**C I T T A' D I L E N D I N A R A**
**PROVINCIA DI ROVIGO**

# DOCUMENTO PROGRAMMATICO PER LA SICUREZZA DEI DATI PERSONALI

## ANNO 2015

**Approvato con delibera di Giunta Municipale n. 90 del 28.04.2015**

## CONTENUTO DEL DOCUMENTO

PARTE I : Note introduttive e preliminari

PARTE II : Documento Programmatico per la Sicurezza del trattamento dei dati personali

PARTE III : Elenco delle schede valutative degli ambienti e delle attrezzature in dotazione agli Uffici

PARTE IV: Descrizione delle caratteristiche tecniche delle attrezzature informatiche utilizzate da ciascun Ufficio

PARTE V : Rilevazione dei trattamenti di dati sensibili e giudiziari eseguiti dagli Uffici in relazione alle rilevanti finalità di interesse pubblico previste dalla legge. Elenco delle strutture e degli incaricati preposti ai trattamenti.

PARTE VI : Criteri tecnici ed organizzativi in ordine alla protezione degli ambienti e degli archivi circa la riservatezza dei dati personali e analisi dei rischi.

PARTE VII : Manuale per la Sicurezza nell'uso delle tecnologie informatiche.
Linee guida per la sicurezza nell'utilizzo delle tecnologie informatiche

SISTEMA DI VIDEOSORVEGLIANZA URBANA - Appendice di aggiornamento al Documento Programmatico sulla Sicurezza dei dati personali redatta in osservanza del Provvedimento Generale del Garante della privacy dell'8 aprile 2010

# PARTE I°

# NOTE INTRODUTTIVE E PRELIMINARI

Scopo del Documento Programmatico per la Sicurezza (DPS) è di fornire (nell'ambito del contesto normativo attuale) le indicazioni necessarie per l'individuazione e la successiva adozione delle misure/sistemi di protezione che debbono essere realizzate ed attivati per una gestione "sicura" del trattamento dei dati personali da parte di tutte le strutture operative ed organizzative del Comune.

Scopo è altresì quello di fornire concrete indicazioni per supportare il personale comunale o terzo autorizzato nell'applicazione degli adempimenti normativi di riferimento, sia nel contrastare eventuali potenziali minacce all'integrità e segretezza dei sistemi informativi comunali.

In questo senso, il decreto legislativo 196 del 30 giugno 2003, "*Codice sulla protezione dei dati personali*" (Codice della privacy), che costituisce la fonte primaria di regolamentazione in materia, non si limita alla sola enunciazione delle informazioni delle persone da proteggere, ma prescrive regole precise e modalità di comportamento a cui gli Enti pubblici e le Aziende devono sottostare, nel momento in cui trattano tali informazioni.

Rispetto alla previgente Legge 675 del 1996 ed al D.P.R. n. 318 del 1999 (che ha introdotto il DPS), le regole stabilite dal D.Lgs. 196/2003 per il trattamento dei dati personali comuni, identificativi, sensibili e giudiziari sono rivolte innanzitutto alla salvaguardia del diritto all'identità e alla riservatezza di ciascun cittadino sancito dalle normative internazionali, con particolare riferimento alla idonea introduzione di apparati tecnici e modalità procedurali per la protezione dei sistemi informativi aziendali.

Pertanto, le soluzioni di sicurezza indicate in questo documento hanno lo scopo di costituire la base per l'attuazione delle politiche generali di sicurezza e di garanzia dei diritti delle persone, alla luce delle nuove disposizioni normative e tecniche e di rappresentare il livello ritenuto adeguato di protezione dei sistemi di gestione degli archivi informatici e non.

L'Amministrazione, si riserva, inoltre, di valutare nel tempo l'idoneità delle misure adottate e di migliorare la barriera di protezione implementando successivamente ulteriori accorgimenti e tecnologie.

## 1. ORGANIZZAZIONE DELLA SICUREZZA

Per assicurare che le contromisure individuate (qualunque siano, dalle logiche a quelle tecnologiche) possano effettivamente essere rese operative, è indispensabile integrare la struttura organizzativa esistente con una rete di responsabilità specifiche sulla sicurezza e condividere una serie di principi e regole che devono guidare la corretta gestione della sicurezza.

La politica generale dell'Amministrazione è di considerare e trattare le informazioni ed i servizi come parte integrante del Patrimonio comunale; è quindi intenzione dell'Amministrazione garantire, in analogia a quanto avviene per le altre attività, il corretto svolgimento delle azioni di prevenzione, protezione e contrasto tramite la definizione delle seguenti logiche organizzative:

- valutazione e descrizione degli ambienti e delle infrastrutture in uso ai Servizi Comunali;
- valutazione della tipologia degli archivi e della natura dei dati trattati;
- analisi dei rischi di perdita e di distruzione delle informazioni;
- monitoraggio dell'attività svolta e dei comportamenti;
- definizione di un certo standard di protezione che riduca al minimo i rischi;
- predisposizione di un modello organizzativo della sicurezza;
- programmazione e realizzazione delle misure si sicurezza;
- attivazione di una politica di corretta responsabilizzazione degli incaricati

## 2. LINEE DI BASE DI INFORMAZIONE SULLA SICUREZZA

Per facilitare ed accelerare lo sviluppo di una adeguata consapevolezza sui rischi e sull'esigenza di proteggere il patrimonio informativo si rende necessario coinvolgere le risorse umane dell'Ente nei seguenti processi che formano requisito indispensabile per qualsiasi processo di sicurezza:

1 - attuare un processo di sensibilizzazione sul valore delle informazioni, sul rischio al quale risultano esposte, sulle misure di sicurezza e sulla importanza di progettarle adeguatamente ed in linea con le risorse e potenzialità del Titolare;

2 - programmare una serie di comunicazioni finalizzate a promuovere la corresponsabilizzazione e la consapevolezza riguardo alle nuove logiche, modelli e comportamenti organizzativi della sicurezza;

3 - pianificare la diffusione di informazioni relativamente agli argomenti chiave della gestione della sicurezza: analisi e gestione del rischio, pianificazione e monitoraggio delle contromisure, normativa e regolamentazione e controllo.

## 3. GESTIONE DELLA SICUREZZA

Per ottenere il funzionamento della sicurezza organizzativa occorre dotare la struttura dell'Amministrazione di un sistema di gestione della sicurezza composto da:

a) Regolamento sul trattamento dei dati personali e sulla sicurezza degli archivi, che definisce gli obiettivi e le finalità del trattamento delle informazioni e delle strategie di sicurezza scelte dall'Amministrazione nonché il modello organizzativo ed i processi per attuarle.
b) Regolamento sul trattamento dei dati sensibili e giudiziari, che definisce le tipologie di dati trattabili e le relative modalità di utilizzo per il conseguimento delle finalità dichiarate di rilevante interesse pubblico.
c) Direttive da seguire per lo sviluppo, la gestione, il controllo e la verifica delle misure di sicurezza da adottare, concernenti anche i comportamenti che il personale deve tenere nella gestione delle informazioni; tali Direttive devono essere modificate al verificarsi di cambiamenti organizzativi e tecnologici.
d) Specifiche procedure, a supporto delle gestione operativa delle contromisure tecnologiche adottate.

## 4. ANALISI E GESTIONE DEL RISCHIO

L'analisi del rischio è un processo fondamentale per la pianificazione, realizzazione e gestione di qualsiasi sistema di sicurezza delle banche dati e dei sistemi di gestione e telecomunicazione informatica.

Infatti, senza una costante valutazione del valore del patrimonio informativo del Comune, dell'intensità delle minacce attuali e potenziali, delle vulnerabilità del sistema e dei potenziali impatti tangibili e intangibili sull'attività e sul posizionamento dell'Amministrazione, risulta impossibile definire un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero verificarsi.

In un sistema di governo delle P.A. sempre più aperto, cooperante, digitale ed interconnesso, anche a livello internazionale, i confini del rischio non hanno più barriere e le minacce diventano tutte possibili e, in qualche misura, sempre più probabili, ciascuna Amministrazione si deve pertanto dotare di un processo di analisi e gestione del rischio secondo lo schema seguente:

- Identificazione e valutazione dei locali e dei beni utilizzati dall'organizzazione, i processi e le informazioni trattate per gli scopi istituzionali.
- Valutazione delle potenziali minacce associate alla lista dei locali e dei beni utilizzando i criteri conosciuti di vulnerabilità.
- Selezione e pianificazione dei controlli sui sistemi di sicurezza e documentazione dei controlli effettuati.
- Adozione di misure idonee alla riduzione dei rischi rilevati per ogni locale, ambiente, archivio e strumento utilizzato.

## 5. LA GESTIONE DELLE MISURE DI PROTEZIONE

Il raggiungimento degli obiettivi di sicurezza richiede non solo l'utilizzo di appropriati strumenti fisici e tecnologici (materiali, tecnici, elettronici, informatici), ma anche gli opportuni meccanismi organizzativi e formativi del personale impiegato.

Infatti, misure soltanto tecniche, per quanto possano essere appropriate e sofisticate, non saranno efficienti se non utilizzate in sintonia con le altre modalità volte a garantire in termini generali la sicurezza del trattamento e dell'archiviazione delle informazioni personali.

Gli strumenti di protezione, quindi, devono essere configurati con riferimento alle risultanze delle elaborazioni condotte dall' Amministrazione in relazione all'analisi dei rischi.

L'impostazione attuale del piano operativo dovrà peraltro tener conto della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture (servizi dell'Ente Locale) preposte al trattamento dei dati stessi.

In questo senso il DPS deve rappresentare l'atto fondamentale di programmazione (piano operativo generale) delle politiche di sicurezza, che costituisce per le amministrazioni l'opportunità di razionalizzare l'intero complesso degli elementi di garanzia per il trattamento dei dati personali.

Il quadro d'insieme può pertanto essere utilmente riferito sia alle misure di sicurezza per il trattamento di dati personali in generale sia, soddisfacendo il dettato normativo, per quello di dati sensibili e giudiziari.

Tale documento ha valenza di piano operativo, raccogliendo una serie di soluzioni organizzative e di linee-guida tecniche generali: esso può essere quindi approvato e successivamente aggiornato dalla Giunta, con propria deliberazione, entro il termine di legge e successivamente inviato ai Responsabili di Settore/Servizio per gli adempimenti di competenza.

# PARTE II

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

# ANNO 2015

# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

## 1. SCOPO

Il presente Documento Programmatico Sulla Sicurezza è adottato allo scopo di definire le politiche di sicurezza in materia di trattamento di dati personali ed i criteri organizzativi per la loro attuazione. In particolare nel Documento Programmatico Sulla Sicurezza (DPS) vengono definiti i criteri tecnici e organizzativi per:

a) la protezione delle aree e dei locali interessati dalle misure di sicurezza e controllare l'accesso delle persone autorizzate ai medesimi locali

b) i criteri e le procedure per assicurare l'integrità delle informazioni;

c) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;

d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni dovuti dalla perdita o distruzioni delle informazioni in possesso dell'Ente.

## 2. CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza (DPS), in raccordo con i Regolamenti comunali di attuazione delle norme sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, definisce le politiche organizzative e gli standard necessari di sicurezza in merito al trattamento dei dati personali.

Il DPS riguarda tutti i dati gestiti dal Comune di Lendinara che siano:

- Personali,
- Identificativi,
- Sensibili,
- Giudiziari,
- Comuni.

Il DPS si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di gestione, elaborazione e conservazione (computer, web, supporti magnetici o di altra generazione, ecc.),
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.).

Il DPS deve essere conosciuto ed applicato da tutti gli Uffici dell'Amministrazione Comunale.

## 3. RIFERIMENTI NORMATIVI

Decreto Legislativo 30 giugno 2003 numero 196,
Decreto Legislativo 18 agosto 2000 numero 267,
Regolamento Comunale sull'ordinamento generale degli uffici e dei Servizi.
Regolamento Comunale per la tutela e la riservatezza rispetto al trattamento dei dati personali.
Regolamento Comunale per la tutela e la riservatezza rispetto al trattamento dei dati sensibili e giudiziari.

## 4. I COMPITI DELLE SINGOLE FIGURE PREVISTE DALLA NORMATIVA A PROTEZIONE DEI DATI PERSONALI NEL SETTORE DELLA SICUREZZA

### 4.1. IL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è il Comune di Lendinara.

E' onere del Titolare individuare all'interno dell'Ente, nominare ed incaricare uno o più responsabili del trattamento dei dati che assicurino e garantiscano l'adozione delle misure di sicurezza previste dalla normativa vigente.

Il Titolare esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del

trattamento, ivi compreso il profilo della sicurezza (cfr art. 28 del D. Lgs. n. 196/2003).

Il Titolare del trattamento può affidare al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni.

Altri compiti in capo al Titolare:

- informa tempestivamente i Responsabili, tramite il "Servizio AA.GG. – Organizzazione e Informatizzazione", circa le variazioni delle norme in materia di trattamento di dati personali, nonché in merito alle regole che definiscono i compiti degli stessi;
- assume, su proposta dei Responsabili, le decisioni in ordine alle finalità del trattamento, ivi compreso il profilo della sicurezza;
- acquisisce sempre tramite il Servizio AA.GG. – Organizzazione e Informatizzazione relazioni annuali dei Responsabili circa i trattamenti effettuati;
- effettua, attraverso il Servizio AA.GG. – Organizzazione e Informatizzazione, controlli sull'operato dei Responsabili, anche verificando la conformità al D.P.S. delle procedure adottate;
- coordina direttamente o su delega l'applicazione delle misure di sicurezza;
- emana annualmente attraverso deliberazione di Giunta Municipale gli aggiornamenti al D.P.S. ed eventuali allegati.

## 4.2. IL RESPONSABILE DEL TRATTAMENTO

Il Responsabile è designato dal Titolare facoltativamente.

In caso di nomina a ciascun Responsabile del trattamento il Titolare del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile del trattamento è a tempo indeterminato e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati, con preavviso scritto di almeno 10 giorni ed eventualmente affidata ad altro soggetto. Se designato il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario, per esigenze organizzative, possono essere designati Responsabili più soggetti, anche mediante suddivisione dei compiti.

I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare.

Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni.

Il Responsabile del trattamento dei dati è preposto alla gestione e tutela dei dati personali che rientrano nell'ambito delle funzioni di propria competenza, nonché alla salvaguardia dell'integrità e della sicurezza degli stessi.

Con riferimento a quanto sopra enunciato, il Responsabile:

a) cura il coordinamento di tutte le operazioni di trattamento dei dati;
b) impartisce istruzioni per la corretta elaborazione dei dati personali;
c) procede alle verifiche sulla metodologia di introduzione e di gestione dei dati, attraverso controlli a campione da eseguirsi periodicamente;
d) è responsabile dei procedimenti di rettifica dei dati;
e) adempie a quanto disposto dalle Autorità ed Organi di vigilanza del sistema amministrativo locale;
f) impartisce disposizioni operative per la sicurezza delle banche dati e dei procedimenti di gestione e/o trattamento degli stessi;
g) cura la relazione delle singole banche dati, cui sovrintende, con il Servizio Sistemi Informativi del Comune.
h) cura la informazione agli interessati relativa al trattamento dei dati ed alla loro comunicazione e diffusione;
i) dispone motivatamente il blocco dei dati, qualora sia necessaria una sospensione temporanea delle operazioni del trattamento, dandone tempestiva comunicazione al Titolare.

Il Responsabile del trattamento ha inoltre il compito di:

- scegliere ed eventualmente attribuire, con l'ausilio dell'Amministratore di sistema, ad ogni Utente

(USER) o incaricato, un Codice identificativo personale (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili e giudiziari qualora si utilizzino elaboratori accessibili in rete; per gli stessi dati qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- Verificare, con l'eventuale ausilio dell'amministratore di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali e le misure indicate al successivo paragrafo 10;
- Garantire che tutte le misure di sicurezza riguardanti i dati in possesso del Comune di Lendinara siano applicate anche eventualmente al di fuori dell'ente, qualora siano cedute a soggetti terzi quali Responsabili del trattamento tutte o parte delle attività di trattamento;
- Informare il Titolare nella eventualità che si siano rilevati dei rischi.

## 4.3. CUSTODE DELLE PASSWORD

Ogni Responsabile del trattamento è custode delle password gestite e ne risponde nelle relative sedi. Ai custodi delle password è conferito il compito di custodire la parola chiave o password per accedere ai dati archiviati nel sistema di elaborazione dei dati.

La nomina di ciascun Custode delle password deve essere effettuata con una lettera di incarico.

Ciascun custode della password deve essere informato della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore.

La nomina a custode della password è a tempo indeterminato e decade per revoca o dimissioni dello stesso.

La nomina del Custode della password in caso di grave inadempienza può essere revocata in qualsiasi momento dal Titolare del Trattamento o dall'Amministratore di sistema senza preavviso, ed essere affidata ad altro soggetto.

L'Amministratore di sistema (di cui al successivo punto 4.4) è supervisore nella custodia delle password dei singoli Responsabili del trattamento e deve predisporre, per ognuno di essi una busta sulla quale è indicato lo USER-ID utilizzato, all'interno della busta deve essere indicata la password usata per accedere alla banca di dati comunale.

Le buste con le password devono essere conservate in luogo chiuso e protetto.

Il predetto Amministratore di sistema deve revocare tutte le password non utilizzate per un periodo superiore a 6 (sei) mesi.

## 4.4. AMMINISTRATORE DI SISTEMA

L'Amministratore di sistema, sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di banche dati. Ai fini del presente documento deve considerarsi Amministratore di sistema la Posizione Organizzativa incaricata dal Sindaco quale Responsabile e Curatore del Sistema Informativo. Lo stesso opererà in sinergia e collaborazione con il Responsabile del Servizio Organizzazione e Informatizzazione.

I succitati Responsabili, per i compiti afferenti all'Amministrazione di sistema, potranno se necessario avvalersi di consulenze tecniche esterne.

Spettano all'Amministratore del Sistema Informativo comunale:

1. il compito di sovrintendere alle risorse del sistema informativo e del sistema di dati organizzato in archivi gestiti elettronicamente, consentendone l'utilizzo secondo i criteri di sicurezza previsti dalla vigente normativa;
2. il compito di coordinare ed eseguire, secondo le indicazioni del Titolare e/o dei Responsabili , il trattamento e/o l'estrazione di dati aggregati;
3. Collaborare con il Servizio Organizzazione e Informatizzazione per:
   - l'eventuale istituzione e aggiornamento di un registro delle banche dell'Ente contenenti dati personali gestite elettronicamente;
   - l'adozione del Documento Programmatico per la Sicurezza ed i relativi aggiornamenti.
4. L'Amministratore esprime parere circa le autorizzazioni e le intese concernenti il collegamento telematico tra il sistema informativo comunale e le banche dati di altri soggetti; collabora per la garanzia

della sicurezza dei sistemi informatici dell'Ente, intendendosi con tale dizione quanto segue:

- ricognizione ed eventuale coordinamento in merito ad implementazione di misure preventive quali: back-up dei dati e dei software, gruppi di continuità, individuazione di centri dati alternativi,
- piano di emergenza: individuazione delle priorità di ripristino con adeguata e costante informazione agli addetti del Comune;
- istruzione dell'attività di ripristino: persone da contattare per ciascun blocco/anomalia, modalità di tenuta e recupero dei nastri copia e/o altri supporti;
- test periodici di verifica: monitoraggio del piano ed aggiornamento del personale circa le nuove misure predisposte;
- disaster recovery;
- redazione, aggiornamento ed eventuale coordinamento per implementazione delle misure minime di sicurezza.

Fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER-ID). in caso di perdita della qualità che consentiva al Responsabile del trattamento (utente o incaricato) l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (USER-ID) per oltre 6 mesi;

5. Spetta esclusivamente all'Amministratore di Sistema:

- la gestione degli elaboratori principali comunali (Server);
- la gestione degli identificativi di rete;
- al configurazione in rete di tutte le postazioni di lavoro connesse.

## 5. NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Il Responsabile del trattamento dei dati procede, d'intesa con il Titolare, all'individuazione all'interno di ciascun servizio comunale degli Incaricati del trattamento, ossia delle persone autorizzate nei vari uffici a compiere le operazioni di trattamento dei dati.

I compiti affidati agli Incaricati devono essere specificati per iscritto dal Responsabile del trattamento che deve controllarne l'osservanza e l'aggiornamento. Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti. Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina. Gli Incaricati al trattamento devono effettuare le operazioni di trattamento loro affidate attenendosi alle istruzioni ricevute. Agli Incaricati viene assegnato un codice personale per l'accesso ai dati gestiti dall'Amministratore di sistema.

La nomina degli Incaricati è a tempo indeterminato e decade per revoca, per sue dimissioni dall'impiego o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

## 5.1 SISTEMA INFORMATICO DELLA BIBLIOTECA COMUNALE

L'Amministratore di sistema non è responsabile per la gestione degli gli elaboratori (pc) e degli archivi informatici della biblioteca comunale, la cui gestione è riconducibile al competente Responsabile di Servizio.

## 6. DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO IN OUT-SOURCING

## 6.1 TRATTAMENTO DEI DATI IN OUTSOURCING

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi in out- sourcing, nominandoli Responsabili del trattamento. In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Nel caso in cui questi non vengano espressamente nominati i Responsabili del trattamento in out-sourcing ai sensi dell'art. 29, comma 2, del D.Lgs. 196/2003 devono intendersi autonomi titolari del trattamento e quindi soggetti al corrispettivi obblighi e pertanto rispondono direttamente e in via esclusiva per le eventuali violazioni alla legge.

Il Titolare del trattamento, ovvero, uno dei Responsabili del trattamento, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei

dati in qualità di Responsabile del trattamento, con particolare attenzione a quel soggetti terzi in out-sourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato.

## 6.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI A CUI AFFIDARE IL TRATTAMENTO DEI DATI IN OUTSOURCING

Il Titolare del trattamento può nominare Responsabile del trattamento in out-sourcing quel soggetti terzi che abbiano i requisiti individuati e professionali dell'art. 29, comma 2, del D. Lgs. 196/2003 (esperienza, capacità, affidabilità).

Il Responsabile del trattamento dei dati in out-sourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati.

## 6.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING

Per ogni trattamento affidato ad un soggetto esterno nominato Responsabile del trattamento in out-sourcing, il Titolare del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno

Il Titolare del trattamento deve informare il responsabile del trattamento dei dati in out-sourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore.

Il Responsabile del trattamento dei dati in out-sourcing deve accettare la nomina, utilizzando apposito modulo.

La nomina del Responsabile del trattamento dei dati in out-sourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro

# 7. INVENTARI E METODOLOGIE OPERATIVE DI TRATTAMENTO DEI DATI

## 7.1 INDIVIDUAZIONE DELLE BANCHE DI DATI OGGETTO DEL TRATTAMENTO

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di:

- Dati personali comuni;
- Dati identificativi;
- Dati personali sensibili
- Dati personali "super-sensibili";
- Dati personali giudiziari.

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro.

## 7.2 INVENTARIO DELLE SEDI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi nelle quali viene effettuato il trattamento dei dati.

## 7.3 INVENTARIO DEGLI UFFICI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati.

In particolare, per ogni ufficio deve essere indicata la sede e se l'accesso è controllato.

Per l'inventario degli uffici deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del trattamento della sicurezza dei dati in luogo sicuro.

Alla data di redazione del presente documento le sedi/uffici di trattamento delle banche dati

coincidono con le sedi operative del Comune di Lendinara site in: Piazza Risorgimento n. 1, Via G.B. Conti n. 26 e n. 32, Via Santa Maria Nuova n. 40 e Via Garibaldi n. 3 (Comando P.L.).

## 7.4 INVENTARIO DEI SISTEMI DI ELABORAZIONE

L'elenco dei sistemi di elaborazione costituisce la parte IV del presente Documento ed è soggetto a revisione annuale. Per ogni sistema debbono essere descritte le caratteristiche e se si tratta di sistema di elaborazione non accessibile da altri elaboratori (stand-alone), in rete, non accessibile al pubblico, in rete accessibile al pubblico. Per ogni sistema deve essere specificato il nome dell'Incaricato o degli Incaricati che lo utilizzano.

## 8. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

## 8.1 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRATA' DEI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, le copie di sicurezza delle banche di dati trattati devono essere eseguite giornalmente, mensilmente ed annualmente su idonei supporti. Sono suggerite dall'amministratore di sistema le modalità di controllo delle copie di back-up la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.

## 8.2 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato. Il Responsabile del trattamento dei dati stabilisce inoltre la periodicità, almeno ogni sei giorni con cui deve essere verificata la disponibilità degli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattati.

I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare, per ogni sistema debbono essere definite, se possibile, le seguenti specifiche:

- il tipo di programma utilizzato;
- la periodicità di aggiornamenti.

Per ogni sistema deve essere predisposto apposito modulo di Rilevazione di virus informatico, sul quale debbono essere annotati eventuali virus rilevati, e se possibile la fonte da cui sono pervenuti al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

I moduli compilati ed aggiornati dagli Incaricati del trattamento debbono essere conservati a cura del Responsabile del trattamento dei dati in luogo sicuro. Tali moduli possono anche essere conservati in software all'interno degli elaboratori stessi o dell'elaboratore centrale.

## 8.3 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'Amministratore di sistema, opportunamente coadiuvato anche da soggetti terzi, deve provvedere a:

- isolare il sistema,
- verificare se ci sono altri sistemi infettati con lo stesso virus informatico,
- identificare l'antivirus adatto e bonificare il sistema infetto,
- installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

L'Amministratore di sistema deve inoltre compilare apposito modulo di "*Report dei contagi da virus informatici*". I moduli compilati devono essere conservati a cura del Responsabile del trattamento dati in luogo sicuro. Tali moduli possono anche essere conservati in software all'interno degli elaboratori stessi o dell'elaboratore centrale.

## 8.4. CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI

Il Titolare del trattamento è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati. Per ogni banca dati deve essere individuato un idoneo luogo di conservazione ed idonei supporti da utilizzare per il back-up dei dati.

Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- agenti chimici;
- fonti di calore,
- campi magnetici,
- intrusioni ed atti vandalici,
- incendio,
- allargamento,
- furto.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati ai seguenti soggetti:

- Responsabile del trattamento della sicurezza dei dati,
- Eventuale Responsabile del trattamento di competenza,
- Incaricato del trattamento di competenza,
- Amministratore di sistema.

## 8.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

Spetta all'Amministratore di sistema decidere se i supporti magnetici utilizzati per le copie di back-up delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati. In caso positivo egli deve provvedere a cancellarne il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.

E' facoltà dell'Amministratore di sistema verificare che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni mi esso registrate.

## 8.6 PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le operazioni di back-up delle banche di dati trattate.

Per ogni incaricato del trattamento il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall' evoluzione tecnologica, se è necessaria una formazione tecnica adeguata.

## 9 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

## 9.1 NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto dal D.Lgs. n. 196/2003, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento dei dati di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati di stampe, tabulati elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento, al di fuori dalle ipotesi di accesso legittimo agli atti e documenti amministrativi.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati elenchi rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

## 9.2 PROCEDURE PER CONTROLLARE L'ACCESSO Al LOCALI IN CUI VENGONO TRATTATI I DATI

AI Responsabile del trattamento dei dati è affidato il compito di redigere a di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati nominando un apposito Incaricato, con il compito di controllare direttamente i sistemi le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati sono stabilite in conferenza di servizi tra tutti i Responsabili del trattamento. Attualmente le chiavi della sala c.e.d. sono consegnate ai seguenti responsabili del trattamento (in ordine alfabetico):

1) Buson Dante quale responsabile dal trattamento per i dati del servizio Affari Generali/Demografici e del Servizio Segreteria/Personale
2) Dallagà Natale quale responsabile dal trattamento per i dati del servizio Polizia Locale ("Municipale");
3) Lucchiari Lorenzo quale responsabile dal trattamento per i dati del servizio Ragioneria/Economato;
4) Melon Paolo quale responsabile dal trattamento per i dati del Servizio Tributi;

## 9.3. PROCEDURE DI ASSEGNAZIONE DEGLI USER-ID

Il Responsabile del trattamento dei dati in accordo con l'Amministratore di sistema, deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.

Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei codici identificativi assegnati per l'Amministratore di sistema, relativamente al sistemi operativi che prevedono un unico livello di accesso. In ogni caso, il codice identificativo assegnato ad un Incaricato del trattamento deve essere annullato se l'incaricato del trattamento ha dato le dimissioni dall'impiego.

## 9.4 PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD

Il Responsabile del trattamento dei dati deve definire in accordo con l'Amministratore di sistema le modalità di assegnazione delle password. In relazione al tipo di banca di dati trattata, l'Amministratore del sistema può decidere che ogni utente Incaricato del trattamento possa modificare autonomamente la propria password di accesso. In questo caso la modifica equivale alla comunicazione al Custode della password.

## 9.5 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica.

Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento dei dati in luogo sicuro, e deve essere trasmesso in copia controllata all'Amministratore di sistema di competenza.

Alla data di redazione del presente provvedimento gli elaboratori connessi alla rete pubblica (Internet) sono specificati nella Parte IV del presente documento come meglio descritto al precedente 7.4.

## 9.6 CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati quali: "Fibra ottica", "Modem", "Router", "ponte radio (Wi-Fi)", "Virtual Private Network (V.P.N.)" i Responsabili del trattamento dei dati possono stabilire, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I Responsabili del trattamento dei dati possono richiedere il supporto del Responsabile del Servizio Organizzazione e Informatizzazione che agirà in concerto con l'amministratore di sistema.

## 10 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

## 10.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali. In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo USER-ID assegnato.

In caso di dimissioni di un incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione all'Amministratore di sistema che provvederà a disattivare la possibilità di accesso al sistema per il soggetto mi questione.

Per redigere l'elenco degli Incaricati del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata all'Amministratore di sistema

Alla data di redazione del presente documento l'elenco degli incaricati è identificabile con la Parte IV di questo Documento Programmatico.

## 10.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

Al Responsabile del trattamento è affidato il compito di verificare ogni anno, entro il 31 dicembre, le autorizzazioni di accesso al dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo che deve essere conservato a cura del Responsabile del trattamento dei dati mi luogo sicuro e deve essere trasmesso in copia controllata all'Amministratore di sistema.

## 10.3 DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO Al DATI

All'Amministratore di sistema è affidato il compito, ove ciò sia possibile e/o consentito dal relativo software di gestione, di redigere e di aggiornare ad ogni variazione la tabella dei permessi di accesso che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.

In particolare per ogni Incaricato del trattamento e per ogni banca di dati debbono essere indicati i privilegi assegnati tra i seguenti:

- Inserimento di dati,
- Lettura e stampa di dati,
- Variazione di dati,
- Cancellazione di dati;
- Trasferimento de dati.

La tabella dei Permessi di accesso deve essere redatta, ove possibile, utilizzando l'apposito modulo che è presente sull'elaboratore principale (server di rete).

## 11.4 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DEI PERMESSI DI ACCESSO Al DATI

Al Responsabile del trattamento è affidato il compio di verificare ogni anno, entro il 31 dicembre, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo che deve essere conservato in luogo sicuro e deve essere trasmesso in copia controllata all'Amministratore di sistema.

## 11.5 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

I Responsabili, di concerto con gli Uffici dell'Ente preposti alla formazione del personale, organizzano gli interventi formativi per gli Incaricati del trattamento, laddove ciò risulti necessario in conseguenza dell'entrata in vigore di nuove normative o di variazione di quelle esistenti o di attivazione di nuovi trattamenti.

Gli interventi di formazione, limitatamente al personale interessato, sono opportuni nei seguenti casi:

- modificazione o integrazione della normativa di riferimento (*);

- modificazione o integrazione delle norme dell'Ente (*);
- variazione della struttura organizzativa dell'Ente;
- ridefinizione delle competenze dei Settori/Servizi e delle strutture subordinate;
- adozione di nuove procedure per la sicurezza dei dati (*);
- variazioni interne di una struttura;
- assunzione di personale (*);
- passaggio di categoria;
- variazione di qualifica;
- trasferimento ad altro Ufficio;
- assegnazione ad altro incarico o mansione;
- istituzione di nuovi trattamenti;
- variazione o aggiornamento dei trattamenti;
- istituzione di nuove procedure;
- variazione o aggiornamento di procedure;
- adozione di nuovi strumenti di trattamento;
- adozione di nuovi strumenti per la sicurezza dei dati (*).

Gli interventi di formazione sono improntati al principio del più ampio decentramento. Nei casi contrassegnati con l'asterisco (*), data la trasversalità delle materie, la formazione viene pianificata in collaborazione fra i vari Settori e Servizi dell'Amministrazione.

Il Responsabile predispone il piano di formazione e registra i corsi di formazione effettuati, dandone conto al Titolare. Nel caso in cui non ricorrano i presupposti per effettuare interventi di formazione, il Responsabile effettua opera di sensibilizzazione del personale, per iscritto e con cadenza almeno semestrale, richiamando i principi cui si ispira la normativa in materia, i provvedimenti delle Autorità competenti, le regole dell'Ente e le prescrizioni contenute nel presente DPS.

## 12. MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

### 12.1 MANUTENZIONE DI SISTEMI DI ELABORAZIONE DEI DATI

All'Amministratore di sistema, di concerto con i Responsabili di servizio, è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati i dati delle apparecchiature periferiche ed in particolare dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati,
- Il rischio di distruzione o di perdita,
- Il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica.

L'Amministratore di sistema, se ritenuto necessario, deve compilare se necessario apposito "*Modulo di evidenziazione dei rischi hardware*".

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

### 12.2 MANUTENZIONE DEI SISTEMI OPERATIVI

All'Amministratore di sistema ha la facoltà di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito tenendo conto in particolare di disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati,
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti,
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare se necessario apposito "*Modulo di evidenziazione dei rischi sui Sistemi Operativi*". Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei

dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

### 12.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

All'Amministratore di sistema è affidato il compito di verificare ogni anno, anche a campione o mediante l'intervento di terzi autorizzati, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati. La verifica anche se omessa non esime comunque da responsabilità l'utente. La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati,
- Il rischio di distruzione o di perdita dei dati,
- Il rischio di accesso non autorizzato o non consentito tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento o perdita di dati.

L'Amministratore di sistema deve compilare se necessario apposito "*Modulo di evidenziazione dei rischi nelle applicazioni*". Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

## 13. MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI

### 13.1 NOMINA E ISTRUZIONI AGLI INCARICATI

Per ogni archivio i Responsabili del trattamento dei dati debbono definire l'elenco degli **Incaricati** autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

Gli Incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni. Qualora i documenti contengano dati sensibili e giudiziari gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

### 13.2 COPIE DEGLI ATTI DEI DOCUMENTI

Quanto indicato nel punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

## 14. REVISIONI

Il presente Documento Programmatico Sulla Sicurezza (DPS), verrà revisionato annualmente ed eventualmente sottoposto a modifiche nel caso se ne ravvisi la necessità od opportunità..

# PARTE III

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

# Elenco delle schede valutative degli ambienti e delle attrezzature in dotazione agli Uffici

**Servizio Affari Generali – Legali - Demografici – Politiche Organizzazione e Informatizzazione**
ubicazione: Via G. B. Conti n. 26

I locali sono accessibili direttamente dall'esterno mediante un accesso.
Le porte esterne non sono del tipo "blindato".
Le finestre sono dotate di grate antintrusione (escluso 1° piano).
Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali sono protetti da sistema di allarme e non sono dotati di sistema rilevazione fumi.
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati; è presente una cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
chiusura a chiave di armadi e delle porte dei locali-archivio;
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Servizio Segreteria / Personale – Protocollo – Messi – Centralino**
ubicazione: Piazza Risorgimento, 1 – Primo Piano

I locali non sono accessibili direttamente dall'esterno.
Le finestre non sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Accesso ai locali in orario extra servizio consentito solo ad autorizzati.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme e non sono dotati di sistema rilevazione fumi (esclusa area bancone messi).
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati; è presente cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari non è controllato
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati..
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
chiusura a chiave degli uffici a fine orario di lavoro; custodia in armadi chiusi a chiave dei fascicoli del personale in servizio e in quiescenza.

* * *

**Locali Server Informatico**
ubicazione: Piazza Risorgimento n. 1 – locali mansardati

I locali non sono accessibili direttamente dall'esterno. E' presente una sola finestra a lucernario di piccole dimensioni.
Le porte interne sono stabilmente chiuse a chiave. Gli apparati informatici sono racchiusi da una gabbia metallica chiusa a chiave.
Nel locale è presente un sistema di allarme antincendio e di rilevazione dei fumi. Non è presente sistema di allarme antintrusione.

I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il locale è climatizzato per garantire l'efficienza operativa dell'hardware informatico.
Accesso ai locali consentito solo ad autorizzati sia in orario di servizio che extra-servizio.

* * *

**Archivio Cartaceo Generale**
ubicazione: Piazza Risorgimento n. 1 – locali mansardati

I locali non sono accessibili direttamente dall'esterno.
Le finestre presenti sono di tipo a lucernario e parzialmente dotate di grata antintrusione.
Le porte dei locali adibiti ad archivio cartaceo sono stabilmente chiuse a chiave
Le chiavi di accesso ai locali sono esclusivamente detenute da: Comando P.L., Messi Comunali, Ufficio Protocollo, Segreteria, LL.PP.
I locali non sono protetti da sistema di allarme ma sono dotati di sistema rilevazione fumi e sono dotati di sistema anticendio/spegnimento automatico.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.

* * *

**Servizio Contabilità ed Economato**
**Pianificazione e Programmazione Economica-Finanziaria - Bilancio**
ubicazione: Piazza Risorgimento n. 1 – Primo Piano

I locali sono accessibili direttamente dall'esterno (ulteriore ingresso con scale di servizio su Via G.B. Conti permanentemente non utilizzato).
N. 2 finestre sono dotate di grate antintrusione e n. 4 non lo sono.
Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione. I locali non sono dotati di sistema anticendio/spegnimento automatico e non sono dotati di sistema rilevazione fumi (esclusa area archivio provvista del solo apparato di rilevazione dei fumi).
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati; è presente una cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
accesso ai locali in orario extra servizio consentito solo ad autorizzati
tutti gli archivi cartacei sono custoditi in armadi chiusi a chiave.

* * *

**Servizio Tributi – Imposte - Tasse**
ubicazione: Piazza Risorgimento n. 1 – Primo Piano

I locali non sono accessibili direttamente dall'esterno.
La finestra non è dotata di grata antintrusione.

Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione e di sistema di allarme fumi.
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati e non è presente cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
chiusura porta dei locali Servizi Finanziari;
custodia archivi cartacei in armadi ignifughi chiusi a chiave.
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Servizio Contratti – Patrimonio – Commercio – Attività Economico.**
Ubicazione: Piazza Risorgimento n. 1 – Piano Terra – Ingresso lato Via Garibaldi n. 3.

I locali sono accessibili direttamente dall'esterno. Sono presenti accessi n. 2.
Le porte esterne non sono del tipo "blindato".
Le finestre sono dotate di grate antintrusione.
Le porte interne sono chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico sono chiuse a chiave.
I locali non sono protetti da sistema di allarme e non sono dotati di sistema rilevazione fumi.
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati o cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
chiusura a chiave di armadi e porte dei locali;
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Comando Polizia Locale**
Ubicazione: Via Garibaldi n. 3 – Piano Terra

I locali sono accessibili direttamente dall'esterno tramite porta non blindata.
Le finestre non sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico non possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione e sono dotati di sistema per la rilevazione dei fumi.
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati e sono presenti una cassaforte ancorata a terra e altre tre casseforti a muro.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed

ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Servizio Tecnico – LL.PP., Espropri e Manutenzioni**
**Studi, Progettazioni, Contabilità, D.L. e Collaudi OO.PP.**
**Servizio Ambiente e Protezione Civile**
Ubicazione: Via Santa Maria Nuova n. 40/A

PIANO TERRA:

I locali sono accessibili direttamente dall'esterno tramite n. 3 porte non blindate.
Le finestre non sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione e non sono dotati di sistema per la rilevazione dei fumi.
I locali non sono dotati di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati e neppure cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari non è controllato.

PIANO PRIMO:

I locali non sono accessibili direttamente dall'esterno tramite porte.
Le finestre non sono dotate di grate antintrusione.
Non tutte le porte interne possono essere chiuse a chiave.
Le porte di parte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione.
I locali non sono dotati di sistema per la rilevazione dei fumi e neppure di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati. E' invece presente una cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.

*norme comuni:*

Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità: accesso ai locali in orario extra servizio consentito solo ad autorizzati., senza l'adozione di ulteriori misure.
I Responsabili dei Servizi quali responsabili del trattamento dei dati hanno redatto l'elenco dei trattamenti ed hanno provveduto a nominare gli incaricati del trattamento dei dati.

* * *

**Servizio Urbanistica**
Ubicazione: Via Santa Maria Nuova n. 40/A

I locali sono accessibili direttamente dall'esterno tramite n. 1 porta non blindata.
Le finestre non sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Le porte di parte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.

I locali sono protetti da sistema di allarme antintrusione.
I locali non sono dotati di sistema per la rilevazione dei fumi e neppure di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati. non è presente cassaforte, viene utilizzata quella in dotazione al Settore 1° - Servizio 2°.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari non è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Servizi Sociali – Pubblica Istruzione – Sport - Spettacolo**
Ubicazione: Via G.B. Conti n. 26 – Piano terra e primo

I locali sono accessibili direttamente dall'esterno tramite n. 1 porte non blindata.
Le finestre sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Le porte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali non sono protetti da sistema di allarme antintrusione.
I locali non sono dotati di sistema per la rilevazione dei fumi e neppure di sistema anticendio/spegnimento automatico.
Non sono presenti armadi in metallo rinforzati o corazzati e neppure cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali non sono sorvegliati da telecamere.
L'accesso agli archivi contenenti dati sensibili o giudiziari non è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Sono state adottate le seguenti misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità:
accesso ai locali in orario extra servizio consentito solo ad autorizzati.

* * *

**Servizio Cultura – Biblioteca – Archivi** storici - Informagiovani
Ubicazione: Via G.B. Conti n. 30

I locali sono accessibili direttamente dall'esterno tramite una porta non blindata.
Le finestre sono dotate di grate antintrusione.
Le porte interne possono essere chiuse a chiave.
Le porte di parte dei locali adibiti ad archivio cartaceo/informatico possono essere chiuse a chiave.
I locali che custodiscono documenti di valore sono protetti da sistema di allarme antintrusione. I medesimi sono dotati di sistema per la rilevazione dei fumi.
Non sono presenti armadi in metallo rinforzati o corazzati e neppure cassaforte.
Non è presente sistema di identificazione delle persone che accedono ai locali.
I locali sono sorvegliati da una telecamera.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
Il Responsabile del Servizio quale responsabile del trattamento dei dati ha redatto l'elenco dei trattamenti ed ha provveduto a nominare gli incaricati del trattamento dei dati.
Non sono state adottate altre particolari misure fisiche/logiche per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.

# PARTE IV

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

# Descrizione delle caratteristiche tecniche delle attrezzature informatiche utilizzate da ciascun Ufficio al 1° aprile 2015

## SERVER

| Utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| Server0 | Amministratore | Server/HP | Xeon 2800 mhz | W2003 | 2 GB | SI | SI | NO | Trend Office Scan |
| Server1 | Amministratore | IBM | Xeon 5200 mhz | W2003 | 2 GB | SI | SI | NO | Trend Office Scan |
| Server2 | Amministratore | Server/HP | Xeon 2800 mhz | W2003 | 3 GB | SI | SI | NO | Trend Office Scan |
| Server3 | Amministratore | Server/HP | Xeon 2800 mhz | W2003 | 3 GB | SI | SI | NO | Trend Office Scan |
| Server4 c/o LL.PP. | Amministratore | Acer | Pentium 2 | W2003 | 1 GB | SI | SI | NO | Trend Office Scan |
| Server5 c/o LL.PP. | Amministratore | HP ML 330 | Xeon E 5603 mhz 1,6 GHZ | W2008 R2 | 8 GB | SI | SI | NO | Trend Office Scan |
| Server6 | Amministratore | Fujitsu Siemens | Xeon 5200 mhz | Linus | 1 GB | SI | NO | NO | |

**SETTORE/SERVIZIO: 1° /1°**

| Utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 79 | Carriero Roberto | HP | Dual Core 2.6 GHZ | W7 | 1gb | SI | si | si * | Trend Office Scan |
| 28 | Destro Lorena | HP | pentium 4 - 2.800 mhz | W XP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 29 | "Segreteria" | Olidata | pentiunm 3 500 mhz | W2000 SP4 | 1GB | SI | si | NO | Trend Office Scan |
| Nn | centralino | Fujitsu Siemens | pentium 4 - 1^ serie | W XP SP2 | 1GB | no | no | no | no |
| 30 | Sacchetto Gianna | HP | pentium 4 - 2.800 mhz | W 7 | 1GB | SI | SI | SI | Trend Office Scan |
| 31 | Carriero Roberto | Fujitsu Siemens | amd athlon xp 2600+ | W2000 SP4 | 512 MB | SI | SI | SI | Trend Office Scan |
| 32 | De Grandis Rosanna | Lenovo | pentium 4 | W XP SP2 | 512 MB | SI | SI | NO | Trend Office Scan |
| 33 | Segretario Generale | Olidata | pentium 3 | W XP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 49 | Toso Giorgio | HP | Dual Core 2.6 GHz | W XP SP2 | 1 GB | SI | NO | NO | Trend Office Scan |
| 50 | Portatile Assessor" | Samsung | Dual Core 2.6 GHz | W7 | 2 GB | SI | SI | NO | Trend Office Scan |
| 4645 | Buson Dante | Fujitsu Siemens | Intel Pentium Dual Core E 6600-3 | W7 | 3GB | SI | SI | SI | Trend Office Scan |
| | punto informativo | HP | Dual Core 2.6 GHz | WXP SP3 | 2GB | SI | si | S | Trend Office Scan |
| 61 | visione sito al pubblico | Lybra | pentium 3 | W XP SP2 | 512 MB | SI | SI | si | Trend Office Scan |
| 84 | Giunta Comunale (portatile) | Acer Power | pentium 4 - 2.800 mhz | W XP SP2 | 1,5 GB | SI | SI | Si | Trend Office Scan |
| 82 | Consiglio Comunale | Acer EEPC | Dual Core 2.6 GHz | XP Home | 1 GB | SI | SI | NO | Trend Office Scan |
| 29 | Piva Beatrice | Fujitsu Siemens | Pentium 4 | WXP SP3 | 512 MB | SI | SI | No | Trend Office Scan |

**SETTORE/SERVIZIO: 1° /2°**

| Utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 19 | "stampe Elettorale" + Coll.to MIN.RO | HP | Dual Core 2.6 GHz | WXP SP3 | 2 GB | SI | NO | NO | Trend Office Scan |
| 3 | "Sportello n. 1" | ECS multimedia | amd sempron 2400+ 1600 mhz | WXP SP2 | 512 MB | SI | SI | NO | Trend Office Scan |
| 2 | "Sportello n. 2" | ECS multimedia | amd sempron 2400+ 1600 mhz | WXP SP2 | 512 MB | SI | SI | NO | Trend Office Scan |
| 4 | Arzenton Paola | ECS multimedia | amd sempron 2600+ 1800 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 5 | Fusaro Carla | ECS multimedia | amd sempron 2600+ 1800 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 6 | Anagrafe 3 | ECS multimedia | amd sempron 2600+ 1800 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 7 | Veronese Anna Rosa | Fujitsu Siemens | amd athlon xp 2600+ | WXP SP2 | 1 GB | SI | SI | SI | Trend Office Scan |
| 8 | Mogentale Lino | Acer Power F1B | pentium 4 - 2800 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 9 | Buson Dante | Acer Power F1 | pentium 4 - 2800 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 2° /1°**

| Utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 24 | Rando Stefania | HP | I 3 | WXP SP3 | 3 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 2° / 2°**

| Utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 25 | Lucchiari Lorenzo | HP | dual core | WXP SP3 | 2 GB | SI | SI | SI | Trend Office Scan |
| 21 | Pasqualini Manuela | Fujitsu Siemens | Penttium 4 | WXP SP3 | 768 MB | SI | NO | NO | Trend Office Scan |
| 20 | Bazzan Gino | ASUS | I3 | W7 | 4 GB | SI | NO | NO | Trend Office Scan |
| 34 | Ferlini Marina | Fujitsu Siemens | Penttium 4 | W7 | 2 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 2° /3°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 15 | "bancone" | HP | pentium 4 - 2800 | W Vista | 1 GB | SI | si | NO | Trend Office Scan |
| 16 | Civieri Stefano | HP | I3 | W7 | 1 GB | SI | si | NO | Trend Office Scan |
| 17 | Passadore Narciso | ASUS | I3 | W7 | 1 GB | SI | SI | NO | Trend Office Scan |
| 18 | Melon Paolo | HP | I5 | W7 | 4 GB | SI | SI | SI | Trend Office Scan |
| 60 | In uso lampade votive | HP | Pentium 4 | WXP SP3 | 768 MB | SI | NO | NO | Trend Office Scan |

**SETTORE/SERVIZIO: 3° /1°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 40 | Assistente sociale | HP | I% | W8 | 3,5 GB | SI | SI | NO | Trend Office Scan |
| 41 | Laurente Cristina | HP | pentium 4 - 2.800 mhz | WXP SP3 | 1 GB | SI | SI | NO | Trend Office Scan |
| 42 | Pizzo Ester | HP | I3 | WXP SP3 | 3 GB | SI | SI | SI | Trend Office Scan |
| 43 | Responsabile | HP | I3 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |
| 67 | Assessore | Fujitsu Siemens | Penttium 4 | WXP SP3 | 768 MB | SI | SI | NO | Trend Office Scan |
|  | (asilo nido) | Fujitsu Siemens | Penttium 4 | WXP SP3 | 768 MB | SI | SI | SI | Free |

**SETTORE/SERVIZIO: 3° /2°**

| utente | nome utilizzatore | marca pc | Cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 48 | Postazione responsabile | HP | Dual Core 2.6 GHz | WXP SP3 | 2 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 4° /3°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 71 | Videosorveglianza | Fujitsu Siemens | pentium 4 - 2400 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
|  |  |  |  |  | 512 MB | SI | SI | SI | Trend Office Scan |
| 74 | Tomanin Loredana | Fujitsu Siemens | pentium 4 - 2400 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
|  | Portatile serv.energia | Packard Bell | I3 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 4° /2°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 70 | Bragioto Angelo | DELL | I5 | W7 | 3GB | SI | SI | SI | Trend Office Scan |
| 75 | === | Olidata | pentiun 4 - 1^ serie | WXP SP2 | 756 MB | SI | SI | no | Trend Office Scan |

**SETTORE/SERVIZIO: 4° /1°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | Lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 72 | Mazzocco Pietro | DELL | I5 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 4° /3°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | Lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 51 | urbanistica1 | Olidata | intel celeron 1200 mhz | W2000 SP1 | 123 MB | Si | NO | NO | Trend Office Scan |
| 12 | Gambalunga Claudio | DELL | I5 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |
| 11 | Postazione ingresso | Olidata | pentium 4 - 2880 mhz | WXP SP2 | 512 MB | SI | NO | NO | Trend Office Scan |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 14 | === | Olidata | pentium 2 mmx | W98 | 64 MB | SI | SI | NO | Trend Office Scan |
| 73 | Rigolin Mirko | Fujitsu Siemens | pentium 4 - 2400 mhz | WXP SP2 | 512 MB | SI | SI | SI | Trend Office Scan |
| 10 | Maragno Luca | Siemens Fujitsu | Dual Core - 2.4 GHz | WXP SP3 | 2GB | SI | SI | NO | Trend Office Scan |
| 38 | Assessore urbanistica-edilizia | HP | pentium 4 - 2800 mhz | WXP SP2 | 1 GB | SI | SI | SI | Trend Office Scan |

**SETTORE/SERVIZIO: 4° /4°**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 35 | Franceschetti Chiara | Siemens Fujitsu | amd athlon | WXP SP1 | 1,5 GB | SI | SI | SI | Trend Office Scan |
| 36 | Chiandotto Natalino | Siemens Fujitsu | amd athlon 2600+ 2140mhz | WXP SP1 | 1,5 GB | SI | SI | NO | Trend Office Scan |
| 37 | Gioso Graziella | Siemens Fujitsu | I3 | WXP SP3 | 512 MB | SI | SI | SI | Trend Office Scan |
| 88 | Zanardi Ortensia | Siemens Fujitsu | Intel Pentium Dual Core E6600- 3 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |
| 89 | LSU | Olidata | pentium 4 - 2880 mhz | WXP SP3 | 512 MB | SI | SI | SI | Trend Office Scan |
| 13 | Mantovani Pier Luigi | Fujitsu Siemens | i 3 | w7 | 2 GB | SI | SI | SI | Trend Office Scan |

**AREA VIGILANZA - POLIZIA LOCALE**

| utente | nome utilizzatore | marca pc | cpu | s.o. | ram | lan | internet | email | antivirus |
|---|---|---|---|---|---|---|---|---|---|
| 39 | Dallagà Natale | DELL | I5 | W7 | 3 GB | SI | SI | SI | Trend Office Scan |
| 44 | Tocchio Loretta | Acer Power | I3 | W7 | 3 GB | SI | SI | NO | Trend Office Scan |
| 47 | Cavallini Eugenio | HP | pentium 4 - 2800 mhz | WXP SP2 | 1 GB | SI | SI | NO | Trend Office Scan |
| 46 | "Ufficio1" | Acer Power | amd athlon XP 2800+ 2000 mhz | WXP SP1 | 752 MB | SI | SI | NO | Trend Office Scan |
| 61 | Cappello Chiara | HP | i 3 | W7 | 2 GB | si | SI | NO | Trend Office Scan |
| 63 | Verza Renzo | HP | Dual Core 2.6 GHz | WXP SP3 | 2 GB | SI | SI | NO | Trend Office Scan |
| 47 | Brognara Giovanna | HP | Dual Core 2.6 GHz | WXP SP3 | 2GB | SI | SI | SI | Trend Office Scan |
| | Portatile | HP | I 3 | W7 | 2 GB | SI | SI | NO | Trend Office Scan |

## CONFIGURAZIONE / PROTEZIONE APPARATI SERVER

### Descrizione

Istallazione su server del software denominato Acronis Backup & Recovery 11 Server for Windows che consente il backup e il ripristino d'emergenza basati su disco e con interfaccia utente di singoli server Windows completo di Acronis Universal Restore, modulo completamente integrato che ripristina server o workstation su hardware differenti o su macchine virtuali, fornendo opzioni altamente flessibili di disaster recovery e migrazione

Sono stati istallati – per l'accesso da e per l'esterno – apparati firewall anche sulla VPN aziendale.

E' stato implementato il sistema di filtraggio dei siti non consentiti tramite il software antivirus in dotazione (TREND MICRO, WORRY-FREE BUSINESS SECURITY-GOVERNMENT ®).

E' stato implementato un sistema di autenticazione degli accessi alla rete internet dalla LAN tramite firewall fisico su nuovo server con utilizzo di sw open source zeroshell.

E' stato istallato il servizio di filtraggio Webbloker su firewall.

Viene effettuata la tracciatura delle autenticazioni sul dominio.

# PARTE V

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

## Rilevazione dei trattamenti di dati sensibili e giudiziari eseguiti dagli Uffici in relazione alle rilevanti finalità di interesse pubblico previste dalla legge

### Elenco delle strutture e degli incaricati preposti ai trattamenti

| Struttura di riferimento | Incaricato del trattamento | Estremi dell'atto di incarico | Trattamenti operati |
|---|---|---|---|
| 1° Settore- 1° Servizio Responsabile del Trattamento: Buson Dante (decreto sindacale n. 2031 del 30.01.2015) | CARRIERO ROBERTO | Atto n. 969 del 21.06.2005 | Protocollazione dei documenti in arrivo ed in partenza e loro classificazione e smistamento. Conservazione di atti e documenti, gestione servizio archivistico. |
| | DESTRO LORENA<br><br>PIVA MARIA BEATRICE | Atto n. 969 del 21.06.2005<br><br>Atto n. 7952 del 22.04.2015 | Gestione dell'anagrafica degli amministratori. Gestione e raccolta di originali di determinazioni e deliberazioni dell'amministrazione comunale.<br>Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il comune. Gestione stipendi, gestione del conto annuale del personale, gestione dati relativi alla compilazione del mod. 770, gestione fascicoli personali dei dipendenti. Gestione dati INPDAP. |
| | TOSO GIORGIO | Atto n. 969 del 21.06.2005 | Pubblicazione degli atti presso l'albo pretorio. Notifica e trasmissione di atti e provvedimenti destinati ad uffici comunali o dagli stessi provenienti. Notifica di atti dell'amministrazione, dello stato e di altri enti pubblici.<br>Gestione e trattamento dati personali dipendenti, accesso ai fascicoli personali. |
| | DE GRANDIS ROSANNA | Atto n. 969 del 21.06.2005 | Pubblicazione degli atti presso l'albo pretorio. Notifica e trasmissione di atti e provvedimenti destinati ad uffici comunali o dagli stessi provenienti. Notifica di atti dell'amministrazione, dello stato e di altri enti pubblici.<br>Protocollazione dei documenti in arrivo ed in partenza e loro classificazione e smistamento. Accesso fascicoli personali, gestione e trattamento dati personale dipendente. Gestione dell'anagrafico degli amministratori. Gestione e raccolta di originali di determinazioni e deliberazioni dell'amministrazione comunale. |
| **Struttura di riferimento** | **Incaricato del trattamento** | **Estremi dell'atto di incarico** | **Trattamenti operati** |
| 1° Settore- 2° Servizio Responsabile del Trattamento: Dante Buson (decreto sindacale n. 2031 del 30.01.2015) | VERONESE ANNA ROSA<br>ARZENTON PAOLA | Atto n. 1017 del 27/06/2005 | Trattamento dei dati identificativi e personali per le finalità istituzionali del comune. Trattamento dei dati sensibili e giudiziari inerenti alle seguenti tipologie: aggiornamento dell'anagrafe dei pensionati; tenuta dell'anagrafe dei cittadini stranieri; dichiarazione di volontà di chi o nell'interesse di chi non può sottoscrivere.; matrimoni con rito cattolico; matrimoni con rito acattolico; pubblicità dello stato di interdizione ed inabilitazione; cremazione di salme o di resti mortali; sottoscrizione delle liste dei candidati dei quesiti referendari; votazione presso i luoghi di cura; aggiornamento liste elettorali; sostituzione scrutatori impediti all'ufficio; esercizio del diritto di voto da |

| | | | |
|---|---|---|---|
| | | | elettori affetti da gravi infermità.<br>Aggiornamento ruoli matricolari. Collaborazione a domande di ammissione di servizio civile nazionale. |
| | FUSARO CARLA<br>MOGENTALE LINO | Atto n. 1017 del 27/06/2005 | Trattamento dei dati identificativi e personali per le finalità istituzionali del comune. Trattamento dei dati sensibili e giudiziari inerenti alle seguenti tipologie: aggiornamento dell'anagrafe dei pensionati; tenuta dell'anagrafe dei cittadini stranieri; dichiarazione di volontà di chi o nell'interesse di chi non può sottoscrivere.; matrimoni con rito cattolico; matrimoni con rito acattolico; pubblicità dello stato di interdizione ed inabilitazione; cremazione di salme o di resti mortali; sottoscrizione delle liste dei candidati dei quesiti referendari; votazione presso i luoghi di cura; aggiornamento liste elettorali; sostituzione scrutatori impediti all'ufficio; esercizio del diritto di voto da elettori affetti da gravi infermità.<br>Aggiornamento ruoli matricolari. Collaborazione a domande di ammissione di servizio civile nazionale.<br>Attività relativa allo sportello QUI ENEL (con accesso alla banca dati di Enel Distribuzione S.p.a.) |
| **Struttura di riferimento** | **Incaricato del trattamento** | **Estremi dell'atto di incarico** | **Trattamenti operati** |
| 2° Settore- 2° Servizio Responsabile del Trattamento: Rag. Lucchiari Lorenzo (decreto sindacale n. 2023 del 30.01.2015) | ------- | ------- | Gestione archivio fatture attive e passive. Gestione pagamenti postali e bancari. |
| | BAZZAN GINO<br>PASQUALINI MANUELA | Atto n. 949 del 16.06.2005 | Gestione archivio creditori/debitori. Gestione archivio fatture attive e passive. Obblighi di certificazioni e di adempimenti fiscali. |
| 2° Settore- 3° Servizio Responsabile del Trattamento: Dott. Paolo Melon (decreto sindacale n. 2026 del 30.01.2015) | PASSADORE NARCISO | Atto n. 948 del 16.06.2005 | Gestione T.I.A. (Tariffa Igiene Ambientale) residui anno 2007. Gestione I.C.I. (Imposta Comunale sugli Immobili): determinazione soggetti passivi ed importi dovuti e relativi controlli. Gestione relazioni con l'utenza allo sportello. Gestione dati su archivio Tassa Smaltimento Rifiuti. Gestione dati su bollettari Imposta Comunale sugli Immobili.<br>Gestione TARI legge n. 147/2013. |
| | CIVIERI STEFANO | Atto n. 948 del 16.06.2005 | Gestione versamenti ICI e relativi controlli. Gestione Gestione C.O.S.A.P. permanente: determinazione soggetti passivi ed importi dovuti e relativi controlli. Gestione flussi informativi sanzioni amministrative per violazioni del C.d.S.<br>Gestione TARI legge n. 147/2013. |

| Struttura di riferimento | Incaricato del trattamento | Estremi dell'atto di incarico | Trattamenti operati |
|---|---|---|---|
| 3° Settore- 1° Servizio Responsabile del Trattamento: Rag. Sacchetto Gianna (decreto sindacale n. 2030 del 30.01.2015) | PIZZO ESTER | Atto n. 956 del 16.06.2005 | Gestione servizio minori, asilo nido e animazione estiva. Fondo sostegno locazione. Assegnazione alloggi ERP. Assegno maternità e nucleo familiare numeroso. Integrazione rette, tutele e curatele. Segretariato Sociale. Erogazione contributi economici (anche con accesso alla banca dati INPS). Servizio domiciliare. Servizio pasti caldi. Telesoccorso. Trasporto disabili e bisognosi. Assistenza domiciliare. Soggiorni climatici terza età. Gestione alloggi ERP (anche con accesso alle banche dati INPS). Accesso alle banche dati SIATEL. Informaimmigrati. Rilascio esenzioni ticket farmaceutici. Rilascio attestazione ISEE. Contributo regionale "Badanti". Legge Regionale 28/1991. Assegni di sollievo. Contributi comunali iniziative sostegno famiglia. Attività relativa ad erogazione contributi acquisto libri di testo e borse di studio. |
| | PIVA MARIA BEATRICE | Atto n. 7777 del 20.04.2015 | |
| | LAURENTE CRISTINA | Atto n. 956 del 16.06.2005 | Gestione servizio asilo nido e animazione estiva. fondo sostegno locazione. Assegnazione alloggi ERP. Assegno maternità e nucleo familiare numeroso. Segretariato Sociale. erogazione contributi economici. Servizio domiciliare. Servizio pasti caldi. Telesoccorso. Trasporto disabili e bisognosi. Assistenza domiciliare. Soggiorni climatici terza età. Contributo regionale "Badanti". Contributi comunali iniziative sostegno famiglia. Gestione nominativi scuole materne ed elementari. Utenti servizio mensa scolastica e scuolabus. Attività relativa ad erogazione contributi acquisto libri di testo e borse di studio. |
| | VICENTINI CARLOTTA | Atto n. 6336 del 30.03.2012 | Gestione minori (con ASL 18). Integrazione rette, tutele e curatele. Segretariato sociale. Erogazione contributi economici. Servizio domiciliare. Servizio pasti caldi. Telesoccorso. Trasporto disabili e bisognosi. Assistenza domiciliare. Soggiorni climatici terza età. Informaimmigrati. Legge Regionale 28/1991. Legge Regionale 5/2001. Assegni di sollievo. |
| 3° Settore- 2° Servizio Responsabile del Trattamento: Dott. Palumbo Alfredo (decreto sindacale n. 2197 del 03.02.2015) | BATTIZOCCO ALESSANDRA | Atto n. 933 del 15.06.2005 | Archivi con dati dei lettori della Biblioteca. |
| | VIARO LAURA | Atto n. … del (in corso di aggiornamento) | |
| **Struttura di riferimento** | **Incaricato del trattamento** | **Estremi dell'atto di incarico** | **Trattamenti operati** |
| 4° Settore- IV° Servizio Responsabile | FRANCESCHETTI CHIARA | Atto n. 929 del 14.06.2005 | Attività relativa alla gestione dei contratti per la concessione di loculi e tombe di famiglia. Attività relativa alla gestione dei contratti per l'incasso dei ° Settore- 1° Servizio Responsabile del Trattamento: |

| | | | |
|---|---|---|---|
| | | | Geom. Angelo Bragioto (Atto n. 13386 del 13.06.2005) Canoni relativi alle lampade votive. Attività di ricerca di familiari dei defunti sepolti nei cimiteri del territorio comunale. Attività relativa alla progettazione e realizzazione di OO.PP. (Professionisti, Titolari di Imprese). |
| Coordinatore IV° Settore Servizio Responsabile del Trattamento: Geom. Angelo Bragioto (decreto sindacale n. 2025 del 30.01.2015) | RIGOLIN MIRKO | Atto n. 992 del 22.06.2005 | Attività di rilascio autorizzazioni varie in materia di ambiente. Attività relativa al rilascio di autorizzazioni varie in materia di fognatura, acquedotto, depurazione, scavi su suolo pubblico, deroga ai rumori. Attività relativa alla sorveglianza e vigilanza nella fase di monitoraggio periodico del territorio per la verifica dello stato dei fossi pubblici comunali, provati e consorziali. Attività indiretta relativa al servizio di nettezza urbana, raccolta differenziata, ecocentro, rilascio di autorizzazioni per l'utilizzo del servizio di ecocentro. Attività di sorveglianza e vigilanza in materia igienico sanitaria ed ambientale. |
| | TOMANIN LOREDANA | Atto n. 992 del 22.06.2005 | Attività relativa al rilascio di autorizzazioni varie in materia di fognatura, acquedotto, depurazione, scavi su suolo pubblico, deroga ai rumori. Attività indiretta relativa al servizio di nettezza urbana, raccolta differenziata, ecocentro, rilascio di autorizzazioni per l'utilizzo del servizio fornito tramite ecocentro. Attività relativa alla progettazione e realizzazione di OO.PP. (Professionisti, Titolari di Impresa). |
| Franceschetti Chiara 4° Settore- IV° Servizio Responsabile | MANTOVANI PIERLUIGI<br><br>GIOSO GRAZIELLA | Atto n. 997 del 23.06.2005<br><br>Atto n. 6723 del 10.04.2014 | Attività relativa alla gestione dei contratti per la cessione di loculi e tombe di famiglia. Attività relativa alla gestione dei contratti per l'incasso dei canoni relativi alle lampade votive. Attività di ricerca dei familiari dei defunti sepolti nei cimiteri del territorio comunale. |
| **Struttura di riferimento** | **Incaricato del trattamento** | **Estremi dell'atto di incarico** | **Trattamenti operati** |
| 4° Settore- 3 Servizio Responsabile del Trattamento: Geom. Claudio Gambalunga (decreto sindacale n. 2024 del 30.01.2015) | MARAGNO LUCA | Atto n. 991 del 22.06.2005 | Trattamento dei dati legati all'espletamento dell'attività relativa: all'edilizia privata; all'urbanistica, al condono edilizio; allo S.U.A.P., agli abusi edilizi. |
| Franceschetti Chiara I° Settore- 4° Servizio Responsabile (decreto sindacale n. 2051 del 30.01.2015 | CHIANDOTTO NATALINO | Atto n. 929 del 14.06.2005 | Raccolta comunicazioni ospitalità stranieri. Denuncie di infortunio sul lavoro. Accertamenti e trattamenti sanitari obbligatori. Rilascio licenze di commercio ed autorizzazioni sanitarie e gestione dei relativi archivi anagrafici. Rilascio licenza di P.S. (pubblici esercizi, spettacoli viaggianti, agenzie d'affari). Rilascio autorizzazioni per esercizio di attività extra-alberghiera. Rilascio licenze di noleggio con conducente, di taxi e di attribuzione di matricole per ascensori. Ricevimento istanze rilascio passaporto e licenza di pesca. |
| | FRANCESCHETTI | Atto n. 929 del | Denuncie di infortunio sul lavoro. Accertamenti e |

| | | | |
|---|---|---|---|
| | CHIARA<br><br>GIOSO GRAZIELLA<br><br><br>ZANARDI ORTENSIA | 14.06.2005<br><br>Atto n. 6723 del 10.04.2014<br><br>Atto n. 6722 del 20.04.2014 | trattamenti sanitari obbligatori. Rilascio licenze di commercio ed autorizzazioni sanitarie e gestione dei relativi archivi anagrafici. Rilascio licenza di P.S. (pubblici esercizi, spettacoli viaggianti, agenzie d'affari). Rilascio autorizzazioni per esercizio di atti-vità extra-alberghiera. Rilascio licenze di noleggio con conducente, di taxi e di attribuzione di matricole per ascensori. Tenuta dei repertori degli appalti. Predisposizione dei contratti d'appalto delle convenzioni e di altri contratti (locazioni attive e passive, concessioni). Stipula, registrazione e conservazione contratti. |
| **Struttura di riferimento** | **Incaricato del trattamento** | **Estremi dell'atto di incarico** | **Trattamenti operati** |
| Area Vigilanza<br>Corpo Polizia Locale<br>Com. Natale Dallagà (decreto sindacale n. 2029 del 30.01.2015) | VERZA RENZO<br>STOCCO GIULIANO<br>CAVALLINI EUGENIO<br>CAPPELLO CHIARA<br>RAIMONDI DAVIDE<br>TOCCHIO LORETTA<br><br>STELLA DANIELE<br>AVANZO LUCA | Atto n. 943 del 15.06.2005<br><br><br><br><br>Atto n. del (in corso di aggiornamento) | Gestione dati relativi a: procedure sanzionatorie, notifica atti giudiziari, accertamenti anagrafici, avvio/cessazioni attività commerciali/artigianali, autenticazione firme a domicilio, trattamenti sanitari obbligatori, attività di polizia amministrativa, vigilanza edilizia, ambientale, igiene e sanità, attività di polizia giudiziaria, annonaria, commerciale ed amministrativa, attività relativa a fiere e mercati, infortunistica stradale, censimento campi nomadi. |
| | BROGNARA GIOVANNA<br><br>ZERBETTO SERGIO | Atto n. 943 del 15.06.2005<br><br>Atto n. del (in corso di aggiornamento) | Gestione dati relativi: procedure sanzionatorie, rilascio autorizzazioni amministrative, rilascio permessi alla sosta invalidi. |

| Sett. | Ufficio che effettua il trattamento | Descrizione Sintetica del trattamento | Natura del trattamento | Natura dei dati* | Categoria di interessati | | Altre strutture (anche esterne) che concorrono al trattamento |
|---|---|---|---|---|---|---|---|
| | | | | S | G | | |
| 1 | Ufficio Segreteria | Gestione dell'anagrafico degli amministratori. Gestione e raccolta di originali di determinazioni e deliberazioni dell'amministrazione comunale. | Cartaceo/ Informatico | 3, 4 | 6, 7 | Amministratori Comunali, Dipendenti, Cittadini residenti e non residenti, Enti Pubblici | Altri uffici del Comune, Prefettura -UTG |
| 1 | Ufficio Personale | Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune e attività relativa al riconoscimento di benefici connessi all'invalidità civile per i dipendenti. Gestione pratiche pensione e Mod. PA04. Attività relative alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai CCL . Gestione Stipendi. Gestione conto annuale del Personale. Gestione dati relativi alla compilazione del modello 770. | Cartaceo/ Informatico | 2, 3, 4, 5 | 6, 7 | Dipendenti ed ex dipendenti dell'amministrazione | Altri uffici del Comune. Provincia di Rovigo – Centro per l'Impiego, OO.SS., Enti assistenziali e previdenziali, Enti assicurativi, Ministero delle Entrate, Uffici Giudiziari, Prefettura –UTG. Medico incaricato ai sensi d.lgs. n. 81/2008. |
| 1 | Ufficio Protocollo / Archivio | Protocollazione dei documenti in arrivo ed in partenza e loro classificazione e smistamento. Conservazione di atti e documenti, organizzazione del servizio archivistico. | Cartaceo/ Informatico | 1, 2, 3, 4, 5 | 6, 7 | Cittadini residenti, utenti vari, dipendenti dell'Ente, Enti Pubblici | Tutti altri uffici del Comune |
| 1 | Ufficio Messi Comunali | Pubblicazione degli atti presso l'albo pretorio. Notifica e trasmissione di atti e provvedimenti destinati agli uffici comunali o dagli stessi provenienti. Notifica di atti dell'amministrazione, dello stato e di altri enti pubblici. | Cartaceo/ Informatico | 2, 5 | 6, 7 | Cittadini residenti | Uffici del Comune e di altri Comuni. Enti Pubblici vari. |
| 1 | Ufficio AA.GG., Legali e Contenzioso | Gestione dati relativi all'attività di rappresentanza e difesa dell'Ente, a denunce penali e querele. Conferimento di incarico a legali. Tenuta archivio contenzioso. | Cartaceo/ Informatico | 3, 4, 5 | 6, 7 | Cittadini residenti e non residenti, Enti vari, Enti Pubblici. | Uffici del Comune. Autorità Giudiziaria, Studi Legali. |

| Set. | Ufficio che effettua il trattamento | Descrizione Sintetica del trattamento | Natura del trattamento | Natura dei dati* | Categoria di interessati | | Altre strutture (anche esterne) che concorrono al trattamento |
|---|---|---|---|---|---|---|---|
| 1 | Servizi Demografici | Gestione dell'Anagrafe e della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE). Gestione degli atti e dei registri dello stato civile. tenuta delle liste elettorali e gestione delle consultazioni elettorali. gestione degli Albi degli scrutatori e dei presidenti di seggio. Gestione dell'elenco dei giudici popolari. Tenuta degli archivi di leva e dei ruoli matricolari e del servizio sostitutivo civile. Gestione dell'attività di polizia mortuaria. Raccolta firme per proposte di referendum. | Cartaceo/ Informatico | 1, 2, 3, 4, 5 | 6, 7 | Cittadini residenti e non residenti | Uffici del Comune e di altri Comuni, Procure della Repubblica, Questure, Forze dell'Ordine, INPS, Ministero del Tesoro, Ministero dell'Interno, Tribunali, USL-ASL, Prefettura-UTG, MTCC, Commissioni Elettorali, Corte d'Appello, Enti Pubblici.. Distretti Militari e Ministero del Welfare. |
| 1 | Ufficio AA.GG. Politiche Organizzazione Informatizzazione | Organizzazione e sviluppo del sistema informativo dell'Ente tramite il collegamento ed il coordinamento delle attività dei diversi Settori. Formulazione proposte di innovazione e adeguamento dei processi e dei sistemi informativi ed informatici. Adempimenti relativi all'aggiornamento del DPS. Gestione Sportello QUI ENEL (con accesso a banca dati ENEL) | Cartaceo/ Informatico | 1, 2, 3, 5 | 6, 7 | Dipendenti dell'Ente impiegati in vari Uffici | Uffici del Comune , Ditte incaricate alla manutenzione dell'hardware e del software. ENEL Distribuzione S.p.a. |
| **Sett.** | **Ufficio che effettua il trattamento** | **Descrizione Sintetica del trattamento** | **Natura del trattamento** | **Natura dei dati*** | **Categoria di interessati** | | **Altre strutture (anche esterne) che concorrono al trattamento** |
| 2 | Curatore Sistema Informatico | Amministrazione del sistema informatico. Controllo della rete informatica di comunicazione tra i computers in dotazione ai diversi Uffici ed i sistemi di memorizzazione centrale, delle procedure | Cartaceo/ Informatico | 1, 2, 3, 4, 5 | 6, 7 | Dipendenti dell'Ente impiegati in vari Uffici | Uffici del Comune , Ditte incaricate alla manutenzione dell'hardware e del software |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | di backup e di sicurezza degli accessi. Assistenza operativa a tutti gli uffici dell'Ente. Manutenzione software di alcune procedure di proprietà dell'Ente e gestione del software acquistato da terzi. Adempimenti relativi al DPS. | | | | | |
| 2 | Ufficio Tributi | Gestione T.I.A., Gestione C.O.S.A.P, Gestione I.C.I.; Archivio ruoli T.A.R.S.U. Attività di accertamento tributi locali; gestione contenzioso tributario. | Cartaceo/ Informatico | | 6,7 | Cittadini residenti e non residenti, Difensori controparte | Altri Uffici del Comune. Poste Italiane S.p.a. (temporaneo) |
| 2 | Ufficio Economato | Gestione archivio fatture attive e passive. Gestione pagamenti postali e bancari. | Cartaceo/ Informatico | | 6,7 | Cittadini residenti e non residenti. Ditte e società commerciali. | Uffici del Comune, Poste Italiane S.p.a., Istituti bancari vari. |
| 2 | Ufficio Ragioneria | Gestione archivio creditori/debitori. Obblighi di certificazioni e adempimenti fiscali. Gestione archivio fatture attive e passive. | Cartaceo/ Informatico | | | Ditte e società commerciali. | Uffici del Comune, Poste Italiane S.p.a., Istituti bancari vari., Tesoreria Comunale |
| **Sett.** | **Ufficio che effettua il trattamento** | **Descrizione Sintetica del trattamento** | **Natura del trattamento** | **Natura dei dati*** | **Categoria di interessati** | | **Altre strutture (anche esterne) che concorrono al trattamento** |
| 3 | Ufficio Servizi Sociali | Gestione servizio: minori, asilo nido, animazione estiva. Fondo sostegno locazioni. Assegnazione alloggi edilizia popolare(anche con accesso alla banca dati INPS). Assegno maternità e nucleo familiare numeroso. Integrazione rette. tutele e curatele. Segretariato sociale. Erogazione contributi economici (anche con accesso alla banca dati INPS); servizio domiciliare. Servizio pasti caldi. Telesoccorso. Trasporto disabili e bisognosi. Assistenza domiciliare. Esenzione tickets farmaceutici. Gestione contribuiti regionali per le badanti. | Cartaceo/ Informatico | 1, 2, 3, 4, 5 | 6, 7 | Cittadini residenti e non residenti. | Uffici Giudiziari (Tribunale minorile e ordinario), Comunità di accoglienza, ASL, Questure e Forze dell'ordine, Istituti scolastici, Cooperative di assistenza, Centri Caritas, Casa Albergo per Anziani di Lendinara, Cooperative di Servizi. Ditte. ATER Rovigo. Regione Veneto. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Pratiche relative alla L. 28/91 e alla L. 5/2001. Soggiorni climatici. Informa-immigrati. Abbattimento barriere architettoniche (su edifici privati). Rilascio attestazione ISEE. Accesso banca dati servizio SIATEL. | | | | | |
| 3 | Ufficio Scuola, Sport, Attività Promozionali | Raccolta nominativi iscritti Scuole Materne ed Elementari e utenti servizi mensa e scuolabus. Attività relativa ad erogazione contributi per acquisto libri di testo e borse di studio. Attività Promozionali. Attività sportive e del tempo libero. | Cartaceo/ Informatico | 2, 5 | 6, 7 | Cittadini residenti e non residenti. | Uffici del Comune, Uffici di altri Comuni, Scuole statali e non statali. Regione Veneto. |
| 3 | Biblioteca | Elenchi relativi ai soggetti destinatari di prestito di libri e/o riviste | Informatico | 2, 3, 4 | | Cittadini residenti e non residenti accreditati all'utilizzo dei servizi bibliotecari | |
| **Sett.** | **Ufficio che effettua il trattamento** | **Descrizione Sintetica del trattamento** | **Natura del trattamento** | **Natura dei dati*** | **Categoria di interessati** | | **Altre strutture (anche esterne) che concorrono al trattamento** |
| 4 | Commercio e Pubblica Sicurezza | Raccolta comunicazioni ospitalità stranieri. Denunce di infortunio sul lavoro.. Accertamenti e trattamenti sanitari obbligatori. Rilascio licenze di commercio ed autorizzazioni sanitarie e gestione dei relativi archivi anagrafici. Rilascio licenze di P.S. (pubblici esercizi, spettacoli viaggianti, agenzie d'affari). Rilascio autorizzazioni per esercizio di attività extra-alberghiera. Rilascio licenze di noleggio con conducente, di taxi e di attribuzione di matricole per ascensori. Ricevimento istanze rilascio passaporto e licenza di pesca. | Cartaceo/ Informatico | 1, 5 | 6,7 | Cittadini residenti e non residenti, Enti Pubblici, Uffici del Comune | Ufficio Anagrafe, Polizia Locale, Uffici di altri Comuni, Prefettura-UTG, Questura, Procura della Repubblica, CCIAA, ASL, Regione Veneto, Ministero delle Finanze, Forze dell'Ordine |
| 4 | Contratti e Patrimonio | Tenuta repertori degli appalti. Predisposizione dei contratti d'appalto, delle convenzioni e di altri contratti (locazioni attive e passive, | Cartaceo/ Informatico | | 6,7 | Imprese e Ditte appaltatrici. Amministratori e Dipendenti Comunali. Enti Pubblici. Banche . | Altri Uffici del Comune, Uffici del Registro e Conservatoria dei Registri Immobiliari. Amministrazioni dello Stato |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | concessioni). Stipula, registrazione e conservazione contratti. | | | | | |
| 4 | Ufficio Urbanistica | Espletamento attività relativa all'edilizia privata e all'urbanistica. Condono Edilizio. Gestione Sportello Unico per le attività produttive. Espletamento attività inerente l'abusivismo edilizio. | Cartaceo/ Informatico | 5 | 6, 7 | Cittadini residenti e non residenti, Imprese edili, Liberi Professionisti, | Uffici del Comune e di altri Comuni. Soprintendenza BB.AA. e Storica, Studi Notarili, Regione Veneto, Provincia di Rovigo, Agenzia del Territorio, Vigili del Fuoco, ASL 18, ARPAV, Operatori tecnici e privati. |
| **Sett.** | **Ufficio che effettua il trattamento** | **Descrizione Sintetica del trattamento** | **Natura del trattamento** | **Natura dei dati*** | **Categoria di interessati** | | **Altre strutture (anche esterne) che concorrono al trattamento** |
| 4 | Ufficio Manutenzioni ed Espropri | Redazione piano particellare. Espropri. Gestione del servizio strade, stabili ed impianti elettrici. Appalti e progettazione OO.PP. | Cartaceo/ Informatico | | 6, 7 | Cittadini residenti e non residenti. Imprese edili, Liberi Professionisti, Ditte per forniture e manutenzioni | Uffici vari del Comune, Regione Veneto, Provincia di Rovigo, ANAS, Veneto Strade, Cassa depositi e prestiti, Operatori tecnici, ditte, privati, Enel, Telecom Italia, Eni Italgas, Polesine Servizi, Soprintendenza BB.AA., Vigili del Fuoco, Prefettura-UTG |
| 4 | Ufficio Tutela Ambiente, Ecologia e Protezione Civile | Gestione indiretta del servizio fognatura comunale e depurazione (acque bianche e nere), nettezza urbana, verde pubblico. Tutela Ambientale. | Cartaceo/ Informatico | 5 | 6, 7 | Cittadini residenti e non residenti. Imprese edili, Liberi Professionisti, Ditte per forniture e manutenzioni | Uffici del Comune, ASL 18, ARPAV, Regione Veneto, Provincia di Rovigo |
| 4 | Ufficio Studi, Progettazioni, Contabilità, D.L. e Collaudi OO.PP. | Appalti e progettazione OO.PP.<br>Procedura AliProg4 (pubblicità degli appalti) | Cartaceo/ Informatico<br>informatico | | 6, 7<br>6, | Cittadini residenti e non residenti. Imprese edili, Liberi Professionisti, Imprese, Società | Uffici Vari del Comune, Regione Veneto, Provincia di Rovigo, Cassa depositi e prestiti, Operatori tecnici, ditte, privati, Enel, Telecom Italia, Eni Italgas, Polesine Servizi, Soprintendenza BB.AA., Vigili del Fuoco, Prefettura-UTG, ASL Ministero delle Infrastrutture |
| **Sett.** | **Ufficio che effettua il trattamento** | **Descrizione Sintetica del trattamento** | **Natura del trattamento** | **Natura dei dati*** | **Categoria di interessati** | | **Altre strutture (anche esterne) che concorrono al trattamento** |
| 4 | Ufficio LL.PP., Servizi Cimiteriali | Appalti e progettazione OO.PP. Gestione contrattuale e pagamenti loculi e lampade votive. | Cartaceo/ Informatico | 2, 4 | 6,7 | Cittadini residenti e non residenti. Imprese edili, Liberi Professionisti, | Uffici vari del Comune, Imprese di Servizi Funebri. |
| Are | Comando Polizia | Notifica atti giudiziari. | Cartaceo/ | 1, 5 | 6, 7 | Cittadini residenti e | Altri Uffici del Comune, |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| a Vig .za | Locale | Accertamenti per iscrizioni e cancellazioni anagrafiche e avvio o cessazione attività commerciali /artigianali. Autenticazione firme a domicilio nei casi previsti dalla normativa. Attività relative al T.S.O. (trattamento sanitario obbligatorio) ed al rilascio permessi ad invalidi. Attività di polizia amministrativa, di vigilanza edilizia e di intervento per ripristino stato dei luoghi dell'ambiente e dell'igiene e sanità. Attività di polizia giudiziaria, annonaria, commerciale ed amministrativa. attività relativa a fiere e mercati. Attività di gestione dei dati relativi alle procedure sanzionatorie ed alla rilevazione dell'infortunistica stradale. Censimento campi nomadi. | Informatico | | | non residenti. | Uffici di altri Comuni, MTCC, ASL, Prefettura - UTG, Procure della Repubblica e Autorità Giudiziaria, Forze dell'Ordine. |
| | * legenda | 1. dati personali idonei a rivelare l'origine razziale ed etnica<br>2. dati personali idonei a rilevare le convinzioni religiose, filosofiche o di altro genere<br>3. dati personali idonei a rivelare le opinioni politiche, l'adesione a partiti e sindacati<br>4. dati personali idonei a rivelare l'adesione ad associazioni o organizzazioni a carattere religioso,filosofico, politico, sindacale<br>5. dati personali idonei a rivelare lo stato di salute o la vita sessuale<br>6. dati personali idonei a rivelare provvedimenti di cui all'art. 3, c.1 lettere da a) a o) e da r) a u) del D.P.R. 14.11.2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dai relativi carichi pendenti<br>7. dati personali idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p. | | | | | |

# PARTE VI

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

# Criteri tecnici ed organizzativi in ordine alla protezione degli ambienti e degli archivi circa la riservatezza dei dati personali e analisi dei rischi.

## A) Criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi

### 1. Protezione delle aree e dei locali interessati

1.1. Le macchine server vanno collocate in un apposito locale (sala server).
1.2. La sala server deve essere dotata di:
*a)* Impianto antincendio adeguato a locali contenenti apparati informatici;
*b)* Impianto di condizionamento ambientale, opportunamente dimensionato;
*c)* Porte e finestre blindate;
*d)* Impianto elettrico a norma;
*e)* Gruppo di continuità.
1.3. L'accesso alla sala server è consentito solo al responsabile del trattamento, o alle persone espressamente autorizzate.
1.4. In assenza del personale autorizzato, la sala server deve essere tenuta chiusa a chiave.
1.5. I supporti di backup vanno tenuti in armadi blindati, posti in locali distanti dalla sala server, non trasportabili e dotati di impianto antifurto.
1.6. Tutte le chiavi vanno custodite da personale delegato dal Responsabile del Servizio.
1.7. Tutte le risorse necessarie per l'attuazione di quanto previsto in questa sezione sono individuate dal Responsabile del Servizio, con l'intervento, ove necessario, di altri funzionari autorizzati da norma di legge o di Regolamento.

### 2. Gestione degli apparati di rete

2.1. Gli armadi che contengono gli apparati di rete vanno tenuti chiusi a chiave. Le chiavi vanno custodite secondo le stesse procedure previste al punto 1.7.
2.2. Le porte telematiche degli apparati di rete che non siano utilizzate devono essere disabilitate tramite il software di gestione.
2.3. Laddove gli apparati di rete vengano gestiti attraverso la rete locale dell'edificio, il loro indirizzamento deve avvenire su una rete IP distinta.

## B) Criteri e le procedure per assicurare l'integrità dei dati.

### 3. Sicurezza del software

3.1. Presso ciascun Ufficio è consentita l'installazione esclusiva delle seguenti tre categorie di software:
*a)* Software commerciale, dotato di licenza d'uso;
*b)* Software realizzato specificamente per gli Enti Locali in genere;
*c)* Software realizzato specificamente per il Comune di Lendinara.
3.2. L'installazione di software va autorizzato dal Responsabile del trattamento.
3.3. Il software deve essere installato solo da supporti fisici originali o dei quali sia nota la provenienza.
3.4. Tramite **l'Amministratore di sistema** si provvede alla distribuzione di un software antivirus aggiornato su tutta la rete aziendale.
3.5. In mancanza di procedure di installazione automatiche, il Responsabile del trattamento garantisce l'effettuazione delle installazioni del software antivirus su tutte le postazioni di lavoro, con continuo aggiornamento degli stessi.

### 4. Integrità dei dati

4.1. Il Responsabile di Servizio, con la collaborazione dell'Amministratore di sistema, mantiene un elenco, da aggiornare con cadenza almeno semestrale, di tutte le attrezzature informatiche dell'ufficio, dello scopo cui sono destinate, della loro locazione fisica, delle misure di sicurezza su esse adottate e delle eventuali misure di adeguamento pianificate.
4.2. Il Responsabile del trattamento individua i volumi logici o le aree di disco da sottoporre a backup, sul server.
4.3. A ciascun utente viene assegnata una directory, in un'area disco di un server che sia sottoposta a backup, dove mantenere i dati che debbono essere mantenuti in maniera sicura. L'accesso a queste directory è consentita esclusivamente all'utente proprietario, nonché agli incaricati del backup.
4.4. L'Amministratore di sistema provvede al backup delle basi-dati.

4.5. Laddove il backup venga effettuato localmente nell'ambito dell'ufficio, gli incaricati effettuano le seguenti operazioni:

*a)* Esecuzione quotidiana del backup, eventualmente attraverso procedure automatiche;
*b)* Verifica almeno settimanale della corretta esecuzione dei backup;
*c)* Mantenimento di un elenco dei backup effettuati;
*d)* Archiviazione dei supporti secondo le disposizione della sezione A) 1.6;
*e)* Verifica, con cadenza almeno mensile, della procedura di recovery dai supporti di backup;
*f)* Effettivo ripristino dei dati in caso di necessità.

**5. Sistema di monitoraggio**

5.1. Deve essere messo in atto un processo di controllo e verifica della sicurezza del sistema informatico, attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicazioni.

5.2. Il sistema di controllo deve registrare:

*a)* Gli accessi, riusciti e falliti, a livello di sistema, di base dati e di applicativo;
*b)* Gli accessi in lettura e scrittura effettuati attraverso il sistema di gestione delle basi dati;
*c)* Tutti gli accessi in lettura e scrittura ai singoli archivi.

5.3. L'Amministratore di sistema ha il compito di verificare le registrazioni di cui al precedente comma.

5.4. Le operazioni di verifica delle registrazioni debbono essere effettuate almeno mensilmente. I problemi riscontrati vanno riportati al Responsabile del Servizio/trattamento, individuerà le opportune contromisure.

5.5. L'individuazione delle responsabilità connesse a modifiche o letture non autorizzate viene effettuata, sulla registrazione di cui alla lettera 5.2.c), su richiesta del Responsabile di Servizio/trattamento.

**C) Criteri e procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica.**

**6. Controllo degli accessi**

6.1. Tutte le stazioni di lavoro debbono essere protette da una password di accensione.

6.2. L'inserimento della password di accensione va effettuato a cura dell'utente, affidandone una copia, in busta chiusa, al responsabile del trattamento, che le custodirà sotto chiave.

6.3. Ai fini dell'assistenza sistemistica, la password di accensione può venire comunicata agli incaricati, e sostituita al termine dell'intervento.

6.4. La password di accensione va modificata con cadenza annuale.

6.5. L'accesso alla rete di sistema va protetto tramite un nome utente e una password.

6.6. Il Responsabile del Servizio/trattamento verifica che gli addetti (utenti/incaricati) cambino la password periodicamente con una frequenza non superiore a 6 (sei) mesi. Le stesse dovranno essere modificate al massimo ogni tre mesi nel caso di trattamento di dati sensibili e/o giudiziari. Il Responsabile deve altresì verificare che gli addetti di cui sopra custodiscano le parole chiave per l'accesso al sistema informatico e consegna agli stessi una copia del Manuale per la sicurezza.

6.7. Dove questo è tecnicamente possibile, l'Amministratore di sistema imposta il sistema in modo di non poter utilizzare lo stesso nome utente per accedere contemporaneamente al sistema da due postazioni di lavoro distinte.

6.8. La password di accesso alla rete:

*a)* Non deve derivare dal nome utente o dai dati personali dell'utente;
*b)* Deve avere una lunghezza di almeno otto caratteri alfanumerici e speciali e deve contenere almeno un carattere non alfabetico e un misto di lettere minuscole e maiuscole.
*c)* Non deve essere una semplice parola rintracciabile in un dizionario;

6.9. Gli applicativi utilizzati per il trattamento devono richiedere a loro volta un nome utente e una password.

6.10. Alle eventuali password di accesso agli applicativi si applicano le indicazioni di cui ai punti 6.7, 6.8 e 6.9. Per gli applicativi che non consentano di automatizzare i controlli di cui al punto 6.8 va previsto un adeguamento, i cui tempi vanno indicati nel documento di cui al punto 4.1.

6.11. Il responsabile di servizio/trattamento, con cadenza almeno trimestrale, provvede alla disattivazione delle utenze su cui risultasse qualche problema (mancato utilizzo da più di sei mesi, un elevato numero di tentativi di accesso non riusciti, o simili).

6.12. Nome utente e password sono strettamente personali. L'utente è tenuto:

*a)* A non comunicare a terzi le password;

*b)* A non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;
*c)* A scegliere la password di accensione diversa dalle altre password;
*d)* Ad attenersi a tutte le indicazioni contenute nel Manuale per la sicurezza (Parte VII).

**7. Trasmissione dei dati**

7.1. Le connessioni telematiche verso le banche dati degli uffici, provenienti dall'esterno dello stesso ufficio, sono distinti in tre categorie:
*a)* Connessioni provenienti da altri uffici dell'Amministrazione Pubbliche;
*b)* Connessioni provenienti dall'interno dell'Ente, su postazioni di lavoro disponibili ai dipendenti;
*c)* Connessioni provenienti da utenti e postazioni di lavoro non appartenenti all'Amministrazione Pubblica.
7.2. Le connessioni di tipo a vengono controllate attraverso il Sistema Informatico di Sicurezza della Rete comunale, secondo le regole seguenti:
7.3. Sul collegamento di ciascun Servizio/Ufficio verso l'esterno è installato un apparato di controllo (*firewall*);
7.4. In maniera predefinita, il firewall è configurato in maniera da permettere alle postazioni di lavoro interne all'ufficio di accedere ai servizi disponibili sulla rete, bloccando i tentativi di accesso provenienti dall'esterno verso il Servizio/Ufficio;
7.5. Le procedure per la sicurezza delle connessioni sono stabilite dall'Amministratore di sistema di concerto con il Responsabile del Servizio/trattamento interessato. Qualora le postazioni pubbliche consentano l'accesso ai dati sensibili o giudiziari, occorrerà stabilire rigorose procedure per l'autenticazione degli utenti (firma digitale, personale di presidio alla postazione, o simili).
7.6. Le procedure per la sicurezza delle connessioni di tipo 7.1.c) sono stabilite dall'Amministratore di Sistema di concerto con il Responsabile del Servizio/trattamento.
7.7. Non sono autorizzati collegamenti telematici distinti da quelli previsti ai punti precedenti o comunque connessioni prive di sistemi di autenticazione del ricevente, di protezione e controllo della trasmissione.
7.8. Qualora siano necessarie connessioni del tipo descritto al precedente punto, queste andranno effettuate da locali dedicati, le cui postazioni non siano connesse alla rete comunale. Per questi locali andranno previste adeguate misure di controllo degli accessi.

**D) Piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.**

**8. Manuale per la sicurezza**

8.1. I Responsabili di Servizio/trattamento provvedono all'eventuale personalizzazione del Manuale per la sicurezza, con la collaborazione dell'Amministratore di sistema.
8.2. Il Manuale per la sicurezza viene aggiornato almeno ogni due anni.
8.3. Il Manuale per la sicurezza viene consegnato a tutti gli utenti / incaricati.

**9. Piano di intervento e formazione**

9.1. L'Amministratore di Sistema provvede ad informare tempestivamente i Responsabili di Servizio/trattamento di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza. Analogamente dovrà essere tempestivamente informato il Servizio Organizzazione e Informatizzazione del 1° Settore.
9.2. I soggetti Responsabili di servizio/trattamento provvederanno, se del caso, ad informare tempestivamente gli incaricati:
*a)* della presenza di virus negli elaboratori dell'Ufficio;
*b)* di prassi da parte del personale non conformi alle disposizioni di sicurezza;
*c)* della periodica necessità di variazione delle parole chiave da parte degli incaricati;
*d)* della disponibilità di programmi di aggiornamento relativi all'antivirus.
9.3. I Responsabili, ove richiesto o ove se ne ravvisi la necessità, provvederanno ad organizzare riunioni per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.

## ANALISI DEI RISCHI: EVENTI E LORO IMPATTO SULLA SICUREZZA

| NATURA | EVENTO | DESCRIZIONE EVENTO ED IMPATTO SULLA SICUREZZA | Note |
|---|---|---|---|
| **Comportamento Operatori** | Sottrazione di credenziali di autenticazione | **Descrizione:**<br>Le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso.<br>**Impatto:**<br>Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto. | |
| | Errore materiale | **Descrizione:**<br>A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati | |
| | Comportamenti illegali conseguenti a minacce su operatori | **Descrizione:**<br>In conseguenza di pressioni di vario tipo (es. minacce, ricatti, pressioni psicologiche) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, dei dati. | |
| | Comportamenti sleali e/o fraudolenti | **Descrizione:**<br>Con comportamento consapevole, derivante potenzialmente da vari fattori (risentimenti verso l'Ente, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può compor-tare la sottrazione, in modo illecito, dei dati. | |

| | | | |
|---|---|---|---|
| **NATURA** | **EVENTO** | **DESCRIZIONE EVENTO ED IMPATTO SULLA SICUREZZA** | **Note** |
| **Eventi relativi agli strumenti** | Virus informatici | **Descrizione:**<br>Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può essersi venuto ad installare o essersi semplicemente eseguito un software spurio del tipo "virus" informatico.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, dei dati. | |
| | Spamming | **Descrizione:**<br>Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono creare false notizie o indurre gli incaricati a cadere in truffe o in siti ingannevoli.<br>**Impatto:**<br>Gli incaricati possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari. | |
| | Accesso da stazioni non autorizzate | **Descrizione:**<br>Soggetti in possesso di credenziali di accesso al sistema o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW da cui è possibile intervenire su una banca dati obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, dei dati. | |
| | Intercettazione di informazioni transitanti sulla rete | **Descrizione:**<br>Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica dell'Ente. Ciò può avvenire in un qualunque punto tra il il sistema utilizzato e il sistema HW/SW degli incaricati<br>**Impatto:**<br>Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati. | |
| **NATURA** | **EVENTO** | **DESCRIZIONE EVENTO ED IMPATTO SULLA SICUREZZA** | **Note** |
| **Eventi relativi agli strumenti** | Malfunzionamento di apparecchiature | **Descrizione:**<br>I sistemi HW/SW con i quali vengono trattati i dati oggetto dell'evento da parte degli incaricati, possono avere/subire dei malfunzionamenti da cui possono derivare azioni reali sui dati, parzialmente o totalmente, diverse da quelle che si volevano operare. | |

| | | | |
|---|---|---|---|
| | | **Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. | |
| | Degrado di apparecchiature | **Descrizione:**<br>I sistemi HW/SW con i quali vengono trattati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare azioni reali sui dati, parzialmente o totalmente, diverse da quelle che si volevano operare.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. | |
| **Eventi relativi al contesto** | Accesso non autorizzato a locali da cui si può accedere ai dati | **Descrizione:**<br>Un soggetto non autorizzato che acceda fisicamente ai locali dai quali si possa entrare e trattare le banche dati può intenzionalmente o inconsapevolmente manipolare le stesse.<br>**Impatto:**<br>Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, dei dati. | |
| | Sottrazione di strumenti contenenti dati e/o programmi | **Descrizione:**<br>I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente.<br>**Impatto:**<br>L'evento comporta la sottrazione in modo illecito di dati. | |

| NATURA | EVENTO | DESCRIZIONE EVENTO ED IMPATTO SULLA SICUREZZA | Note |
|---|---|---|---|
| **Eventi relativi al contesto** | Eventi distruttivi naturali/artificiali, accidentali o volontari | **Descrizione:**<br>I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere colpiti da eventi distruttivi di origine sia fortuita che dolosa.<br>**Impatto:**<br>Dall'evento può derivare la distruzione totale o parziale della banca dati. | |
| | Guasto ai sistemi complementari | **Descrizione:**<br>I sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata (o che contengono) la banca dati possono subire malfunzionamenti derivanti da varie cause.<br>**Impatto:**<br>Dall'evento può derivare la distruzione totale o parziale della banca dati. | |

## PROFILI DI BACK-UP

| Codice | Supporto | Descrizione | Frequenza | Conservazione | Struttura incaricata |
|---|---|---|---|---|---|
| Server 0 | disco esterno USB **Disco-HotSwap** | Copie automatiche dati e della configurazione di sistema | Giornaliera | In appositi contenitori chiusi a chiave | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log |
| Server 1 | disco esterno USB **Disco-HotSwap** | Copie automatiche dati e della configurazione di sistema | Giornaliera | In appositi contenitori chiusi a chiave. | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log.. |
| Server 1 solo xdati Halley | sistema di back up delocalizzato, per proteggere i dati da eventi disastrosi ed assicurare la continuità dei servizi ai cittadini secondo la normativa in materia di continuità operativa e di disaster recovery, Servizio denominato 'Servizio Immedia Cloud Storage' | | | | |
| Server 2 | disco esterno USB | Copie automatiche dati e della configurazione di sistema | Giornaliera | In appositi contenitori chiusi a chiave. | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log. |
| Server3 | disco esterno USB **Disco-HotSwap** | Copie automatiche dati e della configurazione di sistema | Giornaliera | In appositi contenitori chiusi a chiave. | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log. |
| Server 5 | disco esterno USB | Copie automatiche dati e della configurazione di sistema | Giornaliera | In appositi contenitori chiusi a chiave. | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log. |
| Server 6 | disco esterno USB | Copie manuali | periodica | In appositi contenitori chiusi a chiave | **CSI:** impostazione e controllo procedure di esecuzione automatica con verifiche settimanali sul corretto funzionamento attraverso files di log. |
| Tutti gli utenti | Da cartella a cartella personale | Copie manuali a scelta dell'utente | A scelta dell'utente | su disco fisso del server3 cartelle personali mappate come unità Z | operatori |

# PARTE VII°

# Manuale per la Sicurezza nell'uso delle tecnologie informatiche

## AD USO DEGLI INCARICATI

## INTRODUZIONE

Questa appendice al Documento Programmatico per la Sicurezza 2010 vuole fornire ai soggetti che, a vario titolo, sono incaricati del trattamento un ausilio alla gestione ed allo sviluppo della sicurezza dell'informazione.
E' doveroso premettere che la sicurezza delle informazioni è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà. Oggi buona parte del pianeta vive nella società dell'informazione, basata cioè sull'uso delle informazioni come parte integrante delle attività umane. Pertanto, la sicurezza delle informazioni è diventata una componente della sicurezza dei beni in generale. Difatti oggigiorno l'informazione è da tutti riconosciuta quale bene patrimoniale, e tale concetto viene definito dalle linee guida in materia di sicurezza dei dati fin dalla BS7799: "*l'informazione è un bene che, al pari di altri beni che costituiscono il patrimonio di un'azienda, rappresenta un valore per l'organizzazione e necessita pertanto di essere adeguatamente protetto"*:
Qualunque progettualità che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali: la disponibilità, l'integrità e la riservatezza delle informazioni.
**La disponibilità** è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono. Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e
che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili. Per impedire l'inaccessibilità delle informazioni, si deve preservare la disponibilità delle condizioni ambientali (energia, temperatura, umidità, atmosfera, ecc.) e delle risorse hardware e software a fronte sia di problemi interni (guasti, errori, blackout, disastri e altro), sia proteggerle da attacchi esterni, per esempio provenienti da Internet, volti a impedire o a ridurre l'accessibilità ai sistemi e alle informazioni. Sistemi di backup locale e remoto, ridondanza dell'hardware e degli archivi, firewall e router configurati per neutralizzare attacchi DoS (denial of Service), sistemi di climatizzazione, gruppi di continuità, controllo dell'accesso fisico, monitoraggio delle prestazioni, sono alcuni degli strumenti che servono per mantenere la disponibilità.
**L'integrità** è il grado di correttezza, coerenza e affidabilità delle informazioni e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche.
Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio un database.
**La riservatezza** consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate e si applica sia all'archiviazione e sia alla comunicazione delle informazioni. Un'informazione è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione; ad esempio il nome e il numero di conto corrente di una persona, separati, non sono informazioni: è la combinazione dei due dati che costituisce l'informazione.
La riservatezza dell'informazione può essere quindi garantita sia nascondendo l'intera informazione (per esempio con tecniche di crittografia) sia nascondendo la relazione tra i dati che la compongono. La riservatezza non dipende solo da strumenti hardware e software; il fattore umano gioca un ruolo chiave quando vengono ignorate le elementari regole di comportamento: tenere le password segrete, controllare gli accessi a reti e sistemi, rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione), cifrare i documenti e i messaggi riservati e così via.

## LINEE GUIDA PER LA SICUREZZA NELL'UTILIZZO DELLE TECNOLOGIE INFORMATICHE

Il D.lgs 196/2003 identifica i requisiti minimi che devono essere sempre presenti nei sistemi informativi:
- Autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione;
- Utilizzazione di un sistema di autorizzazione;
- Aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei

sistemi;
- Tenuta di un aggiornato Documento Programmatico sulla Sicurezza;
- Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati.

In pratica quanto sopra si traduce in concrete azioni atte a: proteggere i computer ed i dati da accessi di persone non autorizzate che si possono attuare tramite l'utilizzo di password, della cifratura/crittografia dei dati o di altri sistemi di autenticazione, di adottare tutte le cautele possibili atte a prevenire il materiale furto dell'hardware stesso ed infine proteggere i computer da minacce informatiche.
E' bene rammentare che le sanzioni per chi non rispetta o non applica le direttive impartite dalla legge sono abbastanza pesanti; si dividono in illeciti civili e penali e comportano il pagamento di multe e persino la reclusione fino a 36 mesi.

## LA MESSA IN SICUREZZA DEGLI AMBIENTI DI LAVORO

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

## CUSTODIA DEI SUPPORTI DI ARCHIVIAZIONE ELETTRONICA

Per i floppy disk, cd-rom, dvd o altri supporti di archiviazione logica parimenti usati (chiavette di memoria USB, hard disk estraibili o esterni, ecc..) si applicano gli stessi criteri validi per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

## UTILIZZO DELLE PASSWORD

Si ricorda che il citato d.lgs 196/2003 prevede (cfr art. 34) che l'impostazione delle password deve seguire alcune regole: le parole chiave devono avere una lunghezza minima di otto caratteri (o la lunghezza massima possibile ammessa se il sistema non lo permette); le password vanno rinnovate ogni sei mesi (tre mesi per i dati sensibili e giudiziari); le stesse non devono essere composte da nomi comuni o collegati con la vita personale o con l'attività svolta dall'utilizzatore.
Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- La password di accesso al computer (comunemente denominata password da bios) impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
- La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ente.
- La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- La password del salvaschermo (screensaver), infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di accesso al computer (ossia la prima), che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza.
Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura quindi **non fatevi spiare quando state digitando la password.**

## CONSIGLI PER LA SCELTA DELLE PASSWORD

La protezione offerta da una password dipende fortemente dalla sua complessità. Le password brevi e composte da parole comuni sono facili da ricordare e altrettanto da scoprire. Le password complesse sono l'opposto: difficili da scoprire e da ricordare.
Come si può conciliare la sicurezza con parole mnemoniche?
I sistemi operativi **Windows 2000** e **XP** accettano password con una lunghezza massima di 128 caratteri e questo permette il vantaggio di usare delle frasi che hanno il vantaggio di essere lunghe e più facili da ricordare anche se complesse.
Una password che soddisfi i criteri minimi di sicurezza potrebbe essere *K^uy%56F*, ma anche la frase *Domani @ lavorare @lle 9.00 AM accendo il computer* soddisfa i requisiti ed è più semplice da ricordare pur essendo più lunga da inserire.
Le regole di creazione sono semplici: le vocali delle congiunzioni hanno il simbolo @ al posto della lettera a e l'orario è nello standard dei paesi di madrelingua inglese.
Le variazioni possono essere molteplici ed infinite, l'importante è utilizzare il più possibile categorie di caratteri, numerici, lettere maiuscole e minuscole, speciali.
Inoltre rammentate che una password come *pippo* composta da cinque caratteri in minuscolo può essere scoperta in meno di 20 secondi con l'ausilio di un banalissimo programma di crack di password.
Per finire è tassativamente da evitare lo scrivere la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per iscritto, non lasciate in giro i fogli utilizzati. Quindi **mai** lasciare foglietti adesivi con annotata la password sotto il telefono, il portapenne, ecc. ecc.

## SICUREZZA INFORMATICA

Per introdurre l'argomento può essere utile analizzare alcuni luoghi comuni che spesso ricorrono quando ci si occupa di sicurezza informatica:

*Quali prodotti devo acquistare per sentirmi veramente al sicuro?*

Al riguardo si può affermare con assoluta certezza che la sicurezza non si identifica in un prodotto specifico ma in un processo lungo e ripetitivo che consiste nell'adottare una serie di misure volte a prevenire e scoprire i tentativi di accesso non autorizzato ad un sistema informatico.
In questa prospettiva dunque non è sufficiente acquistare un antivirus od un firewall per risolvere tutti i problemi poiché, come prima cosa, occorre cambiare le nostre abitudini in modo da riadattarle ad una nuova prospettiva in cui la sicurezza è l'obiettivo finale.

*Perché dovrei occuparmi degli aspetti inerenti la sicurezza del mio sistema?*

Per il semplice motivo che ormai l'uso del computer non è più limitato alle sole ore d'ufficio ma investe svariati altri aspetti della nostra vita privata (dal divertimento, all'acquisizione e scambio di notizie, al disbrigo di pratiche burocratiche, ecc.). Nel momento stesso in cui accediamo a quell' immenso database di risorse che rappresenta la rete Internet noi diventiamo parte integrante di quest'ultima e siamo sicuramente interessati ad evitare che qualunque individuo possa penetrare nel nostro sistema ed usarlo come base per sferrare attacchi contro altri oppure per rubare la nostra e-mail o carpire qualsiasi altro genere di informazione rilevante.

*Chi può essere interessato ad accedere al mio sistema?*

Praticamente chiunque sia motivato da intenzioni non proprio encomiabili. Per un aggressore l'identità della persona cui appartiene un determinato sistema non ha alcuna importanza poiché l'unico obiettivo è penetrare il sistema stesso per poterlo successivamente riutilizzare o per compiere attività dannose od anche per il solo gusto di farlo.

*Con quale facilità è possibile irrompere in un sistema informatico?*

In alcuni casi si tratta di una facilità disarmante. Purtroppo la complessità del software che viene oggigiorno prodotto si accompagna in alcuni casi ad un livello di imperfezione tale da determinare l'insorgenza di gravi problemi di sicurezza.
Queste vere e proprie "falle" sono quelle alla cui ricerca si spingono gli hacker ( i c.d. pirati informatici) e sono quelle che vengono sfruttate (da chi non appare motivato da una solida etica) per penetrare illecitamente nei sistemi informatici.
Per far fronte a queste lacune i produttori di software sono costretti a rilasciare frequenti patch di aggiornamento la cui applicazione rientra però nella sola responsabilità degli utenti finali. Inoltre non va dimenticato che la complessità del software può a volte investire gli aspetti attinenti la sua corretta configurazione ad un livello tale da spingere l'utente ad usare configurazioni (c.d. di default) che aprono la strada a pericolose inadeguatezze in termini di sicurezza.

*Chi mi garantisce che seguendo un certo tipo di approccio il mio sistema diventa veramente sicuro?*

Nessuno. Qualunque siano le azioni intraprese o le procedure seguite non sarà mai possibile ottenere una garanzia di protezione al 100%.
Nella realtà l'unica cosa di cui si può veramente essere certi è che quanto più si affronta con criterio la tematica tanto minore sarà la probabilità che qualcuno o qualcosa riesca a procurarci un danno.

*La sicurezza informatica si basa sulla difesa della privacy!*

Questa affermazione è vera soltanto in minima parte: in effetti la privacy, intesa come diritto alla tutela delle notizie e delle informazioni riguardanti la propria identità personale e sociale, è senza dubbio uno degli aspetti principali riguardanti la problematica della sicurezza ma non è l'unico né tanto meno il più importante.
Fatta questa precisazione, è tuttavia importante sapere che esiste il rischio reale che qualcuno possa catturare informazioni inerenti le nostre abitudini in rete oppure possa carpire altre notizie attraverso gli stessi strumenti che normalmente utilizziamo (ad esempio il browser) ma, al tempo stesso, occorre anche sapere che esistono dei rimedi utilizzabili per scongiurare questo genere di attività.
Peraltro possiamo ricordare che il modo migliore per proteggere la nostra privacy consiste nell'adottare comportamenti prudenti ed ispirati al buon senso come potrebbe essere quello di non diffondere ingenuamente informazioni di carattere riservato riempiendo spesso inspiegabili forms di registrazione.

## IL DECALOGO DELLA SICUREZZA

Sebbene non sia possibile individuare un complesso ideale di misure di prevenzione possiamo con certezza affermare che molti dei problemi che tipicamente si presentano quando si tratta della sicurezza di un sistema informatico possono essere evitati attraverso l'adozione delle seguenti **azioni correttive** che, nel loro complesso, possono essere trattate come una sorta di decalogo:

**usare un buon antivirus**: qualunque computer connesso alla rete Internet deve esserne munito; inoltre è altrettanto importante provvedere con regolarità all'aggiornamento del file delle firme;
**usare un firewall**: può sembrare eccessivo ma l'uso di dispositivi di filtraggio come i firewall, purché opportunamente configurati, è in grado di offrire un discreto grado di protezione contro determinati tipi di attacco e soprattutto contro tutta una serie di attività preparatorie (come ad es. la scansione delle porte TCP/UDP) che un aggressore in genere compie prima di tentare un accesso non autorizzato;
**non aprire ingenuamente allegati di posta elettronica**: questa semplice regola vale anche per i messaggi di posta che sembrano originati da un indirizzo conosciuto; in ogni caso è sempre opportuno salvare in un file l'allegato e sottoporlo ad una scansione virale (antivirus) prima di aprirlo;
**non eseguire ingenuamente programmi di ogni tipo**: è buona regola accertarsi sempre della genuinità di qualsiasi programma prima di eseguirlo e lo stesso dicasi per tutti quei documenti che possono contenere delle macro; Analogamente **non installate e/o utilizzate in Ufficio programmi per scambio di file sulla**

**rete peer to peer (p2p) quali i vari emule, winmix, kazaa, edonkey, ecc. e tanto meno i programmi di comunicazione istantanea come i messanger e le chat (icq, msn messanger, miranda, trillian, ecc. ecc.)**
applicare sempre le più recenti patch: questo vale non soltanto per il sistema operativo ma anche per il software applicativo;
**prestare la massima attenzione al funzionamento anomalo del sistema operativo**: è assolutamente opportuno guardare sempre con sospetto ai funzionamenti apparentemente inspiegabili del sistema operativo e cercare di individuarne le cause per quanto possibile anche con l'uso di strumenti specifici;
**disabilitare Java, JavaScript ed ActiveX**: queste tecnologie possono costituire una vera spina nel fianco durante la navigazione su Internet; in alternativa, per non rendere la navigazione su alcuni siti frustrante, è possibile proteggersi, ma entro certi limiti, facendo uso di software specifico che funge da filtro per i contenuti interattivi che vengono normalmente ricevuti o utilizzando forme di navigazione anonime tramite proxy server;
**disabilitare le funzionalità di scripting nei client di posta elettronica**: spesso infatti le maggiori vulnerabilità che colpiscono i browser, legate alla presenza di contenuti interattivi, si presentano anche in questo genere di software;
**fare un backup regolare di tutti i dati sensibili**: ugualmente importante è tenere in posti sicuri le copie generate;
**creare un disco di boot**: ciò può aiutare in un eventuale attività di recovery di un sistema compromesso a patto però che la copia sia assolutamente genuina e sia conservata in un luogo sicuro.

## LE MINACCE INFORMATICHE

### Cosa sono i "malicious software" o malware

Le cronache informatiche di questi ultimi tempi hanno fornito la dimostrazione pratica di un dato di fatto innegabile: nessuno può dirsi veramente al sicuro dagli attacchi portati attraverso il cosiddetto codice nocivo. Ma che cosa si intende per codice nocivo ed in quale modo questo può effettivamente produrre un danno ? Con il termine inglese di "malware", contrazione di malicious software, generalmente si intende un qualsiasi frammento di codice di lunghezza variabile che, penetrato all'interno di un computer, si dimostra potenzialmente in grado di danneggiarlo. Dunque la caratteristica che giustifica l'appellativo di nocivo è l'attitudine a causare danni a prescindere dalla circostanza che poi questi effettivamente si verifichino. Per questo motivo in questa categoria rientrano tradizionalmente i virus, i macro virus, i worm ed i cavalli di troia.

### I Virus

Si definisce come virus qualsiasi porzione di codice che si installa all'interno di un programma host al fine di utilizzare quest'ultimo come mezzo di propagazione. Un virus non può essere eseguito in maniera autonoma ed indipendente ma richiede che sia stato attivato un programma host.
Due sono gli elementi che è necessario prendere in considerazione quando si parla di virus: il meccanismo di propagazione ed il tipo di operazioni eseguite una volta che il virus sia attivo e residente in memoria. Il meccanismo di propagazione è forse l'aspetto più importante nel valutare la pericolosità di una determinata classe di codice nocivo.
Infatti mentre in passato il pericolo di una infezione da virus poteva dirsi limitato a pochi pc ed il mezzo di diffusione era costituito principalmente da floppy disk attualmente l'avvento di Internet ha dato un forte impulso alla crescita delle infrastrutture di rete per cui negli scenari odierni i danni causati dai virus possono colpire centinaia di migliaia di sistemi in poco più di una settimana sfruttando mezzi di connettività globale velocissimi come ad esempio la posta elettronica.
A seconda delle caratteristiche di diffusione di cui sono in possesso i virus appartengono a due distinte categorie:
**virus di tipo parassita**: infettano i classici file eseguibili (.com, .exe e .dll) lasciandoli perfettamente utilizzabili ma al tempo stessi utilizzandoli come mezzi di propagazione;
**virus del settore di avvio**: copiano se stessi nel settore di avvio dei dischetti o del disco rigido e si dimostrano particolarmente subdoli poiché sono in grado di acquisire il controllo del sistema al momento del suo bootstrap e quindi molto prima che sia caricato il sistema operativo e, conseguentemente, qualsiasi

programma antivirus;
In quest'ultimo gruppo rientra anche il codice virale che, anziché colpire il settore di avvio, infetta il Master Boot Record vale a dire quell'insieme di istruzioni localizzate all'inizio di qualsiasi disco fisso, cioè nel primo settore del primo cilindro del primo piatto, in grado di interpretare la tabella delle partizioni che contiene la mappa della configurazione dell'intero disco.
Peraltro è proprio questa tipologia di virus quella che presenta le particolarità più insidiose in quanto tende ad acquisire il controllo dell'MBR rilocandolo altrove ed inserendo il proprio codice nocivo all'interno dello stesso.
In questo modo, durante il riavvio della macchina, il virus riesce ad eseguire qualsiasi tipo di operazione: modificare le chiamate del BIOS od intercettare quelle dirette a leggere lo stesso MBR dirottandole verso la copia precedentemente rilocata (l'uso di queste tecniche cosiddette stealth è normalmente diretto ad evitare l'identificazione da parte dei normali antivirus).
Infine non è raro trovare anche virus cosiddetti **multi-partiti** capaci non soltanto di infettare l'MBR od il settore di boot del disco ma anche di esporre caratteristiche di tipo parassita che li rendono idonei a sfruttare una ampia gamma di mezzi di diffusione.
L'uso di tecniche evolute nei moderni virus
L'evoluzione delle tecniche di programmazione ha portato negli ultimi anni alla proliferazione di una nuova generazione di codice virale sempre più insidioso e subdolo rappresentato da:
virus polimorfici;
virus crittografati;
La prima specie raccoglie quei virus che adottano tecniche particolari per rendere la loro impronta virale diversa di volta in volta. Attraverso un complesso e sofisticato processo di recodifica essi creano delle varianti di se stessi ostacolando o rendendo molto più difficoltosa la loro identificazione da parte dei programmi antivirus.
Il secondo genere invece si caratterizza per l'utilizzo di metodi di occultamento della impronta virale che sfruttano la crittografia. In questo caso la logica di crittografia/decrittografia può essere contenuta all'interno dello stesso codice virale oppure può impiegare apposite routine fornite di default dallo stesso sistema operativo.
Peraltro nulla esclude l'impiego congiunto di polimorfismo e crittografia al fine di produrre virus altamente evoluti anche se ciò inevitabilmente si traduce in un codice di maggiori dimensioni la cui realizzazione è alla portata di pochi individui in possesso di capacità tecniche non comuni.

## Cavalli di Troia (Troian Horse)

I cavalli di Troia derivano il loro nome dal celebre episodio dell'Iliade di Omero che vide i Greci sopraffare i Troiani in virtù di uno stratagemma geniale.
Un cavallo di Troia basa tutta la sua potenza sull'inganno in quanto è un programma che dichiara di svolgere determinate funzioni, per di più di utilità, ma che in realtà compie sul sistema dell'utente, e ad insaputa di quest'ultimo, una serie di operazioni dannose che possono essere le più svariate.
Ciò che caratterizza dunque questa tipologia di codice è l'approfittamento della fiducia che l'utente ripone nel codice che accetta di eseguire perché spinto in qualche modo a farlo.
Peraltro, per converso, questa stessa caratteristica è anche la maggiore limitazione di un cavallo di Troia che non può in alcun modo operare sul sistema se non viene attivato da parte dell'utente.
La diffusione di questo genere di codice oggigiorno è talmente elevata che tutti i maggiori produttori di antivirus hanno ormai aggiornato i propri prodotti in modo tale da non identificare più soltanto i tradizionali virus informatici ma anche i ben più subdoli cavalli di troia.

## Spyware & Backdoor

Lo spyware è un software che, caricato inconsapevolmente, è in grado di monitorare l'attività che l'utente sta svolgendo sul proprio computer mentre una backdoor è una parte di codice non documentata o segreta che consente a terzi di inserirsi furtivamente nel computer, proprio come una porta sul retro (è questa la traduzione letterale).

## Worm

Il concetto di worm è molto simile a quello di virus con la sola differenza che un worm non si riproduce localmente ma semplicemente si propaga attraverso sistemi differenti.
Una chiave interpretativa definisce i worm come frammenti di codice autonomi ed indipendenti che esistono solo in memoria consumando le risorse del sistema ed auto-propagandosi.

## Meccanismi di propagazione

Per comprendere in che modo difendersi è innanzitutto necessario capire quali sono i principali meccanismi di propagazione del codice nocivo.
Nell'epoca in cui viviamo il sistema di trasmissione delle informazioni più diffuso e veloce è senza dubbio rappresentato dalla posta elettronica per cui, inevitabilmente, questo è anche il veicolo primario di propagazione del codice nocivo esistente.
Fatta questa considerazione le principali modalità di diffusione di codice nocivo all'interno dei messaggi di posta elettronica sono rappresentate da:
**Macro:** costituiscono un meccanismo efficiente, soprattutto per quanto riguarda i macro virus ed i worm, poiché normalmente vengono eseguite in modo trasparente e non richiedono una interazione con l'utente. Il punto debole è invece rappresentato dal fatto che esse richiedono la presenza di uno specifico client di posta elettronica in grado di interpretare correttamente i comandi in esse contenuti ed, in questa prospettiva, la mancanza di un ambiente universale potrebbe limitarne in un certo senso la diffusione;
**Allegato di posta**: è tuttora il principale veicolo per i virus ed i cavalli di troia ma presenta due punti deboli noti. Il primo è dato dal fatto che esso richiede una interazione con l'utente il quale deve essere spinto ad aprire l'allegato mentre il secondo è costituito dalla sua offensività che è ovviamente limitata ad una specifica piattaforma in relazione alla forma assunta dall'allegato stesso (ad esempio file .exe). Questa ultima limitazione è tuttavia soltanto fittizia se si pensa alla enorme diffusione di cui godono oggigiorno le piattaforme Windows rispetto a tutte le altre.
Non dimentichiamo inoltre che, accanto alla e-mail, un altro mezzo di diffusione del codice nocivo è rappresentato dal web ed in questo caso il pericolo assume principalmente la forma di programmi che vengono scaricati dagli innumerevoli archivi software esistenti in rete.

## POSTA ELETTRONICA E SPAM

L'elevata visibilità a livello mondiale resa possibile dalla posta elettronica ha un rovescio della medaglia i cui effetti sono visibili a chiunque abbia usato questo servizio almeno una volta: il suo nome è SPAM, Junk Mail (posta spazzatura), UCE (Unsolicited Commercial Email) o più semplicemente posta indesiderata. Si manifesta sotto forma di messaggi ricorrenti, non richiesti esplicitamente, di carattere principalmente commerciale e inviati contemporaneamente a migliaia di destinatari.
Il fenomeno è oramai un flagello a livello mondiale non solo perché infastidisce l'utente finale che deve spendere il proprio tempo a separare i messaggi utili da quelli indesiderati ma soprattutto perché si rivela essere un vero e proprio furto di risorse.
Lo spamming è estremamente remunerativo come mezzo pubblicitario grazie al costo di gestione irrisorio. Si è calcolato che è sufficiente che un solo utente su qualche migliaio acquisti il prodotto reclamizzato perché la bilancia dello spammer risulti in attivo. Il motivo di questo successo sta essenzialmente nella scarsità di risorse necessarie per mettere in opera questa attività e l'utilizzo illegale di servizi presenti sulla rete.
In passato l'opera dello spammer è stata paragonata a quella del volantinaggio che spesso contribuisce a riempire le nostre buchette delle lettere. La differenza è in realtà enorme.
Nel caso della campagna pubblicitaria basata su volantini la società promotrice si accolla l'intero onere della stampa e della distribuzione.
Nel caso dello spam il costo della distribuzione ricade quasi interamente sul destinatario, sul suo provider e sugli eventuali server di posta usati per l'inoltro.

## Come difenderci

Di motivi validi per combattere lo spam e quelli che ne fanno uso ce ne sono a sufficienza. Come dobbiamo comportarci a riguardo? In generale possiamo agire su tre diversi fronti: prevenzione, filtraggio e denuncia.
Il primo aspetto si prefigge lo scopo di individuare una serie di regole e di tecniche per evitare che gli spammer entrino in possesso del nostro indirizzo di posta attraverso strumenti di ricerca automatica. In seguito se ne parlerà diffusamente.
Se dobbiamo occuparci di filtraggio significa che l'aspetto preventivo non è stato sufficiente. Questo può succedere se l'indirizzo della nostra casella è stato generato automaticamente, se è stato inserito manualmente nel loro database o se, ovviamente, siamo stati poco cauti e lo abbiamo divulgato su internet senza precauzioni.
Per agire su questo fronte è indispensabile l'uso di un client di posta elettronica o un programma di terze parti che analizzi le email in ingresso ed in base ad una serie di regole da noi impostate separi quelle legittime da quelle pubblicitarie. I filtri in genere possono essere impostati per riconoscere un certo mittente o destinatario, per riconoscere particolari vocaboli presenti nell'oggetto o nel corpo dell'email e in base a questi decidere l'azione da compiere. È inoltre possibile eliminare direttamente il messaggio oppure memorizzarlo in una cartella speciale per essere ulteriormente analizzato dall'utente. Non sempre comunque questo tipo di strategia da dei buoni frutti: lo spam non individuato può essere ancora numeroso e alcune email legittime possono essere erroneamente scartate.
Per quando riguarda l'eventuale denuncia ad organi competenti si hanno due possibilità: la segnalazione ad organi di Abuse e, nel caso estremo, la denuncia al Garante per la protezione dei dati personali.
In ogni caso è possibile la segnalazione dello spammer ai servizi di Abuse del provider su cui risiede il suo sito e dei proprietari dei server usati illegalmente per inviare la posta. Sicuramente questa azione risulta molto più dannosa per gli spammer rispetto ad un semplice filtraggio perché in questo modo si cerca di minare direttamente la fonte. Una email filtrata automaticamente ci evita semplicemente l'incombenza di farlo manualmente. Ci fa sicuramente risparmiare tempo ma non elimina il problema alla radice né impedisce il furto di risorse.

## Le catene di Sant'Antonio

il termine deriva da una tradizione molto diffusa a partire dagli anni Cinquanta del secolo scorso (il 1900): si riceveva una lettera che iniziava con *"Recita tre Ave Maria a Sant'Antonio"* e proseguiva descrivendo le fortune capitate a chi l'aveva ricopiata e distribuita a parenti e amici e le disgrazie che avevano colpito chi invece ne aveva interrotto la diffusione. All'epoca la catena si diffondeva ricopiandola a mano e per posta; poi si è gradatamente tecnologizzata. Con l'avvento delle fotocopiatrici è scomparsa la ricopiatura manuale, e con l'arrivo di Internet è cessata anche la spedizione postale, soppiantata dalla più efficiente (e meno costosa) distribuzione istantanea via e-
mail.

## Ma che male fa diffondere una catena di sant'Antonio?

Tanto.
Le catene spedite dal posto di lavoro vi possono costare il lavoro! Spesso i programmi di posta aggiungono automaticamente in coda a ogni messaggio il nome del mittente e quello dell'azienda o dell'istituto presso il quale lavora il mittente. Il risultato è che una catena spedita dal posto di lavoro sembra "autenticata" dall'azienda/istituto, che difficilmente gradisce che il proprio nome venga abusato da un dipendente e associato a una bufala.
La diffusione di false notizie può portarvi in tribunale. L'incauta diffusione di un appello può avere conseguenze legali per chi l'ha fatto circolare.
Quelle autentiche che contengono appelli per curare persone malate spesso proseguono per anni dopo la morte della persona citata. Di conseguenza, i familiari continuano per anni a ricevere offerte di aiuto che non solo sono assolutamente inutili, ma ricordano loro ogni giorno la scomparsa di una persona cara. Voi come vi sentireste, se ogni mattina vi chiamassero in tanti al telefono per chiedervi come sta vostra figlia morta di

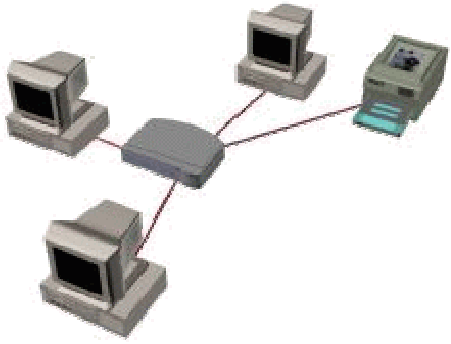
leucemia?
Grazie all'inesperienza degli utenti della Rete, le catene viaggiano con centinaia di indirizzi di e-mail al seguito. Gli spammer (i pubblicitari-spazzatura di Internet) usano queste catene per raccogliere indirizzi a cui mandare la loro assillante pubblicità più o meno pornografica, virus e compagnia bella. Se partecipate a una catena di Sant'Antonio, anche il vostro indirizzo finirà nelle liste degli spammer.

## LA RETE AZIENDALE

**Reti di computer: il Comune di Lendinara è dotato di una rete LAN e di una VPN (Virtual Private Network) per collegare fra loro i vari computer e sedi aziendali.**

### Che cos'è una rete?

Una rete informatica è un insieme di PC e di altri dispositivi che sono collegati tra loro tramite cavi o non. Il sistema consente a questi dispositivi di comunicare tra loro e di condividere informazioni e risorse. Le reti possono avere dimensioni differenti ed è possibile ospitarle in una sede singola oppure dislocarle in tutto il mondo.



Una rete che è collegata su un'area limitata si chiama "Rete Locale" oppure LAN (Local Area Network). Spesso la LAN è localizzata in una sola sede. Per WAN (Wide Area Network) si intende un gruppo di dispositivi o di LAN collegate nell'ambito di una vasta area geografica, spesso mediante linea telefonica o altro tipo di cablaggio (ad es. linea dedicata, fibre ottiche, collegamento satellitare, ecc..). Uno dei più grandi esempi di WAN è l'Internet stessa.
Esistono diverse tecnologie LAN; le più comuni sono: Ethernet e Fast Ethernet. Una rete può essere formata da una o più di queste tecnologie. Le reti Ethernet e Fast Ethernet funzionano in modo simile e la differenza principale è data dalla velocità alla quale trasferiscono le informazioni.
Ethernet funziona a 10 Megabit per secondo (o Mbps) e Fast Ethernet funziona a 100Mbps.
I dispositivi di una rete comunicano trasmettendosi reciprocamente informazioni; le informazioni trasmesse sono gruppi di piccoli impulsi elettrici, detti pacchetti. Ogni pacchetto contiene l'indirizzo del dispositivo che esegue la trasmissione (l'indirizzo di sorgente) e l'indirizzo del dispositivo che riceve i dati (l'indirizzo di destinazione). Queste informazioni vengono utilizzate dai PC e da altri dispositivi presenti nella rete per aiutare il pacchetto a raggiungere la propria destinazione. Le reti Ethernet e Fast Ethernet impiegano un protocollo chiamato CSMA/CD (Carrier-Sense Multiple Access with Collision Detection). In tal modo può comunicare solo un dispositivo per volta. Quando due dispositivi cercano di comunicare simultaneamente, tra i pacchetti trasmessi si verifica una collisione che viene rilevata dai dispositivi trasmittenti. I dispositivi cessano quindi di trasmettere e attendono prima di inviare nuovamente i loro pacchetti.
Il meccanismo è paragonabile ad una conversazione tra un gruppo di persone; se due persone parlano contemporaneamente, si fermano entrambe e una di esse inizia a parlare nuovamente.

### Quali sono i vantaggi di avere una Rete?

In una rete LAN (Local Area Network), le informazioni e le risorse possono essere condivise. Questa possibilità offre diversi vantaggi:

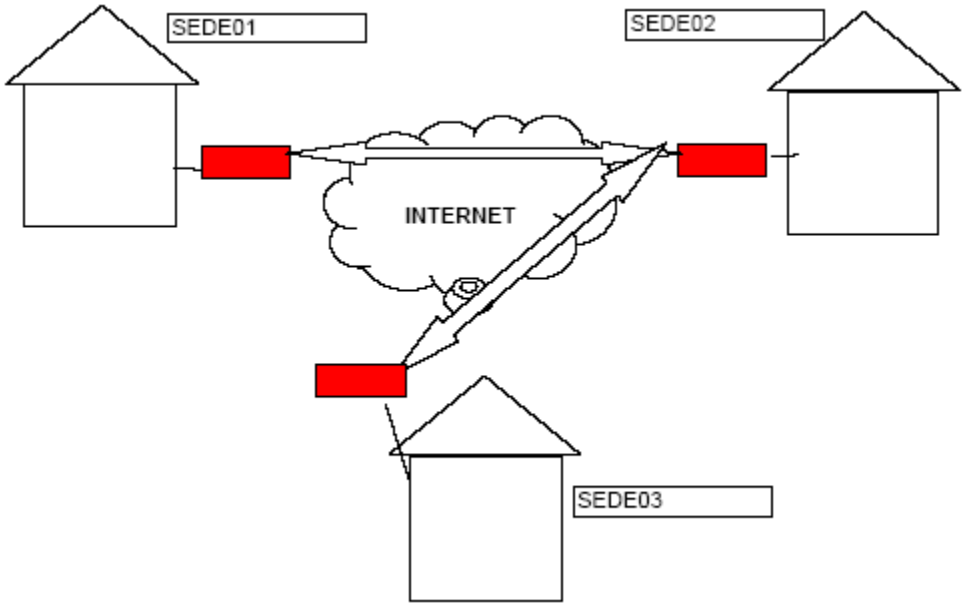
- E' possibile condividere periferiche costose, come le stampanti. In una rete, tutti i computer possono

accedere alla stessa stampante.

- E' possibile inoltrare dati tra utenti senza l'uso di floppy disk. Trasferendo file attraverso la rete, non si perde tempo nel copiare i file su un dischetto o su un altro PC. Inoltre vi sono meno limitazioni sulle dimensioni del file che può essere trasferito attraverso una rete.
- E' possibile centralizzare programmi informatici essenziali, come gli applicativi finanziari e contabili. Spesso gli utenti devono poter accedere allo stesso programma in modo che possano lavorarvi simultaneamente. Un esempio di ciò potrebbe essere un sistema di prenotazione di biglietti in cui è importante evitare di vendere due volte lo stesso biglietto.
  E' possibile istituire sistemi di backup automatico dei file. E' possibile usare un programma informatico per fare il backup automatico di file essenziali, risparmiando tempo e proteggendo l'integrità del proprio lavoro.

**V.P.N. (Virtual Private Network)**

Sono state attivate due VPN che connettono la rete informatica del Comune di Lendinara (SEDE02) con la rete informatica degli Uffici Cimiteriali (SEDE01) e con la rete informatica degli Uffici LLPP (SEDE03). Tali VPN permettono la comunicazione sicura dei dati, tra i tre punti, utilizzando tunnel criptati passanti per le linee internet. Tutti i passaggi di dati tra Comune e Cimitero e tra Comune e LLPP avvengono tramite VPN, negli altri casi sono inibiti dai firewall installati. Questa rete di computer è a tutti gli effetti una Intranet e come tale devono essere applicati gli stessi accorgimenti previsti dal DPsS per le reti informatiche locali.




I computer appartenenti alle tre sedi possono interagire tra loro come se fossero in un'unica rete fisica. La configurazione utilizzata non permette di accedere direttamente dalla Sede01_LLPP alla Sede03_Serv.Cimiteriali. Le comunicazioni ed i dati che transitano, da una sede ad un'altra tramite Internet, utilizzano una chiave software di crittografazione che di fatto ne impediscono il riconoscimento ai non autorizzati.

Le tre sedi sono state dotate di accessi centralizzati ed indipendenti alla rete Internet. I computer appartenenti ad una sede possono accedere autonomamente ad Internet salvo esplicite restrizioni decise dall'Amministratore della rete informatica. Ogni sede è provvista di protezione specifica (firewall) contro le intrusioni dall'esterno non autorizzate. Gli accessi dall'esterno alla rete informatica comunale possono essere autorizzati solo dall'Amministratore della rete informatica. Ogni altro accesso alla rete Internet (router, modem, ecc.), diverso da questi tre punti (firewall), deve essere inibito perché potenziale punto debole della rete informatica per l'ingresso di virus ed intrusioni.

Gli apparecchi sono stati installati, presso le varie sedi, configurati e collaudati per attivare le VPN automaticamente all'accensione senza intervento umano. Questa funzionalità ne garantisce il ripristino in caso di mancanza di alimentazione temporanea della rete elettrica.

## PICCOLO GLOSSARIO:

**adware.** Un programma che inietta pubblicità nel computer.
**area di notifica.** La zona in basso a destra della barra delle applicazioni di Windows.
**autorun.** Funzione di Windows che avvia automaticamente i programmi contenuti su CD e DVD.
**backup.** Copia di sicurezza di dati e/o programmi.
**boot virus.** Virus che si attiva all'avvio del computer.
**browser.** Programma per navigare nelle pagine del Web. Esempio classico: Internet Explorer.
**cartella.** Una suddivisione del vostro disco rigido, che può contenere file di vario genere, come un cassetto di uno schedario.
**chat.** Modo di comunicare istantaneamente via Internet tramite messaggi di testo.
**cleaner.** Programma antivirus specificamente progettato per eliminare uno o più virus specifici da un computer già infetto.
**dialer.** Programma che tenta di cambiare più o meno di nascosto il numero di telefono composto per collegarsi a Internet, sostituendolo con un costosissimo numero a pagamento.
**directory.** Lo stesso che cartella.
**estensione.** Il suffisso in coda ai nomi dei file. Nel nome di file documento.sxw, sxw è l'estensione.
**firewall.** Programma o dispositivo che filtra il traffico ostile o a rischio proveniente da Internet o uscente dal vostro computer.
**HTML.** Il linguaggio informatico usato per comporre le pagine diInternet e l'e-mail piena di effetti grafici.
**keylogger.** Programma o dispositivo che registra e inoltra al suo padrone tutto quello che viene digitato dalla vittima sorvegliata.
**link.** Rimando o collegamento verso una pagina di Internet o verso un indirizzo di posta.
**memoria USB.** Dispositivo ultracompatto per portare in giro notevoli quantità di dati.
**newsgroup.** Area di Internet dedicata alle discussioni a tema, accessibile tramite appositi programmi
**nickname.** Pseudonimo usato da un utente di Internet per brevità, per farsi riconoscere o per diventare anonimo e non farsi riconoscere.
**patch.** Aggiornamento-correzione di un programma o sistema operativo.
**phishing.** Truffa via Internet, che consiste nel mandare a milioni di utenti falsi e-mail che sembrano provenire da società rispettabili ma in realtà portano chi abbocca a consegnare i propri dati segreti ai truffatori.
**popup.** Pagina pubblicitaria che compare a sorpresa sopra quella che stiamo leggendo.
**RAM.** La memoria temporanea del computer, usata come area di lavoro.
**spam.** Pubblicità indesiderata diffusa via e-mail.
**spammer.** colui che dissemina lo spam.
**spyware.** Programma che comunica segretamente a terzi l'attività svolta al computer dalla sua vittima, per spionaggio o per raccogliere dati statistici.
**systray.** Lo stesso che area di notifica.
**trojan horse.** Virus che si spaccia per un programma utile o divertente ma ha in realtà un secondo fine.
**webmail.** Metodo per usare l'e-mail tramite il browser invece di usare un programma apposito.
**worm.** Un virus con le gambe. In altre parole, un programma ostile che è in grado di propagarsi da un computer all'altro senza richiedere l'intervento della vittima.

# PARTE VIII

# Documento Programmatico sulla Sicurezza del trattamento dei dati personali

# ANNO 2015

# SISTEMA DI VIDEOSORVEGLIANZA URBANA

## Appendice di aggiornamento al Documento Programmatico

## sulla Sicurezza dei dati personali

## redatta in osservanza del Provvedimento Generale del Garante della privacy

## dell'8 aprile 2010

## INDICE

## 1. Premessa

Il presente provvedimento ha lo scopo di disciplinare il trattamento dei dati personali acquisiti dal Corpo di Polizia Locale di Lendinara mediante un sistema di video sorveglianza, le cui caratteristiche sono esplicitate al punto 7 del presente Documento e sono rispondenti alle prescrizioni adottate dal Garante per la protezione dei dati personali nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010.

Il presente provvedimento garantisce inoltre che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei cittadini, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

## 2. Definizioni

Ai fini del presente documento si intende per:
- "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
- "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a)* a o) e da *r)* a *u),del* d.P.R. 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti; .
- "Garante", l'autorità istituita ai sensi del d.lgs. n.196/2003;
- "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi

previsti dal d.lgs. n.196/2003;
- "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

**3. Ambito di applicazione del documento**

Il presente provvedimento disciplina il trattamento dei dati personali realizzato mediante l'impianto di videosorveglianza urbana attivato presso il Comune di Lendinara, riguardante le seguenti aree di circolazione:

- Piazza Risorgimento;
- tratto di Via Garibaldi;
- tratto di Via Varliero;
- tratto di Via Adua;
- Ponte di Piazza;
- Piazza S. Marco;
- Piazzale Kennedy;
- Piazzale Duomo;
- tratto di Via S. Sofia;
- tratto via Ca' Morosini (accesso al piazzale Ecocentro);
- via Marconi e intersezione vie Canozio - De Gasperi;
- Piazzale Statuto.

**4. Normativa di riferimento**

Il presente provvedimento è stato adottato nel rispetto oltre che di quanto previsto dal Provvedimento generale del Garante per la privacy dell'8 aprile 2010 anche nel rispetto della disciplina generale in materia di protezione dei dati personali prevista dal d.1gs. 196/2003 (c.d. "Codice della privacy") nonché nel rispetto della legge n. 65 del 7 marzo 1986 (legge-quadro sull'ordinamento di Polizia Municipale) e ss.mm. li. e delle specifiche leggi regionali di settore.

Per quanto non espressamente previsto dal presente documento si rinvia oltre alla normativa di riferimento suddetta, anche al Documento Programmatico sulla Sicurezza approvato dalla Giunta Municipale con deliberazione n. 112 dell'11 giugno 2004 e annualmente aggiornato, da ultimo con deliberazione di Giunta Municipale n. 48 del 13 aprile 2012.

**5. Scopo del sistema di videosorveglianza**

Lo scopo essenziale dell'installazione del sistema di video sorveglianza è quello di tutelare il patrimonio dei comuni nonché di garantire la tutela e la sicurezza dei cittadini e specificatamente:
- garantire una ordinata e civile convivenza nelle città e nel territorio di riferimento, anche con riguardo alla riduzione dei fenomeni di illegalità e inciviltà diffusa;
- garantire una maggiore prevenzione e controllo dei fenomeni importanti per la sicurezza della circolazione stradale, per la protezione ambientale, la tutela dei cittadini e per i bisogni emergenti;
- garantire una maggiore tutela e sicurezza della popolazione.

**6. Rispetto dei principi generali del Garante dell' 8 aprile 2010.**

*1. Rispetto del principio di liceità*

Il sistema di video sorveglianza rispetta il principio di liceità del trattamento in quanto è fondato su uno dei presupposti di liceità che il Codice prevede espressamente per il settore pubblico: lo svolgimento di funzioni istituzionali (articoli da 18 a 22 del d.lgs. 196/2003). Il sistema è infatti installato esclusivamente per le finalità summenzionate (si veda a tal proposito il precedente: 5. Scopo del sistema di videosorveglianza).

La videosorveglianza, inoltre, nel caso di specie avviene nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi: le vigenti norme dell' ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori).

È altresì palese il rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.

*2. Rispetto del principio di necessità*

Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e comunque di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Il principio di necessità è rispettato in quanto è escluso un uso superfluo e sono evitati eccessi e ridondanze. Infatti, il sistema informativo e il relativo programma informatico sono conformati in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi ed il software è configurato in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati (si veda nello specifico la sezione relativa alle caratteristiche tecniche del sistema).

*3. Rispetto del principio di proporzionalità*

Il principio di proporzionalità è rispettato poiché, nel commisurare la necessità di un sistema al grado di rischio presente in concreto, è stata evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza.

L'impianto di videosorveglianza è infatti stato attivato in quanto altre misure sono state ponderatamente valutate insufficienti o inattuabili.

L'attuale sistema di video sorveglianza è, quindi, lecito in quanto ha rispettato il C.d. principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento.

La proporzionalità è stata valutata in ogni fase o modalità del trattamento, per esempio quando si è dovuto stabilire:

- se fosse stato sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti;
- se fosse realmente essenziale ai fini prefissi raccogliere immagini dettagliate;
- la dislocazione, l'angolo visuale, l'uso di zoom automatici e le tipologie – fisse o mobili – delle apparecchiature;
- quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca di dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi;
- la durata dell'eventuale conservazione.

*4. Rispetto del principio di finalità*

Gli scopi perseguiti sono stati resi determinati, espliciti e legittimi. Il sistema di videosorveglianza è infatti volto esclusivamente al perseguimento di finalità di pertinenza del Corpo di Polizia Locale (si veda a tal proposito il precedente: 5. Scopo del sistema di videosorveglianza).

Sono in particolare perseguite finalità determinate e rese trasparenti, direttamente conoscibili attraverso adeguati cartelli di avvertimento al pubblico e riportate nell'informativa pubblicata sul sito

del Corpo Unico (se veda a tal proposito la sezione specifica relativa ai cartelli di avvertimento e all'informativa ai cittadini).

## 7. Caratteristiche tecniche del sistema di videosorveglianza

7.1 Sistema **tvcc vtr** apparecchiature elettroniche da adottare:

- Telecamera Dome Surveyor VFT Colore Day&Night ad Alta Sensibilità completa di Custodia da Esterno con Cupola Trasparente e relativi accessori per il montaggio Pendente.
- Telecamera in CCD da 1/4" Risoluzione orizzontale 540 linee, rapporto SIN >50 dB. Zoom Ottico Integrato 35X, Zoom Digitale 12X, Sensibilità 0,02 Lux. Dispone di 4 Contatti ingresso per il collegamento di Allarmi locali e un Relè di comando correlato. Gestione di 79 Preset, 8 Tour formati da 32 comandi, 2 AutoTour su Autoapprendimento.
- Gestione di Privacy Zone per mezzo di 16 Zone di Mascheramento. Real Time Clock Interno per la gestione della Data e Ora e della Schedulazione per un ottimale funzionamento in piena autonomia.
- Titolazione completa per Settori, Allarmi, Zone, ecc. compreso di trasformatore di alimentazione, staffa da muro ed adattatore ad angolo o palo.
- KLX-60 KN versione 5.2 Videoserver di rete per registrazione telecamere IP, dimensionato per la registrazione continua delle telecamere sopradescritte per un minimo garantito di 72 ore
- S500AG Ponte radio per trasmissione/ricezione.
- S600AG Ponte radio per trasmissione/ricezione per torre ripetitrice.
- Monitor LCD 19 " per armadio.
- Scwitcher 81N 10-100MB con alimentazione POE.
- Scheda rete TCP-I P per telecamera Domo
- Antenna Pac 1424-E

Si segnala che le telecamere potranno essere successivamente anche aumentate di numero, sempre ed esclusivamente per perseguire le finalità previste dal presente documento.

*7. 2. Tipologie di telecamere*

Le telecamere suddette possono essere di due tipologie: - videocamere fisse - videocamere mobili.

*7. 3. Tempo di conservazione delle immagini*

In applicazione del principia di proporzionalità le immagini vengono conservate per un periodo massimo di 7 giorni successivi, dopo di che vengono automaticamente cancellate dal sistema informatico.

*7. 4. Sala di controllo*

La sala di controllo dell'intera sistema di videosorveglianza è collocata pressa la sede della Centrale Operativa del Corpo della Polizia Locale. Solamente pressa tale sede è possibile visionare le immagini dell'intera sistema di videosorveglianza.

## 8. Misure di sicurezza

Presso la sede del Corpo della Polizia Locale sono state adottate le seguenti misure di sicurezza volte a ridurre al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta dei dati relativi alla videosorveglianza.

*Sicurezza fisica*

Gli accessi sono controllati. L'accesso del personale avviene, solitamente, durante l'orario di lavoro. In casi eccezionali e per motivi esclusivamente lavorativi è consentito l'accesso anche al di fuori dei giorni stabiliti e dell'orario fissato.

È prevista la chiusura a chiave degli ingressi principali e la presenza costante del personale interna durante l'orario di lavoro.

In generale, sono adattate le seguenti prescrizioni:
- l'ingresso nei luoghi di lavoro è controllato e selezionato ed è consentito durante l'orario di apertura;
- fuori dagli orari di apertura al pubblica l'accesso alle singole strutture è permesso anche alle Società e Ditte e persone incaricate delle pulizie interne, dietro apposita autorizzazione scritta;
- i documenti contenenti dati personali sensibili sono custoditi in armadi o cassetti chiusi a chiave al termine dell'orario di lavoro o in caso comunque di allontanamento anche momentanea dal proprio Ufficio di tutti i dipendenti.

*Misure per prevenire rischi dipendenti da comportamenti degli operatori*

I rischi dipendenti da comportamenti dei soggetti incaricati dei trattamenti sono contrastati da misure di informazione e formazione degli operatori. A tutto il personale saranno consegnate delle regale di corretta gestione dei dati personali.

Sarà periodicamente verificata la corretta gestione e conservazione delle credenziali di autenticazione. I comportamenti fraudolenti sono perseguiti can le consuete misure di carattere disciplinare e prevenuti da attività di verifica e controllo riservata al Comandante della Polizia Locale o suo delegato.

*La privacy e gli strumenti utilizzati dalla polizia locale*

I possibili errori materiali sono prevenuti da criteri procedurali che prevedono controlli e verifiche.

*Trattamenti informatici*

*Funzione di autenticazione - Gestione delle password*

Il trattamento di dati personali con strumenti elettronici è consentito solo ai titolari dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione stabilite e previste consistono in un codice per l'identificazione di ciascun incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

Sono attribuite una o più credenziali per l'autenticazione per l'accesso ai vari programmi. Sono state impartite agli incaricati le dovute istruzioni affinché ciascuno adotti le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso e di uso esclusivo.

Ciascuna parola chiave prevista dovrà essere, di norma, composta da almeno otto caratteri alfanumerici. Nel caso in cui lo strumento elettronico non lo permetta, la parola chiave sarà composta da un numero di caratteri pari al massimo consentito. Essa non potrà contenere riferimenti agevolmente riconducibili all'incaricato e dovrà essere modificata da quest'ultimo almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave dovrà essere modificata almeno ogni tre mesi.

Se possibile, la scadenza delle password sarà comunicata automaticamente dal sistema informatico tramite sistema di gestione temporizzato.

In caso di prolungata assenza o impedimento dell'incaricato (malattia, ferie, aspettativa, ecc.) che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il titolare e/o il responsabile potrà assicurare la disponibilità di dati o strumenti elettronici previa richiesta dell'incaricato che necessita tale disponibilità.

Gli incaricati sono stati avvertiti di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi saranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali saranno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

*Sistema di autorizzazione*

Per gli incaricati possono essere individuati profili di autorizzazione di ambito diverso

attraverso un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Ad ogni utente vengono associati uno o più profili che sono stati specificati prima del trattamento.

Gli utenti sono diversificati a seconda del profilo: ad esempio consultazione, consultazione ed elaborazione, accesso totale (amministratore di sistema).

Periodicamente, e comunque almeno annualmente, sarà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

La gestione di autenticazione e profili per ogni singolo incaricato viene valutata dal responsabile settore informatico in base alle necessità che il singolo incaricato ha di accedere ai dati - svolgimento delle funzioni e dei compiti che gli sono affidati.

## 9. **Cartelli di avvertimento e informativa ai cittadini**

I cittadini sono stati opportunamente informati della presenza della zona di videosorveglianza per il tramite di apposita cartellonistica conforme ai dettami previsti dal Garante. Il supporto con l'informativa, in particolare, è stato collocato all'ingresso delle aree sottoposte a videosorveglianza e sono stati previsti un formato ed un posizionamento tali da essere chiaramente visibili.

Si segnala inoltre che sul sito internet del Corpo di Polizia Municipale verrà pubblicata un'informativa ai cittadini contenente le specificazioni previste all'articolo 13 del d.lgs. 196/2003.

## 10. Responsabili e incaricati del trattamento e persone autorizzate ad accedere al sistema

Sono stati designati per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e nei casi in cui si è ritenuto indispensabile per gli scopi perseguiti, visionare le registrazioni, è stato previsto un numero molto ristretto di soggetti a ciò autorizzati. Sono inoltre stati previsti diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione.