COMUNE DI BIANZE’

GDPR UE 679/2016

DISCIPLINARE INTERNO SULL’UTILIZZO ATTREZZATURE INFORMATICHE

REV. 1.0 DEL 04/10/2022

GLOSSARIO

***I*nternet**: è la rete mondiale per la trasmissione dati che collega i server pubblici di società, enti pubblici, istituzioni, organizzazioni, soggetti privati.
Lan: Local Area Network, rete dati che interconnette le apparecchiature informatiche all'interno di un'organizzazione
Password: parola di sicurezza, è normalmente abbinata alla userid (utente) per formare le credenziali di autenticazione
Account: è quell'insieme di funzionalità, strumenti e contenuti attribuiti ad un utente ed è il meccanismo attraverso il quale il sistema informatico gli mette a disposizione un ambiente con contenuti e funzionalità (dati e programmi), isolandolo dalle altre utenze. Vi si accede attraverso le credenziali di autenticazione (riconoscimento): nome utente e password.
Dominio: entità logica che individua un insieme di risorse comuni (file, cartelle, programmi), gestite da uno o più server, il cui accesso avviene mediante l'account
Virus informatico: programma informatico che, all'insaputa dell'utente, può compromettere in varia misura il pc, i programmi ed i dati su di esso ospitati
Backup: procedura di salvataggio dei dati e programmi su supporti magnetici a lunga durata ed alta capacità (tipicamente cassette a nastro)
Dischi di rete: supporti di memorizzazione di massa accessibili attraverso la rete dati e non fisicamente collocati sul pc dell'utente
Server: elaboratore dotato di particolari caratteristiche hardware (memoria, potenza del processore, affidabilità dei componenti, alimentazione) in grado di sopportare grossi carichi di lavoro e garantire continuità operativa
File server: server dedicato alla memorizzazione dei file degli utenti (dati e programmi) in modo centralizzato attraverso l'uso della rete dati
Proxy server: server dedicato a gestire e intermediare gli accessi ad Internet per conto dei pc residenti sulla lan comunale.
Log file: file di registrazione di eventi (es. accessi Internet) gestito da un server
Notebook: computer portatile (a volte chiamato anche “laptop”)
Netebook: computer portatile caratterizzato da dimensioni e peso ridotti e maggiore portabilità
Chiavette USB: dispositivi portatili che vengono inseriti in apposite porte disponibili sui pc sia fissi che portatili, sono normalmente dispositivi di memorizzazione dati (in sostituzione degli ormai obsoleti floppy disk), ma possono anche essere dispositivi di collegamento a reti senza fili (wireless) quali Bluetooth e WiFi, e altro ancora
Webmail: modalità di accesso ad una casella di posta elettronica attraverso pagine web, mediante l'uso di un browser (Firefox, Internet Explorer)
Black list: elenco di siti web il cui accesso è bloccato dal proxy server
White list: elenco dei soli siti web ammessi alla navigazione dal proxy server
Timeout: intervallo di tempo che definisce una scadenza di validità (di connessione, di password,...)

INTRODUZIONE

All’interno delle disposizioni che un Ente deve darsi per tutelare la sicurezza e la privacy dei dati da essa trattati, riveste una particolare importanza il corretto utilizzo delle attrezzature informatiche che l’Amministrazione mette a disposizione dei propri dipendenti sia che si tratti di dispositivi fissi collocati presso gli uffici e i luoghi di lavoro sia che si tratti di dispositivi mobili o di possibilità di accesso alla rete aziendale da remoto.

L'espansione dell'uso di personal computer negli uffici del Comune di Bianzè ha portato con sé un sempre maggiore numero di persone che interagiscono, attraverso le varie applicazioni software, con dati personali e sensibili.
Per questo serve una doverosa presa di coscienza da parte di tutti che la sicurezza dei dati passa dalla definizione, adozione e rispetto di regole di comportamento in grado di salvaguardare il patrimonio informativo del Comune di Bianzè da minacce che di giorno in giorno si fanno sempre più pericolose. I controlli sull'uso degli strumenti informatici, devono garantire il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy e proteggere il sistema informatico del Comune di Bianzè, essendo i computers strumenti di lavoro e la cui utilizzazione personale è preclusa.
Uno dei canali che maggiormente veicola minacce di tipo informatico (genericamente poste sotto il nome di virus informatici) è Internet tramite l'accesso ai siti web, l'uso della posta elettronica, programmi per la messaggistica istantanea (chat), programmi per la videoconferenza e lo scambio di file, ecc...
Si deve riconoscere, per altro, che l'uso di Internet rappresenta un'incredibile opportunità per migliorare il lavoro quotidiano e la sua efficienza, ad esempio ciò che prima veniva fatto con la carta, oggi lo si può fare con documenti informatici scambiati attraverso l'email. Anche sul fronte dell'informazione Internet ha aperto opportunità di conoscenza enormi attraverso l'uso di siti di ricerca, banche dati online, quotidiani e riviste online, siti tematici specializzati sui più svariati temi. Con tutto questo sono anche arrivate nuove modalità di contatto ed aggregazione attraverso l'uso delle comunità virtuali (Facebook, Twitter, Google+, Linkedin...) e siti web di proposta/condivisione di contenuti (YouTube, Flikr, Twitter,...).
La stessa comunicazione istituzionale e promozionale del A.T.O. N° 2 non può più ignorare l'uso del web come canale informativo per i cittadini, altri enti e la Pubblica Amministrazione in genere, infatti l'azione legislativa dei recenti Governi ha sempre più spinto verso l'uso dello strumento di Internet per migliorare i servizi e migliorarsi internamente (siti istituzionali, uso della posta elettronica tradizionale e certificata, servizi online per i cittadini, adozione di tecnologie per la dematerializzazione,...).
Questa dualità opportunità/pericolo rappresentata dalle nuove tecnologie deve essere correttamente governata sia attraverso l'impiego di adeguate tecnologie per la sicurezza che mediante l'adozione di comportamenti consapevoli da parte degli utilizzatori (si ricorda che circa l'80% delle compromissioni alla sicurezza derivano da comportamenti scorretti, consapevoli o inconsapevoli, del personale interno alle aziende e solo il 20% delle minacce proviene direttamente dall'esterno).

PRINCIPI GENERALI

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo del Comune di Bianzè deve sempre ispirarsi al principio della diligenza e della correttezza. Tali comportamenti devono sempre essere adottati dai dipendenti nell'ambito del rapporto di lavoro e da qualsiasi persona, a prescindere dal rapporto contrattuale intrattenuto con la stessa (collaboratori, consulenti, operatori esterni, amministratori...), che venga autorizzata all'uso di tali risorse.

I due capisaldi su cui si fondano le regole esposte nella presente policy informatica sono:
• è VIETATO ogni utilizzo di apparecchiature informatiche, di personal computer, delle reti e di dati, diversi dai fini strettamente istituzionali;

• deve essere evitato qualsiasi comportamento che possa minare l'integrità del patrimonio informativo comunale e provocare danni al sistema informatico nel suo complesso.

Per garantire quanto sopra, ciascun dipendente o collaboratore che abbia in utilizzo le apparecchiature informatiche del Comune di Bianzè, deve sottostare al seguente Codice di Comportamento:

1 USO DEL PERSONAL COMPUTER E DELLA RETE (MSUSI-1)

1.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

1.2 Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Bianzè solo attraverso specifiche credenziali di autenticazione.

1.3 A ciascun lavoratore è fatto esplicito divieto di:

- modificare qualsiasi caratteristica *hardware* e *software* impostata sul proprio *personal computer*, dal sistemista di rete o dal Responsabile dei Sistemi Informativi del Comune salvo preventiva autorizzazione scritta da parte del Responsabile dei Servizi Informativi;
- installare e/o eseguire qualsiasi tipologia di programmi informatici diversi da quelli autorizzati e contenuti nell'allegato alle Misure Minime di Sicurezza, anche nel caso in cui si tratti di *software* opportunamente licenziato, di *software* in prova (c.d. "*shareware*"), ovvero di *software* gratuito e liberamente scaricabile da Internet (c.d. "*freeware*") senza il preventivo assenso scritto del Responsabile dei Servizi Informativi che provvederà ad aggiornare l'allegato dei software autorizzati; è consentita a ciascun dipendente autorizzato, l'installazione di release di aggiornamento dei software già previamente autorizzati e già installati;
- prelevare da Internet, copiare e/o archiviare sul *personal computer* qualsiasi genere d'informazioni (come, a mero titolo esemplificativo e non esaustivo, *file* audio, video, eseguibili, ecc.) non necessarie all'attività lavorativa;
- utilizzare qualsiasi tipologia di supporti di archiviazione removibile o di tecnologia di comunicazione per la memorizzazione o l'invio verso l'esterno di informazioni inerenti il rapporto di lavoro, se non a fronte di comprovate esigenze di servizio;
- lasciare incustodito e accessibile per periodi prolungati il proprio pc, anche solo dovuti all'assenza dall'Ufficio per partecipazione a riunioni o sopraluoghi esterni senza l'apposizione del blocco schermo, ovvero cedere a soggetti terzi e non autorizzati il proprio *personal computer*, soprattutto successivamente al superamento della fase di autenticazione;
- eliminare la richiesta di *password* per il salvaschermo (*screensaver*), impostata automaticamente in caso di prolungata inattività da parte del lavoratore sulla sua postazione di lavoro, al fine di evitarne un utilizzo improprio in caso di assenza anche temporanea.

1.4 Fatte salve particolari esigenze tecniche o lavorative, le postazioni di lavoro, inoltre, devono essere spente al termine della giornata lavorativa e poste in blocco attività nella pausa pranzo.
Nella pausa pranzo quando la postazione è posta in blocco, l'utente dovrà avere cura di uscire da tutte le applicazioni aperte, sia ai fini di ulteriore sicurezza poiché l'accesso alle applicazione richiede esso pure un login e una password e sia al fine di consentire nella pausa pranzo le eventuali attività di aggiornamento degli applicativi o l'esecuzione di scansioni programmate da parte dal Responsabile Sicurezza Sistemi informativi (Amministratore di sistema)

1.5 Il Responsabile dei sistemi informativi (Amministratore di sistema) è autorizzato ad accedere in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento dell'utente. La presente attività può essere messa in atto unicamente per finalità di sicurezza e di controllo del corretto comportamento ma in nessun caso può essere attuata per controllare le attività dell'utente.

1.6 Il Responsabile dei sistemi informativi (Amministratore di sistema) è autorizzato a collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, anche senza autorizzazione dell'utente, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utente e al Responsabile dei servizi informativi (Amministratore di sistema)

1.7 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal Responsabile dei sistemi informativi né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
L'inosservanza della presente disposizione espone lo stesso Comune di Bianzè a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente. In tale caso la sanzione verrà applicata all'utente che ha violato il divieto di installazione.
1.6 Salvo preventiva espressa autorizzazione del Responsabile dei Servizi informativi (Amministratore si sistema) non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

2. UTILIZZO DI PC PORTATILI (MSUSI-2)

2.1 Il Comune di Bianzè dispone di n. 2 notebook , installati e configurati come normali pc di rete .
L'utente a cui è affidato in uso un pc portatile è responsabile del personal computer portatile eventualmente assegnatogli dall'Amministrazione e deve custodirlo pertanto con diligenza, sia durante gli spostamenti che nel corso del normale utilizzo.
Ai personal computer portatili si applicano tutte le regole di utilizzo previste per i personal computer.
Durante l'utilizzo all'esterno dell'ente il computer portatile non deve mai essere lasciato incustodito e deve essere adeguatamente preservato nei luoghi e con i mezzi più idonei per la sua ottimale protezione.
Al suo interno, inoltre, devono essere immagazzinate le informazioni strettamente necessarie all'attività che si svolge al di fuori del Comune, onde limitare la perdita di informazioni aziendali in caso di danno, smarrimento o furto.
In caso di furto o smarrimento, l'utente assegnatario del personal computer ha l'obbligo d'informare tempestivamente il titolare del trattamento dei dati e o delegato e il Responsabile dei Servizi Informativi (Amministratore di sistema) , nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo all'Amministrazione, la copia dell'atto di denuncia.

3.GESTIONE DELLE PASSWORD E CREDENZIALI DI ACCESSO E DI AUTENTICAZIONE (MSUSI-3)

3.1 Accesso alla postazione di lavoro

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Responsabile servizi informativi (Amministratore di sistema) , previa formale richiesta del Responsabile dell'ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Nel caso di collaboratori a progetto e coordinati e continuativi e/o altri collaboratori saltuari, la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Responsabile dell'ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.
L'accesso ad ogni postazione di lavoro informatica è governato da un sistema d'identificazione personale basato sull'utilizzo di credenziali di accesso (consistenti in username e password), che ne permettono l'utilizzo nei modi e nelle forme definite da ciascun profilo aziendale esclusivamente al lavoratore autorizzato.
Le credenziali di accesso sono e devono essere conosciute esclusivamente dal soggetto per il quale sono state predisposte.
La parola chiave (password), così come previsto dalla legge, deve essere composta da almeno 13 (tredici) caratteri alfanumerici (lettere minuscole, maiuscole e numeri), e caratteri "speciali".
Ci sono alcune **regole d'oro** da seguire quando si imposta la parola di accesso di un account:

- creare password lunghe con almeno 13 caratteri
- alternare lettere, numeri, punteggiatura e altri simboli, ad esempio _*@%,#,$,& – in questo modo sarà più difficile per gli hacker decriptare la tua parola chiave
- usare lettere minuscole e maiuscole
- non scegliere come password parole comuni e informazioni pubbliche facilmente reperibili online
- usare password casuali per evitare che gli algoritmi degli hacker scoprano le tue credenziali in modo automatico.

Non deve contenere, inoltre, riferimenti direttamente riconducibili al lavoratore e deve essere obbligatoriamente rimpiazzata al suo primo utilizzo e, successivamente, almeno ogni 3 (tre) mesi.

Soggetto preposto alla custodia delle credenziali del Comune di Bianzè è il Segretario Comunale, il quale è l'unico soggetto autorizzato al reset della password in caso si renda necessario accedere alla postazione dell'utente per estrema necessità in caso di sua assenza o a seguito di dimenticanza della password corretta.

3.2 Accesso al sistema di gestione aziendale

Gli applicativi del Comune di Bianzè sono gestiti per mezzo della piattaforma DigitalPal la quale raggruppa tutte le procedure informatiche Siscom, con le seguenti eccezioni.

a) L'Anagrafe Nazionale della Popolazione Residente è il progetto di anagrafe unica a livello nazionale che raccoglie i dati e i servizi demografici dei cittadini residenti in Italia e iscritti all'AIRE. Oltre ad evitare duplicazioni nelle informazioni, grazie ad ANPR i cittadini possono verificare e chiedere una rettifica dei propri dati demografici e fruire dei servizi anagrafici in un unico luogo, indipendentemente dal comune di residenza.
b) del software di gestione delle contravvenzioni del servizio di vigilanza licenziati da MAGGIOLI spa;
c) del software di gestione tributi licenziato dalla Ditta Servizi Locali
d) del software di gestione pratiche edilizie licenziato da Technical Designer – GISMASTER
e) Piattaforma online Servizi Locali Spa per la gestione dei tributi. La parte che vedono i cittadini si chiama Bianzè Digitale. Tale piattaforma gestisce certificati anagrafici, catasto, pagamento e rimborsi, dichiarazioni online. Gestisce TARI, IMU, TASI E CANONE UNICO (EX TOSAP)

L'accesso alla piattaforma degli applicativi Siscom è gestito attraverso Siscmaster, governato da un sistema d'identificazione personale basato sull'utilizzo di credenziali di accesso (consistenti in username e password), che ne permettono l'accesso esclusivamente al lavoratore autorizzato.

Il sistema Siscmaster, attraverso l'identificazione dell'utente con il proprio user id e password abilita i singoli utenti alle diverse procedure in base alla autorizzazioni previste a monte dal Responsabile dei sistemi informativi (SISCOM).

Esiste un doppio sistema di autorizzazione all'utilizzo di procedure e di attività regolamentate in primo livello dalle autorizzazione legate alla password di accesso a Siscmaster e in secondo livello dalle autorizzazioni legate alle password di accesso ai vari applicativi.

Per questo motivo ciascun utente è tenuto ad accedere al programma Siscmaster unicamente a mezzo di proprio user id e password.

Le password di accesso a SISCMASTER devono avere minimo 14 (quattordici) caratteri alfanumerici di cui almeno uno speciale.

4. UTILIZZO DELLA RETE INTERNA AZIENDALE

4.1 Per l'accesso alla rete del Comune di Bianzè , ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
4.2 La rete telematica aziendale è l'insieme delle tecnologie – apparati e programmi – mediante i quali si realizza la connettività interna tra i vari componenti del sistema informatico aziendale.
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi da quelli per cui sono state predisposte.
Pertanto, qualunque applicazione o file ad essa correlato che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in dette unità di rete.
Su di esse, inoltre, vengono regolarmente svolte attività di controllo, amministrazione e backup da parte del Responsabile sicurezza sistemi informativi (Amministratore del Sistema).
Alla luce di ciò, è fatto esplicito divieto di:

- utilizzare la rete interna aziendale per fini non espressamente previsti e/o autorizzati;
- connettere in rete locale apparecchiature elettroniche (PC, stampanti, ecc.) o altri qualsiasi altro genere di apparato che possa alterare la configurazione della rete interna e/o danneggiare le applicazioni.

Portare particolare attenzione all'utilizzo di dispositivi USB (hard disk e memory pen) , poiché devono essere controllate prima dell'utilizzo da un software antivirus opportunamente configurato dall'amministratore di sistema.
4.3 Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio preimpostato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.
4.4 Il Responsabile dei sistemi informativi o il responsabile della gestione della rete possono in qualunque momento procedere alla rimozione di ogni file o applicazione che verranno ritenuti essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente o Responsabile dei sistemi informativi provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
4.5 L'accesso alle risorse informatiche del Comune di Bianzè da parte di Ditte e/o Fornitori esterni, viene concesso previa valutazione dei Rischi ed attraverso l'implementazione e l'uso di sistemi di controllo.

5. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI (MSUSI-4)

5.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti knowhow dell'Ente, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
5.2 I supporti magnetici contenenti dati sensibili DEVONO essere adeguatamente custoditi in armadi chiusi.
E' vietato l'utilizzo di supporti rimovibili personali.
L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

6 USO DELLA POSTA ELETTRONICA (MSUSI-5)

6.1 La casella di posta elettronica assegnata del Comune di Bianzè è uno strumento di lavoro.
Coloro i quali sono assegnatari di una o più caselle di posta elettronica, pertanto, sono responsabili del loro corretto utilizzo.
6.2 Il Comune di Bianzè , pur proteggendo con gli opportuni software i sistemi di gestione delle caselle email da messaggi potenzialmente pericolosi, fa comunque esplicito divieto a tutti gli utenti di:
- utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, ecc., salvo diversa ed esplicita autorizzazione;
- utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi completamente estranei al rapporto di lavoro o alle interrelazioni lavorative tra colleghi;
- aprire email e/o soprattutto gli allegati provenienti da mittenti sconosciuti o che abbiano anche solo un contenuto insolito; in caso di dubbio è fatto obbligo di avvisare preventivamente il Responsabile dei Servizi Informativi, che darà istruzioni in merito;
- inviare o dar corso a catene telematiche di messaggi (anche dette "Catene di Sant'Antonio").

6.3 Le e.mail spedite e ricevute debbono essere conformi, nella forma e nei contenuti, agli standards aziendali prefissati e dovrà essere utilizzato il software di gestione Olimpo (di Siscom) per la ricezione delle mail . Per l'invio è possibile utilizzare Olimpo per quelle che passano dal protocollo e Outlook per le altre .
6.4 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
6.5 Per evitare di accedere alla casella di posta elettronica personale, sono stati creati gli indirizzi di servizio @ruparpiemonte.it - @legalmail.it e @comune.bianze.vc.it che garantiscono a più persone di ricevere lo stesso messaggio.
6.6 Il Responsabile dei sistemi informativi (Amministratore di sistema), nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potranno accedere alla casella di posta elettronica dell'utente in caso di sua prolungata assenza.

7 NAVIGAZIONE IN INTERNET (MSUSI-6)

7.1 La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile e il *personal computer* abilitato alla navigazione costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.

Un suo utilizzo indiscriminato, però, può rendere il Comune di Bianzè vulnerabile sotto il profilo della sicurezza.
Alla luce di ciò, il Comune di Bianzè, anche per limitare il più possibile i controlli, ha adottato alcune misure ritenute opportune per proteggere i propri sistemi elettronici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.
In particolar modo, ha:

- individuato le categorie di siti considerate non correlate con la prestazione lavorativa;
- impedito la navigazione su detti siti attraverso l'utilizzo di un sistema di filtri sulla navigazione e sulle attività ritenute potenzialmente dannose (ad es., *download* e/o *upload* di *file* o *software* aventi particolari caratteristiche, per dimensione o per tipologia di dato);
- predisposto nel tempo la conservazione dei dati strettamente limitati al perseguimento di finalità organizzative, produttive e di sicurezza.

7.2 L'utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e, più in generale, delle modalità con cui opera.
7.3 Il prelievo (*download*) di immagini, di file audio o musicali, di file video e in ogni caso di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri lavoratori non è in alcun modo consentito.
7.4 All'utente, pertanto, non è concesso di:

- servirsi o dar modo ad altri di servirsi della stazione di accesso ad Internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalle norme vigenti;
- scaricare da Internet qualsiasi tipo di *software*; eventuali necessità devono essere appositamente richieste per iscritto al Responsabile del Servizi Informativi;
- utilizzare *Internet Provider* diversi da quello ufficiale predisposto dalla Società e connettere la propria stazione di lavoro aziendale alle reti di tali *Provider* con sistemi di connessione diversi da quello centralizzato (ad es. attraverso *modem*, *internet key*, ecc.);
- usare la rete in modo difforme da quanto previsto dalla presente *Policy* e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete Internet.

7.5 L'Amministrazione si riserva comunque il diritto di memorizzare in appositi registri automatizzati (*log file*) i link delle pagine accedute attraverso la rete Internet, nelle forme e secondo le modalità esplicitate di seguito nella presente *Policy.*

8 PROTEZIONE ANTIVIRUS (MSUSI-7)

8.1 Ogni lavoratore deve tenere comportamenti atti alla cooperazione fattiva con l'Amministrazione per ridurre al minimo il rischio di attacchi ai sistemi informatici aziendali attraverso software malevolo (ad es.,worm, virus, trojan, ecc.) e, più in generale, attraverso l'azione di programmi di cui all'art. 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.
8.2 Ogni utente e o amministratore, pertanto, è tenuto a:

- controllare la presenza e il regolare funzionamento del software antivirus installato sulla propria postazione;
- segnalare prontamente al Responsabile dei Servizi Informativi (Amministratore di sistema) il caso in cui il software antivirus non riesca automaticamente ad eliminare la minaccia dai sistemi aziendali;

- verificare con il software antivirus, prima dell'apertura di qualsiasi file, ogni dispositivo (ad es., chiavette USB, DVD, CD, hard disk esterni, ecc.) proveniente dall'esterno della nostra struttura e il cui utilizzo sia stato anteriormente autorizzato dal Responsabile dei Servizi Informativi.

8.3 Il Comune di Bianzè si riserva il diritto di installare su ogni postazione di lavoro elettronica i programmi che impediscano l'installazione e la diffusione di software potenzialmente dannoso per la sicurezza della rete aziendale.
La rimozione arbitraria di detti programmi è assolutamente vietata.
8.4 Il Comune di Bianzè deve pianificare su tutti i pc una scansione programmata che verrà eseguita settimanalmente.
Qualora l'antivirus segnali anomalie di presenze di virus l'operatore deve segnalarlo al Responsabile dei sistemi informativi (Amministratore di sistema) . Si dovrà aver cura di verificare che, ove sia stata rilevata la presenza di un virus, lo stesso sia stato rimosso o posto in quarantena.

9. UTILIZZO DEL SISTEMA DI TELEFONIA (MSUSI-8)

9.1 L'Amministrazione utilizza un sistema di telefonia per gestire le conversazioni telefoniche sia all'interno dell'Ente che verso la rete telefonica tradizionale e cellulare.
L'utilizzo del sistema è autorizzato esclusivamente per soli scopi lavorativi, anche se un modestissimo e oculato utilizzo per scopi personali è comunque tollerato.
9.2 L'Amministrazione si riserva il diritto di utilizzare sistemi elettronici volti a verificare il livello di spesa delle utenze telefoniche assegnate e l'analisi delle direttrici di chiamata, senza però svolgere un'attività di monitoraggio dei numeri chiamati e della durata delle conversazioni, in ottemperanza a quanto previsto dall'art. 4 della Legge n. 300/1970 (Statuto dei lavoratori).

10. UTILIZZO DI APPARATI PER LA TELEFONIA MOBILE (MSUSI-9)

10.1 Ogni lavoratore che sia assegnatario di un telefono cellulare ovvero di qualsiasi dispositivo per la telefonia mobile, ivi comprese anche le sole schede SIM, ha l'obbligo di utilizzare detti strumenti esclusivamente per scopi intimamente connessi all'attività lavorativa e alle motivazioni che hanno spinto l'Amministrazione a questa specifica dotazione, salvo espressa e motivata autorizzazione e abilitazione all'utilizzo nella forma del dual bind.
10.2 Al fine di evitare qualsivoglia accesso e utilizzo indesiderato o illecito, è fatto obbligo che ciascun dispositivo venga protetto dal suo utilizzatore quantomeno attraverso un codice PIN ovvero una parola chiave (*password*).
10.3 Al momento della restituzione, l'utilizzatore ha l'obbligo di cancellare qualsiasi informazione registrata all'interno del dispositivo, ivi compresi, a titolo esemplificativo e non esaustivo, nomi e cognomi, numeri di telefono, messaggi, fotografie, video e quant'altro sia conservato al suo interno.
10.4 È fatto obbligo che ciascun dispositivo venga custodito con estrema diligenza.
10.5 In caso di furto o smarrimento, l'utente assegnatario del dispositivo ha l'obbligo d'informare tempestivamente il proprio diretto Responsabile e il Responsabile dei Servizi Informativi, nonché di denunciare tempestivamente l'accaduto alle Forze dell'Ordine, fornendo all'Amministrazione la copia dell'atto di denuncia.

11. SISTEMA DI BACKUP DATI (MSUSI-11)

11.1 Il backup dei dati comunali attualmente viene effettuato in modalità automatico pianificata giornaliera su NAS esterno.
11.2 Il backup del sistema "Siscom" viene effettuato anche quotidianamente su "Cloud" attraverso l'utility AhsayObm impostata sul ServerApp

11.2 Il controllo dei dati comunali viene fatto tutti i venerdi' dall'amministratore di sistema, che in caso di anomalie hardware o procedurali segnalerà la disfunzione al titolare del trattamento dei dati a mezzo mail

11.3 E' da prevedere, poiché non esistente un sistema di Disaster Recovery.

COMUNE DI BIANZE’

GDPR UE 679/2016

DISCIPLINARE INTERNO SULLE MISURE SULLA SICUREZZA E COMPORTAMENTO DEL PERSONALE

REV. 1.0 DEL 04/10/2022

PREMESSA

Le misure di sicurezza tecniche e organizzative si configurano come norme comportamentali e organizzative che devono essere pienamente e totalmente rispettate all'interno della struttura per garantire una corretta ed efficace protezione dei dati personali trattati dall'Ente. Tutti i soggetti che intrattengono a qualsiasi titolo (dipendenti , amministratori, collaboratori) rapporti con l'Ente e sono potenziali gestori o utilizzatori di dati personali sono tenuti a rispettare costantemente e rigorosamente le istruzioni, gli obblighi e i divieti contenuti nel presente disciplinare e hanno il dovere di segnalare ogni situazione di dubbia interpretazione, ogni violazione di cui vengano a conoscenza delle norme qui contenute e qualsiasi altro elemento di pericolo per la violazione dei dati personali che non sia stato preso in considerazione nel presente documento.

1.DISCIPLINARE DELLE MISURE DI SICUREZZA ORGANIZZATIVE

1 RIUNIONI PERIODICHE IN MATERIA DI SICUREZZA (MSO-1)

1.1 Il Comune di Bianzè garantisce una particolare attenzione alle misure di sicurezza attraverso una programmazione periodica di riunioni tra le figure di vertice dell'Ente e tra le figure di vertice e tutti i dipendenti al fine di garantire che tutto il personale sia costantemente informato sulle novità legislative od operative che possono interessare la sicurezza e la tutela dei dati personali dei dipendenti stessi, dei cittadini e di tutti i dati gestiti e presenti all'interno della struttura.

1.2 Viene stabilita una cadenza semestrale anche per le riunioni periodiche da effettuarsi con il DPO per verificare insieme la presenza di eventuali criticità nella sicurezza della gestione dei dati o la necessitò di procedere a rettifiche o adeguamenti o correzioni in alcune modalità operative e gestionali.

1.3 Il personale neo assunto dovrà seguire, entro un mese dall'assunzione in servizio, un corso di formazione tenuto dal Responsabile dei servizi informativi dell'Ente nel quale dovrà essere edotto di tutte le norme contenute nel dossier privacy a tutela e protezione dei dati personali gestiti dall'ente oltre ad essere edotto sulle norme di comportamento e condotta a cui i dipendenti pubblici e in particolare i dipendenti del Comune di Bianzè devono sottostare.

2 INFORMAZIONE E FORMAZIONE AI RESPONSABILI, AGLI INCARICATI E A TUTTI I DIPENDENTI (MSO-2)

2.1 Il Comune di Bianzè ha individuato la figura del D.P.O (Data Protection Officer) con funzioni di organizzazione e coordinamento delle attività necessarie a consentire che il Comune sia considerato in regola con la normativa europea sulla Privacy. E' compito del D.P.O organizzare riunioni periodiche di formazione rivolte agli incaricati e a tutti i dipendenti, come da suo specifico "Incarico" con finalità di:

a) far conoscere e accertarsi che tutti siano a conoscenza della responsabilità, dei doveri e delle misure da seguire per garantire la tutela dei dati personali da parte del Comune di Bianzè nei confronti di tutti i soggetti di cui il Comune gestisce o detiene i dati.
b) impartire istruzioni affinchè sia garantito l'aggiornamento della modulistica utilizzata da tutti gli uffici con rispetto alla normativa europea sulla privacy.
c) assicurarsi che tutti gli uffici, nel momento in cui gestiscono o trattano dati personali procedano alla messa a conoscenza della informativa privacy gli utenti.
d) formare e informare tutti gli uffici, i servizi e gli incaricati, sulla necessità di rispettare le norme privacy sulla tutela e protezione dei dati personali anche nelle procedure web eventualmente attivate.

3 AGGIORNAMENTO PERIODICO DELLE PROCEDURE E DELLE ISTRUZIONI OPERATIVE SU COME LAVORARE PER GARANTIRE LA TUTELA, PROTEZIONE E SICUREZZA DEI DATI IN RELAZIONE A NOVITÀ LEGISLATIVE E NUOVI ADEMPIMENTI (MSO-3)

3.1 E' compito del Titolare del trattamento dei dati garantire l'aggiornamento periodico delle procedure e impartire eventuali direttive in merito alla necessità di modificare le istruzioni operative previgenti necessarie a garantire la tutela, la protezione e la sicurezza dei dati in occasione di novità legislative, nuovi adempimenti richiesti, nuovi procedimenti o attività attivate o nuove procedure software utilizzate.

4 PREDISPOSIZIONE E AGGIORNAMENTO DEI REGOLAMENTI SULLA GESTIONE DELLE ATTIVITÀ DI EVENTUALI ATTIVITA' DI VIDEOSORVEGLIANZA (MSO-4)

4.1 E' compito del Responsabile della Videosorveglianza (Responsabile della gestione associata del servizio di Polizia locale) curare l'aggiornamento dei regolamenti interni sulla gestione delle attività inerenti la videosorveglianza.

4.2 I Regolamenti sulla videosorveglianza dovranno essere predisposti ed aggiornati in base alla normativa specifica di riferimento nel rispetto della tutela dei dati personali delle persone oggetto delle riprese e nel rispetto della tutela dei diritti dei lavoratori per quanto riguarda la videosorveglianza nei locali interni dell'asilo nido o in altri locali interni che eventualmente venissero posti sotto sorveglianza.
4.3 E' compito del Responsabile della Videosorveglianza accertarsi che sia esposta la necessaria cartellonistica informativa che renda noto all'utenza e ai soggetti la presenza di zone videosorvegliate.
4.4 Dovrà essere sempre reso noto il nominativo del Responsabile della videosorveglianza per eventuali reclami o richieste.

5 AGGIORNAMENTO PERIODICO DELLA MODULISTICA AI CAMBIAMENTI LEGISLATIVI, AGGIORNAMENTO PERIODICO DEL REGISTRO DEI TRATTAMENTI IN BASE AI PROCEDIMENTI AMMINISTRATIVI E AI DATI TRATTATI (MSO-5)

5.1 E' compito del Titolare del trattamento dei dati coordinare e disporre le attività anche con riferimento ai diversi uffici e servizi dell'ente affinchè la modulistica utilizzata sia adeguata ai cambiamenti legislativi, aggiornata e attuale e affinchè venga periodicamente aggiornato il Registro dei trattamenti in base ai procedimenti amministrativi adottati e alle tipologie di dati trattati.

5.2 A tal fine la modulistica e il registro dei trattamenti e il dossier privacy dovranno sempre contenere espresso riferimento alla versione, all'ultimo aggiornamento e alla data di aggiornamento.

6 RIORGANIZZAZIONE PERIODICA DELLE MODALITÀ DI CONSERVAZIONE DEI DOCUMENTI E DEI DATI INFORMATICI E CARTACEI (MSO-6)

6.1 Il Titolare del trattamento dei dati, coadiuvato dal D.P.O dovrà garantire la revisione periodica delle modalità di conservazione dei dati sia informatici che cartacei.

6.2 I dati trattati dovranno essere conservati unicamente per il periodo di tempo strettamente necessario e richiesto dalla normativa sugli archivi.

6.3 Una volta scaduti i termini di conservazione previsti dalla normativa sull'archiviazione, i dati personali di cui il comune è in possesso dovranno essere distrutti e resi inutilizzabili e illeggibili mediante distruzione dei documenti o cancellazione dei file che li contengono.

COMUNE DI BIANZE’

GDPR UE 679/2016

DISCIPLINARE INTERNO INERENTE LE MISURE DI ORGANIZZAZIONE DELLA SICUREZZA TECNICA E FISICA

REV. 1.0 DEL 04/10/2022

PREMESSA

Le misure di sicurezza tecniche e organizzative si configurano come norme comportamentali e organizzative che devono essere pienamente e totalmente rispettate all'interno della struttura per garantire una corretta ed efficace protezione dei dati personali trattati dall'Ente. Tutti i soggetti che intrattengono a qualsiasi titolo (dipendenti , amministratori, collaboratori) rapporti con l'Ente e sono potenziali gestori o utilizzatori di dati personali sono tenuti a rispettare costantemente e rigorosamente le istruzioni, gli obblighi e i divieti contenuti nel presente disciplinare e hanno il dovere di segnalare ogni situazione di dubbia interpretazione, ogni violazione di cui vengano a conoscenza delle norme qui contenute e qualsiasi altro elemento di pericolo per la violazione dei dati personali che non sia stato preso in considerazione nel presente documento.

1.DISCIPLINARE DELLE MISURE DI SICUREZZA TECNICHE

1 TUTELA DELLA PRIVACY ATTRAVERSO LA TUTELA DELLA STRUTTURA (MST1)

1.1 Il Comune di Bianzè garantisce e tutela la privacy delle informazioni e delle documentazioni presenti all'interno della struttura e gestite dal proprio personale attraverso i seguenti accorgimenti tecnico-organizzativi:

a) Obbligo di garantire la chiusura delle porte di accesso principali e secondarie alla struttura ogni qualvolta la struttura è chiusa al pubblico..
b) Possibilità di accesso alla struttura dalle porte principali o secondarie, nei momenti di chiusura al pubblico o al mattino o nel momento del rientro pomeridiano, in orario di entrata, unicamente a mezzo di chiavi di cui è dotato ciascun dipendente in servizio stabile presso il Comune di Bianzè oltre ad ogni amministratore
c) Garanzia della tutela e salvaguardia dei locali in assenza di personale, di notte, nei giorni festivi e negli orari notturni mediante sistema di allarme.
d) I dipendenti, esclusi i Responsabili, al di fuori del loro orario di lavoro, non sono autorizzati ad entrare all'interno della struttura se non previa autorizzazione scritta del Responsabile in caso di necessità di svolgimento di attività lavorativa straordinaria.
e) Le finestre e le tapparelle dei locali al piano terra dovranno essere chiusi a fine giornata lavorativa a cura del personale di ogni ufficio.
f) Esiste un sistema antifurto a codice che copre il piano terra Ufficio Vigili, primo piano Uffici Comunali e secondo piano. L'antifurto è collegato all'istituto di vigilanza privato.

2. TUTELA DELLA PRIVACY NEI SINGOLI UFFICI E NELLE POSTAZIONI DI LAVORO E AREE DI TRATTAMENTO (MST2- MST3- MST4- MST5)

2.1 E' auspicabile che, ove all'interno degli uffici non sia possibile conservare in armadi chiusi i documenti contenenti dati personali, si provveda a fine giornata a chiudere a chiave gli uffici **(MST2)**. Le chiavi di accesso agli uffici devono essere ufficialmente consegnate ai dipendenti comunali e agli amministratori, insieme con le chiavi dei cancelletti di sicurezza posti all'entrata, con apposito verbale di consegna.
Le chiavi di accesso agli uffici devono essere ufficialmente consegnate alla ditta di pulizie esterna insieme con le chiavi dei cancelletti di sicurezza posti all'entrata, con apposito verbale di consegna.

2.2 I Dipendenti e i collaboratori hanno l'obbligo di mantenere in ordine la propria postazione di lavoro (scrivanie, armadi, schedari, casseforti, archivi) oltre ad avere cura degli strumenti elettronici vari come PC, fotocopiatrici, stampanti. In particolare si dovrà avere cura di non lasciare in una posizione di facile accesso nessuna cartellina, fascicolo o documento che contenga dati personali oggetto di trattamento e tutelati dalla normativa sulla privacy **(MST5)**. Detti documenti, a trattamento terminato, devono essere riposti in luoghi sicuri e possibilmente chiusi o comunque non facilmente accessibili e consultabili se non a mezzo di sistemi fraudolenti. I documenti ridondanti o non più necessari devono essere distrutti e resi illeggibili a mezzo di distruggi documenti o comunque frantumazione degli stessi al fine di rendere impossibile il loro utilizzo. Gli armadi, gli schedari, gli archivi, quando possibile, devono essere tenuti chiusi a chiave a meno che non vi si acceda reiteratamente in lassi di tempo molto brevi per cui chiuderli a chiave creerebbe un disservizio; in questi casi è comunque necessario averne sempre il controllo visivo. Ove possibile, in ogni caso, vanno chiusi a chiave a fine giornata lavorativa. E' assolutamente indispensabile che siano chiusi a chiave almeno gli armadi contenenti dati sensibili (dai del personale, dati inerenti condizioni di salute, dati giudiziari ecc.) **(MST3).** La chiave degli armadi deve essere conservata a cura del titolare dell'ufficio.

2.3 Gli accorgimenti di cui sopra vanno seguiti anche in caso di assenza momentanea dalla propria postazione di lavoro, ove la stessa superi i 10 min. e non resti nessun altro collega all'interno dell'Ufficio. In tale caso va chiusa almeno la porta dell'ufficio.

2.4 Le aree ove si trovano uffici o postazioni di lavoro, archivi, sportelli, sale riunioni, sono soggetti, come i dati trattati, alla necessità di essere protetti. A tal fine l'accesso a tali aree è limitato agli incaricati al trattamento dei dati, ai Responsabili esterni e interni o a terzi, purchè identificati e autorizzati. All'interno di ciascun ambiente, nel normale orario lavorativo, deve sempre essere presente almeno un incaricato. Ove per esigenze particolari ciò non sia possibile, le porte degli uffici devono essere chiuse, così come devono essere chiuse le finestre, soprattutto se facilmente accessibili dall'esterno. Tutto ciò al fine di prevenire eventuali intrusioni finalizzate al furto o al danneggiamento di strumenti lavorativi e informazioni contenenti dati personali o sensibili o informazioni comunque che ricadano nella sfera della riservatezza di scelte politiche e programmatiche ancora in corso di esame **(MST4)**

2.5 La presenza di chiunque si trovi all'interno degli ambienti e/o utilizzi strumenti atti al trattamento senza essere stato identificato e previamente autorizzato, va subito segnalata al titolare del trattamento dei dati che prenderà i dovuti provvedimenti.

2.6 Non è consentito in genere a personale appartenente ad una specifica area e settore, accedere, a uffici appartenenti ad altra area o settore in assenza del titolare dell'ufficio o del Responsabile e tantomeno accedere ai documenti presenti e riposti in armadi.

3. TUTELA DELLA PRIVACY NEI CONFRONTI DEL PERSONALE ESTERNO ADDETTO ALLA PULIZIA DEI LOCALI E PERSONALE DI SERVIZIO PER MANUTENZIONI (MST6)

3.1 E' consentito l'accesso ai locali del Comune di Bianzè e ai singoli uffici da parte del personale incaricato del servizio di pulizia dei locali dipendente da ditta esterna anche in assenza di altro personale presso la struttura ove le esigenze di servizio richiedano che lo stesso venga svolto in orario della giornata di assenza del personale dipendente.

3.2 In tale caso il Responsabile della Ditta esterna dovrà fornire al Comune di Bianzè i dati e le generalità del personale da lui incaricato di accedere ai locali anche in assenza del personale comunale per l'effettuazione delle pulizie giornaliere o periodiche e dovrà garantire di aver comunicato al proprio personale l'obbligo di rispetto delle regole di riservatezza al momento dell'accesso ai singoli uffici e all'eventuale visione di documenti o fascicoli negli stessi collocati.

3.3 Nel caso si rendesse necessario l'accesso ai locali del Comune di Bianzè da parte di lavoratori o prestatori di servizi per attività di manutenzione, l'accesso dovrà essere effettuato solo ed esclusivamente alla presenza di personale dipendente e mai a struttura chiusa e non presidiata.

4. TUTELA DEI DATI CONTENUTI NELLA SALA SERVER (MST-07)

4.1 Il Server di rete del comune che contiene i dati informatici dell'ente dovrà essere accessibile unicamente dal responsabile sicurezza sistemi informativi (Amministratore di sistema) e alle persone appositamente individuate e incaricate dall'amministratore di sistema del Comune .

5. TUTELA DEI DATI RILEVATI E DELLE IMMAGINI VISIBILI DAL SISTEMA DI VIDEOSORVEGLIANZA (MST-08)

5.1 Il comune di Bianzè è dotato di tre strumenti e servizi di videosorveglianza: uno strumento che monitora gli accessi delle auto ai varchi di ingresso della città ed è in grado di rilevare le targhe ai fini assicurativi e di revisione

5.2 Il sistema di videosorveglianza è disciplinato da apposito e separato documento indicato come "Regolamento sulla videosorveglianza" allegato al Dossier Privacy. Con finalità esclusivamente inerenti le misure organizzative e tecniche di gestione della videosorveglianza, si ritiene utile in tale sede disciplinare

la tutela della privacy legata ai locali nei quali è controllato il terminale video che consente il monitoraggio e la visione delle immagini rilevate dalle telecamere.

a) Il terminale video dedicato alla videosorveglianza è collocato presso l'ufficio della polizia municipale in apposita ala dell'ufficio non direttamente visibile da parte delle persone che occasionalmente possono trovarsi a sostare presso l'ufficio

b) Il terminale video deve sempre essere posto in modalità blocco schermo in modo da non consentire neppure occasionalmente che persone non autorizzate possano prendere visione di quanto trasmesso dalle telecamere in tempo reale.

c) l'ufficio vigili dovrà sempre essere chiuso a chiave e reso accessibile da altri soggetti non autorizzati in caso di assenza dei vigili .

Per le altre norme in materia di tutela dei dati trattati con lo strumento della videosorveglianza si rimanda al Regolamento.

Data :

Firma per presa visione :

Titolare del trattamento dei dati : .....

(firma digitale ai sensi dell'art. 21 del d.lgs. 82/2005 e del DPCM 13/11/2014)

D.P.O (Data Protection Officer) : .....

(firma digitale ai sensi dell'art. 21 del d.lgs. 82/2005 e del DPCM 13/11/2014)

Amministratore di Sistema : .....

(firma digitale ai sensi dell'art. 21 del d.lgs. 82/2005 e del DPCM 13/11/2014)

Tutti gli incaricati al trattamento dei dati comunali : ……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……