COMUNE MANZANO

Provincia di Udine

MANUALE TECNICO-ORGANIZZATIVO PER LA GESTIONE DEI DATI E L'UTILIZZO DEGLI STRUMENTI INFORMATICI PER IL PERSONALE IMPIEGATO ALL'INTERNO DEL COMUNE DI MANZANO

Approvato con Deliberazione G.M. n. del

Indice

Premessa

Il presente Manuale intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Comune di Manzano nonché dell'UTI del Natisone per la parte impiegata presso la sede comunale di Manzano, le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.
Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Manzano.
I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Manuale costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione delle verifiche, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 sulla protezione dei dati personali.
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1 - Oggetto e finalità

Il presente Manuale è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/2016 sulla protezione dei dati personali (d'ora in avanti Reg. 679/2016 o GDPR);
- ai sensi del Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" *(in S.O n. 123 alla G.U. 29 luglio 2003, n. 174)* integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" *(in G.U. 4 settembre 2018 n.205)*;
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa».*

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità dell'Ente e pienamente rispettoso della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2 - Principi generali e di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Manuale sono gli stessi espressi nel GDPR, e, precisamente:

a) **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/2016);
b) **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
c) **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 Il dipendente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, sanitari o altri dati, elementi e informazioni dell'Ente dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro, se non previa richiesta.
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office. Il tutto compatibilmente con le dotazioni assegnate e lo spazio a disposizione.
d) E' vietato divulgare a familiari ed amici dettagli dell'attività svolta e della struttura informatica comunale.
e) E' vietato colloquiare con colleghi di attività d'ufficio, al telefono o di persona, in presenza di estranei.

f) E’ vietato gettare atti e/o appunti d’ufficio nella spazzatura, se non dopo averli debitamente parcellizzati tramite i sistemi distruggi-documenti o altro idoneo sistema.
g) Per le riunioni e gli incontri con utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell’Ente è preferibile, se presenti, utilizzare le eventuali sale dedicate.
h) Moderare il tono della voce ogni qualvolta si trattino argomenti inerenti dati personali.
i) Chiudere a chiave tutti i cassetti (se contenenti dati personali o particolari), gli armadi (se contenenti dai personali o particolari) e le porte, al termine dei propri orari di servizio.

3 - Tutela del lavoratore

3.1 Alla luce dell’art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell’art. 1 del presente Manuale, non è finalizzata all’esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest’ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/2016.

4 - Campo di applicazione

4.1 Il presente Manuale si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell’Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto. L’applicazione del presente Manuale è inoltre estesa a tutto il personale dell’UTI del Natisone, del personale in convenzione, e loro collaboratori, che operano, a qualsiasi titolo, all’interno della sede del Comune di Manzano.

4.2 Ai fini delle disposizioni dettate per l’utilizzo delle risorse informatiche e telematiche, per “utente” deve intendersi ogni dipendente e collaboratore ecc. ecc. in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come “incaricato del trattamento”. Rientrano in tali figure anche gli assegnatari provvisori di credenziali quali stagisti, studenti, incaricati a svolgere servizi interni su affidamento da parte dell’Ente ecc. ecc.

5 - Gestione, assegnazione e revoca delle credenziali di accesso

5.1 Le credenziali di autenticazione per l’accesso alle risorse informatiche vengono assegnate dall’Amministratore di Sistema, previa formale richiesta del Responsabile dell’Unità Operativa, da inviare tramite e-mail all’indirizzo principale dell’Ente Comune di Manzano almeno 10 giorni lavorativi antecedenti la presa in servizio dell’operatore, nell’ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Per ciascun nuovo utente dovrà essere specificato, all’atto della richiesta, il nome, cognome ed un indirizzo e-mail valido (anche provvisorio). Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile dell’Unità Operativa con il quale il collaboratore si coordina nell’espletamento del proprio incarico secondo quanto indicato nel presente comma. La richiesta di attivazione delle credenziali dovrà inoltre comprendere l’elenco dei sistemi informativi per i quali deve essere abilitato l’accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all’Ufficio Sistema Informativo Comunale dal Responsabile di riferimento.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente, di solito costituito dal nome e cognome dell'utente scritto in minuscolo tutto attaccato es. "*nomecognome"*, (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.

5.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare). Le password utilizzate per l'accesso ai diversi servizi devono essere diversificate, al fine di evitare la loro facile replicabilità.

5.4 È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi (o quando richiesto dal sistema o software utilizzato). Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali particolari, è obbligatorio il cambio password almeno ogni tre mesi.

5.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore ecc. ecc., il Responsabile dell'Unità Operativa di riferimento dovrà comunicare formalmente e preventivamente (almeno 10 giorni lavorativi prima del verificarsi dell'evento se conosciuto) all'Ufficio Sistema Informativo Comunale la data effettiva a partire dalla quale le credenziali saranno disabilitate. Qualora la cessazione del rapporto si riferisca al Responsabile dell'Unità Operativa stessa, spetta al Segretario Comunale provvedere all'espletamento di tale incombenza.

5.6 Le credenziali d'accesso sono personali, segrete, non cedibili e non divulgabili. Ove tali codici d'accesso non siano stati attribuiti è vietato l'utilizzo di codici assegnati ad altri utenti.

5.7 Ogni utente deve conservare diligentemente tutte le credenziali d'accesso assegnate, in modo da consentire il loro facile e immediato recupero ed aggiornamento, garantendo nel contempo la riservatezza assoluta di tali informazioni. In caso di cessazione dal servizio, indipendentemente dalla motivazione, (pensione, mobilità, trasferimento ecc. ecc.) l'utente che dispone di credenziali relative ad account attivati in nome e per conto dell'Ente, dovrà procedere per tempo al relativo passaggio di consegne.

6 - Utilizzo della rete del Comune di Manzano

6.1 Per l'accesso alle risorse informatiche del Comune di Manzano attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

6.2 È proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per Unità Operativa o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, e-mail personali, film ecc. ecc.. Ogni materiale personale rilevato dall'Amministratore di Sistema o dall'Ufficio Sistema Informativo Comunale a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli Strumenti in uso sarà rimosso senza ulteriori avvisi, ferma restando ogni eventuale

responsabilità personale in caso di danni causati. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella “Documenti” o “Desktop” dell’utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse dell’Ente, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.4 Senza il consenso dell’Ufficio Sistema Informativo Comunale, o dell’Amministratore di Sistema, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell’Ente a device esterni (hard disk, chiavette usb, CD, DVD e altri supporti).

6.5 Senza il consenso dell’Ufficio Sistema Informativo Comunale, o dell’Amministratore di Sistema, è vietato salvare documenti elettronici dell’Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

6.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi (anche della posta elettronica), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.7 il Comune di Manzano mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall’esterno dei confini dell’Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L’accesso mediante VPN viene concesso a consulenti, professionisti, tecnici e fornitori che nell’ambito di un rapporto contrattuale con il Comune di Manzano necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Manzano che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all’accesso mediante VPN dovranno seguire le prescrizioni del punto 5.

6.8 All’interno delle sedi del Comune di Manzano potrà essere resa disponibile anche una rete senza fili, c.d. “Wi-Fi”. Tali reti consentono l’accesso alle risorse dell’Ente e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L’accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell’ambito di un rapporto contrattuale con il Comune di Manzano necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Manzano che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L’impostazione della connessione Wi-Fi sarà effettuata contattando l’Ufficio Sistema Informativo Comunale che a sua volta disporrà in merito all’Amministratore di Sistema.

6.9 L’Ufficio Sistema informativo Comunale si riserva la facoltà di negare o interrompere l’accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell’Ente.

6.10 Ove non esistano specifiche diverse disposizioni, è vietato inserire codici di protezione all’accesso su singoli files (ad esempio di elaborati con sistemi di trattamento testi, fogli di calcolo, ecc.).

7 - Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software e applicativi)

7.1 Il dipendente/collaboratore ecc. ecc. è consapevole che gli Strumenti forniti sono di proprietà del Comune di Manzano e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore ecc. ecc. si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.2 L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

7.3 Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Sistema Informativo Comunale ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

7.4 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte del personale dell'Amministratore di Sistema.

7.5 L'installazione di software sui posti-lavoro informatizzati può avvenire solamente a fronte di autorizzazione scritta del Responsabile dell'Unità Operativa, previo nulla osta da parte del Sistema Informativo Comunale, con intervento dell'Amministratore di Sistema: tutti gli estremi delle licenze d'uso dei software installati, devono essere comunicati al Sistema Informativo Comunale.

7.6 I sistemi devono essere sempre custoditi: l'utente è tenuto a disattivare il sistema, o bloccarne l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

7.7 I sistemi assegnati dovranno essere disattivati e spenti al termine dell'orario di servizio.

7.8 I posti-lavoro informatizzati non possono essere resi inaccessibili localmente con sistemi di tipo fisico (hardware), al fine di permetterne la costante accessibilità da parte dell'assistenza tecnica e la loro pronta configurabilità e riallocazione fisica, per esigenze organizzative.

7.9 Costituisce buona regola la pulizia periodica (almeno mensile) degli archivi memorizzati sui sistemi in uso (PC, web-mail, ecc.), con cancellazione dei file obsoleti o non più utili.

7.10 La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzarli sulle condivisioni dell'Ente, in modo che i dati possano essere utilizzati anche da altri utenti, evitando sempre l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ufficio Sistema Informativo Comunale.

7.11 Gli operatori dell'Ufficio Sistema Informativo Comunale possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché

tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

7.12 È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

7.13 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

7.14 È vietato l'utilizzo di supporti di memoria magneto-ottici (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti dell'Ente, salvo che il supporto utilizzato sia stato fornito/autorizzato dall'Ufficio Sistema Informativo Comunale. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità istituzionali dell'Ente.

7.15 È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.

7.16 È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema. Assolutamente vietato connettere alla rete comunale eventuali apparati personali di qualsiasi natura essi siano.

7.17 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, lo stesso è obbligato a comunicarlo tempestivamente all'Ufficio Sistema Informativo Comunale ovvero all' Amministratore di Sistema.

7.18 I sistemi messi a disposizione di utenti non sottoposti alle presenti prescrizioni (es. Biblioteca, Ludoteca ecc.), non possono accedere alla rete del Sistema Informativo Comunale. Saranno pertanto instradati su apposite distinte reti virtuali ed avranno accesso solamente alle risorse elaborative locali ed alla rete internet.

7.19 La firma digitale viene, di norma, assegnata ai funzionari e loro sostituti, aventi potere di firma.

7.20 I sistemi anti-virus installati a protezione delle stazioni di lavoro assegnate, non possono essere disattivati se non a cura dell'Amministratore di Sistema per specifiche motivazioni.

7.21 L'archivio anagrafico è consultabile telematicamente da parte degli utenti autorizzati, in ossequio alla normativa vigente, mediante i sistemi tecnologici disponibili e con i profili di limitazione correlati alle esigenze del servizio.

7.22 Ogni postazione di lavoro è configurata in modo che:

7.22.1 alla richiesta dell'utente di accesso ad internet, il sistema si colleghi all'apposita pagina del portale web del Comune di Manzano contenente il riepilogo dei sistemi gestionali in uso agli uffici/servizi del Comune di Manzano.

7.22.2 Nell'elenco dei "preferiti" dei browser di navigazione internet, siano presenti i collegamenti a tutti i sistemi gestionali in uso agli uffici/servizi del Comune di Manzano.

8 - Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente /collaboratore ecc. si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

8.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dal proxy dell'Ente con le sue policy di sicurezza debitamente implementate e aggiornate, ad esempio per i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente. Il Comune di Manzano si avvale di un

sistema di content filtering fornito dalla RAFVG in convenzione e gestito direttamente da Insiel spa. Qualora l'accesso necessario ad un determinato link venga impedito da tale sistema, il Responsabile dell'Unità Operativa ne chiede lo sblocco in forma scritta tramite e-mail all'Ufficio Sistema Informativo Comunale che provvederà ad inoltrare la richiesta, se ritenuta lecita, ad Insiel spa.

8.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video (se non pertinenti all'attività svolta), l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

8.3 È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema.

8.4 L'Ente si riserva di bloccare l'accesso a siti "a rischio" anche di default, con l'uso del content filtering gestito da Insiel spa, attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri.

8.5 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco mediante una e-mail indirizzata all'Ufficio Sistema Informativo Comunale, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 12 e 12.2 del presente Manuale. Al termine dell'attività l'Amministratore di Sistema o gli addetti dell'Ufficio Sistema Informativo Comunale ripristineranno i filtri nella situazione iniziale.

8.6 È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dall'Ufficio Sistema Informativo Comunale, con il rispetto delle normali procedure di acquisto, fatto salvo quanto previsto dal successivo punto 8.12.

8.7 È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema.

8.8 È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8.9 È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Ufficio Sistema Informativo Comunale. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali.

8.10 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità quali ad esempio tenere misurata la performance della banda a parte del Servizio Informativo Comunale, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da YouTube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

8.11 E' autorizzato l'accesso ed uso, sia durante l'orario di servizio che al di fuori dello stesso, a tutti i social network nei quali è iscritta la Squadra Comunale di Protezione

Civile del Comune di Manzano da parte del Responsabile Comunale della Squadra, dal Coordinatore della medesima, dal personale incaricato, di quello dell'Ufficio Sistema Informativo Comunale e da parte dei Volontari di PC Digitali individuati dal Sindaco nonché dal Consigliere Delegato al Servizio di Protezione Civile.

8.12 In ossequio alla Direttiva n°02/09 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica – è consentito ai dipendenti l'uso della rete internet aziendale per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio per effettuare adempimento on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici ecc., ovvero per tenere rapporti con istituti bancari e assicurativi ecc.). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, ha, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e degli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.

8.13 Il dipendente può altresì, su autorizzazione dell'Ufficio Sistema Informativo, aiutare il cittadino che ne faccia richiesta, e che non abbia a disposizione la tecnologia necessaria e neppure la competenza informatica di base, ad accedere attraverso le credenziali che fornirà, ai servizi pubblici/privati richiesti (es Inps, Inail, Enel, Rai ecc. ecc.) per procedere allo svolgimento di operazioni a lui necessarie e richieste.

8.14 Presso la Biblioteca Comunale sono attive 3 postazioni PASI (Punti per l'Accesso ai Servizi Innovativi) fornite dalla Regione Friuli Venezia Giulia tramite Insiel spa, che rappresentano un'opportunità, consentendo infatti a tutti i cittadini di accedere gratuitamente ai servizi on-line (internet, skype ecc.) e ai siti erogati dalle Pubbliche Amministrazioni (Regione, UTI, Comune, Aziende Sanitarie ecc..) oltre naturalmente a tutte le risorse disponibili in rete. Le postazioni, dotate di computer con stampante, sono accessibili a tutti i residenti e ai non residenti, in particolar modo a chi, a casa, non dispone di un personal computer, a chi non ha una connessione internet a larga banda, a chi non possiede una confidenza sufficiente con lo strumento informatico (in questo caso l'utente può avvalersi dell'aiuto del responsabile del punto PASI). Per accedere ai servizi dei centri PASI l'utente dovrà recarsi con la propria Carta Regionale dei Servizi presso il centro PASI dove il responsabile del centro provvederà ad attivare un codice PIN personale (i cittadini di minore età devono essere abilitati al servizio da cittadini maggiorenni che dichiarano con autocertificazione ai sensi del DPR. 445/2000 di essere titolare della potestà parentale). Qualora vi siano delle difficoltà nell'utilizzo della CRS, il Responsabile del centro provvederà in modo diverso, secondo le indicazioni ricevute da Insiel spa, annotando in apposito file digitale i dati dell'utente nonché il relativo periodo di navigazione.

Al fine di garantire l'equa fruizione dell'accesso a tutti gli interessati, l'Ente gestore del Centro ha la facoltà di limitare la durata massima delle sessioni di utilizzo delle postazioni. Ogni utente è tenuto a rispettare la privacy degli altri utenti ed ha il divieto di:

1. eseguire interventi diversi da quelli necessari all'uso ordinario delle postazioni, in particolare è proibito accendere e spegnere i dispositivi, aprire le stampanti, scollegare cavi, spostare le apparecchiature dalla loro sede;
2. installare programmi e utilizzare software diverso da quello già installato sulla postazione, ed alterarne la configurazione o svolgere operazioni che influenzino o compromettano la regolare attività delle postazioni;
3. navigare su siti web a contenuto osceno, razziale, violento o che comunque incoraggino forme di attività illecite; l'utente è riconoscibile e responsabile in ordine alla violazione degli accessi protetti, del copyright e delle licenze d'uso;

4. accedere ai giochi d'azzardo.

La violazione da parte dell'utente degli obblighi previsti, può comportare la sospensione o l'esclusione dall'accesso al servizio, fermo restando la responsabilità personale dell'utente qualora il suo comportamento rappresenti una violazione delle norme vigenti.

Il personale di presidio:

1. ha il compito di accendere e spegnere i dispositivi e le postazioni, e provvedere ai ricambi del materiale di consumo;
2. ha la facoltà, in qualunque momento, di verificare il corretto utilizzo degli strumenti da parte degli utenti del servizio, eventualmente allontanando gli utenti che non rispettano il regolamento del centro.

Si informa che l'Ente, per il tramite dell'Ufficio Sistema Informativo Comunale, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.
Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, Insiel spa registra e detiene per 12 mesi i dati di navigazione (file di log riferiti al traffico web).

9 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente/collaboratore ecc. si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

9.1 Ad ogni utente viene fornito un account e-mail dell'Ente nominativo, generalmente coerente con il modello nome.cognome@comune.manzano.ud.it e l'utilizzo dell'e-mail deve essere limitato prevalentemente a scopi dell'Ente evitando ogni eccesso nell'utilizzo. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

9.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro (coerenti con il modello ufficio@comune.manzano.ud.it il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente. Il Responsabile dell'Unità Operativa di riferimento individua almeno due operatori, per ciascuna di tali caselle, da abilitare alla loro gestione; operatori che saranno abilitati dal Sistema Informativo Comunale, tramite Insiel spa, ad accedere a tale casella, con le stesse credenziali utilizzate per l'accesso alla e-mail personale fornita dall'Ente tramite Insiel spa.

9.3 Ogni casella di posta elettronica deve essere configurata in modo che, in calce ad ogni messaggio, siano sempre riportate le generalità del mittente, il ruolo, il servizio/ufficio e l'Amministrazione di appartenenza, i recapiti telefonici fissi e cellulari (di servizio), fax ed e-mail. Di seguito deve essere contenuto un avvertimento ai destinatari nel quale sia dichiarata la natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

9.4 l'accesso alla casella generale dell'Ufficio è consentito, attraverso l'uso delle proprie credenziali che permettono già l'accesso alla propria casella e-mail, al personale autorizzato dal responsabile dell'Unità Operativa e comunicato preventivamente

all’Ufficio Sistema Informativo Comunale che richiederà ad Insiel spa di attivare la relativa abilitazione. In caso di variazioni, il responsabile dell’Unità Operativa è obbligato a darne comunicazione immediata all’Ufficio Sistema Informativo Comunale che provvederà in merito.

9.5 La casella di Posta Elettronica Certificata istituzionale dell’Ente è integrata nel Protocollo Informatico del Comune di Manzano.

9.6 L’iscrizione a mailing-list o newsletter esterne con il proprio indirizzo dell’Ente personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l’affidabilità del sito che offre il servizio.

9.7 Allo scopo di garantire sicurezza alla rete dell’Ente, è assolutamente vietato aprire messaggi di posta in arrivo da mittenti di cui non si conosce l’identità, oppure si sospetta della genuinità della stessa, o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. *.pdf È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza è fatto obbligo di contattare l’Amministratore di Sistema o l’Ufficio Sistema Informativo Comunale per una valutazione dei singoli casi.

9.8 Non é consentito diffondere messaggi del tipo *”catena di S. Antonio”* o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.9 Nel caso fosse necessario inviare allegati *“pesanti”* è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario utilizzare lo specifico strumento di trasmissione reso disponibile dall’Ufficio Sistema Informativo Comunale, tramite Insiel spa. Su autorizzazione dell’Ufficio Sistema Informativo Comunale è anche possibile utilizzare, in via straordinaria, la propria casella di posta elettronica personale (in questo caso con personale si intende non quella rilasciata dall’Ente ma la propria e-mail privata) per l’invio di allegati particolarmente voluminosi secondo il sistema proprio del provider utilizzato.

9.10 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell’Ente, i dati personali e/o particolari di competenza dell’Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

9.11 Non è consentito, di norma, l’invio automatico di e-mail all’indirizzo e-mail privato (attivando per esempio un “inoltro” automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, sull’account e-mail dell’Ente nominativo, dovrà essere inserito un messaggio di cortesia “Out of Office”, facendo menzione di chi o quale struttura, all’interno dell’Ente, assumerà le mansioni durante l’assenza ed indicando almeno un indirizzo e-mail alternativo di tipo collettivo, tipo ufficio@comune.manzano.ud.it. L’invio automatico di e-mail all’indirizzo e-mail privato (attivando per esempio un “inoltro” automatico delle e-mail entranti) è consentito esclusivamente sulle caselle e-mail fornite agli Amministratori dell’Ente (Assessori e Consiglieri Comunali), con attivazione da richiedere all’Ufficio Sistema Informativo Comunale.

9.12 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Responsabile dell'Unità Operativa competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

9.13 È vietato inviare posta elettronica in nome e per conto di un altro utente;

9.14 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. La conservazione di messaggi con allegati è da evitare per quanto possibile, provvedendo al tempestivo salvataggio dell'allegato sulle condivisioni dell'Ente.

9.15 Tutta la corrispondenza istituzionale dovrà essere inviata direttamente dagli utenti esterni che intendono avvalersi dei servizi dell'Ente, all'indirizzo di posta elettronica certificata dell'Ente corrispondente a: comune.manzano@certvog.fvg.it.

9.16 E' concesso in via eccezionale, l'accesso alla propria casella di posta elettronica privata per il solo tempo necessario alla sua consultazione ferma restando ogni e qualsivoglia responsabilità in capo al dipendente circa le ricadute che tale atto potrebbe cagionare al sistema informativo comunale secondo i principi già espressi nell'art.8.12 del presente Manuale.

9.17 Qualora per intrattenere rapporti con gli utenti, aziende ecc. sia utilizzata in fase interlocutoria la propria e-mail personale fornita dall'Ente, dovrà essere specificato a chiare lettere che l'invio della corrispondenza ufficiale indirizzata all'Ente ed oggetto di protocollazione dovrà essere trasmessa solo ed esclusivamente all'indirizzo: comune.manzano@certgov.fvg.it, senza doppi passaggi;

Si informa che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.
Si informa altresì che l'Ente, per il tramite dell'Ufficio Sistema Informativo Comunale, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail in quanto la gestione del servizio di posta elettronica è gestito direttamente da Insiel spa secondo la convenzione in essere tra il Comune di Manzano e la RAFVG.
Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Amministratore di Sistema potrà accedere all'account di posta elettronica del Servizio, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, l'e-mail dell'Ente affidata all'utente sarà immediatamente cessata e non potrà più né ricevere né inviare alcuna comunicazione. Nel caso di rinnovo delle cariche elettive dell'Ente, tutte le e-mail rilasciate a nome dei Consiglieri ed Assessori saranno cessate il giorno stesso della proclamazione dei neo-eletti (fatti salvi i casi di riconferma). Si precisa che anche l'e-mail sindaco@comune.manzano.ud.it nel giorno della proclamazione degli eletti sarà svuotata completamente del suo contenuto e rimessa a disposizione del neo eletto Sindaco.

10 - Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del Comune di Manzano e sono resi disponibili all'utente per

rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

10.1 Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentita solo nel caso di comprovata necessità ed urgenza, per il limitato tempo strettamente necessario alla comunicazione stringata, specifica ed essenziale (ad. es. comunicare a casa un ritardo dovuto a questioni lavorative, problematiche sanitarie urgenti o riguardanti figli minori ecc. ecc.).

10.2 Al fine di garantire un corretto utilizzo dei servizi di telefonia (VoIP, mobile, ecc.) l'Ente predispone, ove tecnicamente possibile, adeguate configurazioni dei sistemi che consentano l'effettuazione o meno delle diverse tipologie di chiamata (es. chiamate su telefonini, internazionali etc.).

10.3 Accesso ai dati trattati dall'utente: per motivi di sicurezza del sistema telefonico, per motivi tecnici e/o manutentivi e programmazione dei costi, comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ufficio Patrimonio e/o Informatica, tramite l'Amministratore del Sistema e/o Insiel, accedere direttamente, nel rispetto della normativa sulla protezione dei dati, a tutti gli strumenti di telecomunicazione aziendali.

10.4 La Regione garantisce, per le finalità di accertamento e repressione dei reati, la conservazione dei dati di traffico telefonico entro il limite di settantadue mesi, ai sensi dell'articolo 24, comma 1, della L.167/2017.

10.5 Il sistema telefonico VoIP è fornito dalla Regione Autonoma Friuli Venezia Giulia nel contesto di specifica convenzione; le misure di sicurezza e protezione informatica, anche al data-base con i dati trattati, sono a carico di tale gestore ed erogatore di servizio.

10.6 Gli utenti del sistema telefonico devono intendersi adeguatamente informati di quanto citato nei precedenti 5 capoversi, mediante il presente Manuale.

10.7 Nei periodi di assenza per congedo, ogni operatore avrà cura di deviare la propria linea telefonica fissa su altra terminazione, regolarmente presidiata, dell'Ufficio/servizio di appartenenza.

10.8 Appena sarà resa disponibile l'applicazione di un codice "pin" per l'accesso al proprio apparato telefonico, ciascun dipendente sarà obbligato a farne uso al fine di evitare che terzi lo possano utilizzare per effettuare chiamate a sua insaputa;

10.9 Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

10.10 Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Ufficio Sistema Informativo Comunale.

10.11 È vietato l'utilizzo improprio delle fotocopiatrici dell'Ente.

10.12 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

10.12.1 Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative.

10.12.2 Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili).

10.12.3 Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.

10.12.4 Evitare di stampare la corrispondenza digitale già registrata nel Protocollo Informatico, strumento conforme alle regole del CAD (Codice Amministrazione Digitale) anche per quanto inerente alla conservazione sostitutiva.

10.13 Al fine di evitare la divulgazione di informazioni a persone terze non autorizzate, il rilascio delle stampe inviate sulle stampanti di gruppo avverrà solo previa digitazione di apposita password personale e segreta (se attribuita ad ogni utente) ovvero mediante l'immediato ritiro da parte del personale delle copie stampate.

10.14 L'utilizzo del fax deve intendersi come sistema di comunicazione residuale, limitatamente nei confronti di entità privatistiche, essendo obbligatorio l'utilizzo della comunicazione digitale nei rapporti tra Pubbliche Amministrazioni. I Fax in arrivo al numero principale del Comune, sono deviati dal sistema sull'indirizzo principale di posta elettronica certificata dell'Ente;

10.15 Tutti i documenti acquisiti tramite scanner/fotocopiatore, devono essere immediatamente rimossi, o cancellati, dalla relativa cartella condivisa, nello stretto tempo necessario al raggiungimento della propria postazione di lavoro a cura dell'utente che ha operato la scansione. Tutti i file che rimarranno depositati nella cartella condivisa, saranno immediatamente cancellati dal personale incaricato ferma restando ogni altra responsabilità in carico all'operatore che non vi ha provveduto per tempo.

11 - Assistenza agli utenti e manutenzioni

11.1 L'Ufficio Sistema informativo Comunale e l'Amministratore di Sistema possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

11.1.1 – verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.

11.1.2 – verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.

11.1.3 – richieste di aggiornamento software e manutenzione preventiva hardware e software.

11.2 Gli interventi tecnici posso avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema ed il personale dell'Ufficio del Sistema Informativo Comunale sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare alla sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente Manuale.

12 – Verifiche sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente è tenuto a vigilare sul rispetto delle direttive contenute nel presente Manuale.

L'Amministratore di Sistema provvederà quindi alla verifica delle eventuali anomalie riscontrate sul sistema informativo comunale provvedendo in merito, nei limiti consentiti dalle norme legali e contrattuali. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. Le verifiche devono essere effettuate nel rispetto del Regolamento UE 2016/679 e del presente Manuale e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l'adozione del presente Manuale ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

12.2 Si evidenzia che l'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Manuale. Tali informazioni, che possono contenere dati personali eventualmente anche particolari dell'Utente, possono essere oggetto di accesso da parte dell'Amministratore di Sistema per motivazioni esclusivamente volte a garantire la sicurezza immediata e l'inviolabilità dei sistemi informativi comunali. Lo stesso Amministratore di Sistema eventualmente si farà carico di comunicare, se ritenuto prioritario, all'Ufficio di Informatica, le difformità riscontrate.

Tutte le eventuali verifiche sopra descritte, se assolutamente e inderogabilmente necessarie per motivi di sicurezza immediata o violazione del sistema informativo comunale, avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Manuale. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

13- Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/2016 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), è conservata da Insiel spa per un massimo di 12 mesi, salvo esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

13.2 Insiel spa dovrà assumere tutte le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 - Partecipazione ai Social Media

14.1 L'utilizzo a fini promozionali ai social media (Facebook, Twitter, Linkedin, Telegram, watsapp, dei blog, dei forum ecc. ecc., anche professionali ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media.

14.3 E' vietata la partecipazione ai social media durante l'orario di lavoro, per finalità personali con l'esclusione di quelle legate al benessere ed alla sicurezza della persona per il tempo strettamente necessario alla consultazione che non dovrà essere mai sistematica.

14.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

14.5 L'utilizzo dei social media è interdetto agli utenti/collaboratori sulla rete informatica del Comune di Manzano fatta eccezione per tutto ciò che attiene la gestione della Protezione Civile Comunale; deroghe potranno essere concesse a singoli utenti, previa motivata richiesta da indirizzare al Sindaco tramite il Responsabile dell'Unità Operativa all'Ufficio Sistema Informativo Comunale.

15 – Attività Sindacale e R.S.U.

15.1 Nell'ambito dell'agibilità sindacale prevista dal CCRL vigente è consentito l'uso di tutte le apparecchiature a disposizione dell'Ente (PC, stampanti, fotocopiatrici, scanner, e-mail personale, internet inclusi consumabili ecc. ecc.), senza limitazioni od oneri a carico, per l'espletamento dell'attività sindacale da parte delle RSU elette, Dirigenti sindacali o personale dipendente individuato dalle organizzazioni sindacali territoriali che operano nell'ambito dell'Amministrazione Comunale di Manzano, per fini sindacali.

16 - Sanzioni disciplinari

16.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti ecc.ecc. di osservare le disposizioni portate a conoscenza con il presente Manuale.

17 – Entrata in vigore

17.1 Il presente Manuale sarà operativo ed efficace per tutti gli interessati a partire dall'avvenuta pubblicazione all'albo pretorio della delibera di adozione.

18 – Abrogazione

18.1 si intende abrogata la "policy interna sul trattamento dati e sull'utilizzo degli strumenti di elaborazione e comunicazione delle informazioni" adottato con Deliberazione Della Giunta Comunale n°128 del 11.05.2009;

19. - Divulgazione

19.1 Copia del presente Manuale sarà notificato a tutto il personale comunale e suoi collaboratori, al personale dell'UTI del Natisone allocato presso il Comune di Manzano e suoi collaboratori, al Segretario Comunale ed agli Amministratori nonché trasmesso alla Presidenza dell'UTI del Natisone e pubblicato sul sito Istituzionale dell'Ente.