Ministero dell'Interno
e) <u>Schede</u>		Trasmesse al Ministero dell'Interno
f) <u>Atti relativi alla regolamentazione della propaganda (conservando la documentazione riassuntiva)</u>	5 anni	
g) <u>Verbali sezionali dei referendum abrogativi</u>	5 anni 10 anni	
5) <u>ISTANZE, PETIZIONI E INIZIATIVE POPOLARI</u>		
a) Raccolta di firme per referendum previsti dallo Statuto: un fasc. per ciascuna iniziativa	5 anni dopo il Referendum	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 4 PARTITI, MOVIMENTI POLITICI, SINDACATI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>PARTITI, MOVIMENTI POLITICI, SINDACATI</u> Rapporti con il Comune	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 5 REGIONE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>REGIONE</u> Rapporti con il Comune	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 6
UNIONE EUROPEA**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1. <u>UNIONE EUROPEA</u> Rapporti in riferimento	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 7
PROVINCIA**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
2. <u>PROVINCIA</u> Rapporti con il Comune	Permanente salvo sfoltimento	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 8
CIRCOLARI - NORME - STATISTICHE**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LIGISLAZIONE E CIRCOLARI ESPLICATIVE</u>		
a) Pareri chiesti dal Comune su leggi specifiche	Permanente	
b) Circolari	Permanente	
c) Circolari emanate dal Comune	Permanente	
2) <u>STATISTICHE CAT. VI</u>	Permanente	



CATEGORIA VII
GIUSTIZIA E CULTO

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 1
PRETURA - TRIBUNALE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>GIUDICI POPOLARI</u> a) Liste dei Giudici Popolari b) Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fasc. per ciascun periodo	Permanente 3 anni dall'ultima revisione	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 2
ARCHIVIO NOTARILE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ELENCHI NOTAI</u>	Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 3
CULTO

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
2) <u>SANTUARIO B.V. GRAZIE</u> a) Corrispondenza generica fine a se stessa (che non genera un suo procedimento)	Permanente salvo sfooltimento relativo ad atti 5 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 4
CIRCOLARI - NORME - STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEGISLAZIONE E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su Leggi specifiche b) Circolari pervenute c) Circolari emanate dal Comune	Permanente Permanente Permanente	
2) <u>STATISTICHE CAT. VII</u>	Permanente	



CATEGORIA VIII
LEVA

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 1
LEVA**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEVA</u> a) Liste di Leva: una per anno b) Lista degli eliminati/esentati: una per anno	Permanente Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 2
SERVIZIO MILITARE - RUOLI - CONGEDI**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>RUOLI MATRICOLARI</u> a) Ruoli Matricolari: uno per anno b) Carteggio tra i Comuni per l'aggiornamento dei ruoli matricolari c) Corrispondenza per la richiesta e la trasmissione dei certificati di esito leva d) Richiesta di invio di notizie varie relative a militari (esclusi i periodi bellici) e) Corrispondenza generica fine a sé stessa (inviti, varie non esaminate etc ...) che non genera un suo procedimento	Permanente 10 anni 10 anni 10 anni 10 anni	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 3
SERVIZIO CIVILE SOSTITUTIVO DI LEVA**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
==	==	==

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

**CLASSE 4
AUTORITA' MILITARI - DISTRETTO - DEMANIO MILITARE**

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>CASERME, ALLOGGI E SERVITU' MILITARI</u> a) Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
2) <u>REQUISIZIONI PER UTILITA' MILITARI</u> a) Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 5
ISTITUZIONI E ASSOCIAZIONI MILITARI

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>ASSOCIAZIONI - ISTITUZIONI MILITARI</u> a) 1 fascicolo per ogni associazione e/o istituzione militare costituita	Permanente	

^^^^^^^^^^^^^^^^^^^^^^^^^^^^

CLASSE 6
CIRCOLARI - NORME - STATISTICHE

TIPOLOGIA DOCUMENTAZIONE	CONSERVAZIONE	NOTE
1) <u>LEGISLAZIONE E CIRCOLARI ESPLICATIVE</u> a) Pareri chiesti dal Comune su Leggi specifiche b) Circolari pervenute c) Circolari emanate dal Comune	Permanente Permanente Permanente	
2) <u>STATISTICHE CAT. VIII</u>	Permanente	



CATEGORIA IX
CULTURA – ISTRUZIONE – SPORT
TEMPO LIBERO

N.B.:CORRISPONDENZA GENERICA fine a sé stessa che non genera suo procedimento
relativo a tutte le classi della presente categoria → 5 anni

