C O M U N E D I M E O L O

Provincia di Venezia

REGOLAMENTO PER LA GESTIONE E L'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI

ADOTTATO CON DELIBERAZIONE DI GIUNTA COMUNALE N. 102 IN DATA 06.11.2020

INDICE

Art. 1	-	Introduzione…….	Pag.	2
Art. 2	-	Principi generali di riservatezza nelle comunicazioni……..	"	4
Art. 3	-	Gestione, assegnazione e revoca delle credenziali di accesso…….	"	5
Art. 4	-	Utilizzo delle infrastrutture di rete e File System……	"	6
Art. 5	-	Utilizzo degli strumenti elettronici (pc, notebook e altri strumenti con relativi software ed applicativi…….	"	7
Art. 6	-	Utilizzo di telefoni, fax, stampanti, fotocopiatrici, scanner…….	"	8
Art. 7	-	Navigazione Internet e utilizzo della rete…….	"	9
Art. 8	-	Utilizzo della posta elettronica…….	"	10
Art. 9	-	Manutenzione, modifiche, furto o smarrimento delle risorse ICT……...	"	11
Art. 10	-	Protezione antivirus……..	"	12
Art. 11	-	Accesso ai locali……...	"	12
Art. 12	-	Controlli……...	"	12
Art. 13	-	Utilizzo dei social network……...	"	14
Art. 14	-	Conservazione……..	"	14
Art. 15	-	Disposizioni ulteriori……	"	14
Art. 16	-	Pubblicità…….	"	15
Art. 17	-	Violazioni…….	"	15

1. Introduzione

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'Ente e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso.
Le apparecchiature messe a disposizione dall'Ente sono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi, secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.
Poiché anche nella normale attività lavorativa, alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine dell'organizzazione, risulta necessario per l'Ente stabilire regole procedurali e clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare, finalizzate non tanto a censurare comportamenti consapevolmente scorretti e già di per sé proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati dell'Ente.
Il Comune di Meolo adotta il presente Regolamento per l'utilizzo delle dotazioni informatiche e di telecomunicazione per fornire un quadro preciso di indicazioni in merito ai criteri ed alle modalità d'assegnazione d'utilizzo delle stesse.

1.1 Definizioni

Le risorse ICT, messe a disposizione dall' Ente, oggetto di tutela, descritte nel presente documento, sono:

- il patrimonio informativo, detenuto dall'Amministrazione, in formato elettronico e/o cartaceo;
- i servizi informatici erogati dall'Amministrazione;
- le postazioni di lavoro (PC desktop e simili) e "mobili" (PC portatili e simili);
- i dispositivi cellulari (smartphone);
- i software di comunicazione (tipo "messenger, hangouts, zoom, skype" e simili se previsti);
- i server, e tutto il materiale hardware in generale.

Le parole e le espressioni, usate nel presente Regolamento, hanno il seguente significato:
Amministratore di Sistema - In ambito informatico, figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti.
Bios – Software di basso livello che fornisce ad un PC le funzioni di base per l'accesso all'hardware. E' il primo programma eseguito all'accensione, prima ancora del sistema operativo.
Chat line - Il termine chat (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente chatroom (letteralmente "stanza delle chiacchierate"), detto anche channel (in italiano canale), spesso abbreviato chan.
Download o upload - In generale con questo termine si intende il trasferimento di dati da un computer locale a uno remoto utilizzando un apparato di comunicazione, ad es. il modem, o tra computer della stessa rete Per download si intende anche la visualizzazione sul proprio computer di una pagina internet.
Forum – Struttura informatica che consente la discussione online, tramite internet, degli utenti. Utilizzato per la discussione su temi specifici.
Guest book - Fornisce ai visitatori l'opportunità di lasciare commenti (sul sito) per i nuovi utenti che entreranno nel sito.
Mailing list – Sistema organizzato per la partecipazione di più persone in una discussione asincrona mediante e-mail.
Malware – Software creato con l'intento di causare danni ad un sistema informatico o di carpire dati personali memorizzati in un sistema informatico.

Newsletter – notiziario scritto diffuso tramite e-mail agli utenti iscritti.
Phishing – attività illegale che sfrutta messaggi di posta elettronica ingannevoli per ottenere l'accesso a informazioni personali, anche di carattere riservato, con la finalità del furto di identità, nell'ambito di comunicazioni elettroniche. Utenti truffatori inviano messaggi che imitano logo e grafica di siti istituzionali, con richieste di inserimento di dati personali, come numeri di carta di credito, codici personali e segreti di accesso etc. Si possono individuare da un attento esame del contenuto del messaggio che spesso contengono collegamenti a siti non istituzionali.
Proxy - Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client. In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software.
Remote banking - Per remote banking si intende l'insieme di servizi automatizzati che permettono ai clienti, grazie all'uso di terminali o di un semplice telefono, di collegarsi alla banca presso la quale intrattengono il conto corrente ed effettuare una serie di operazioni bancarie, oppure di ricevere informazioni in tempo reale. A seconda del mezzo di comunicazione utilizzato si può parlare di phone banking ed internet banking.
Social network – servizio online che consiste nella connessione di persone legate da diversi legami sociali, quali interessi comuni, rapporti di lavoro, legami affettivi fino alla conoscenza casuale.
Spam – messaggi di posta elettronica, non sollecitati, con contenuto generalmente commerciale.
***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif** - Si tratta di estensioni di file che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.
Trattamento - qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Archivio - qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Titolare del trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Dato identificativo - dato personale che permette l'identificazione diretta dell'interessato.

Dato anonimo - il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.2 Finalità del presente documento

Il presente documento si prefigge di tutelare le risorse ICT dell'Amministrazione e di promuovere in tutto il personale una corretta cultura per la protezione dell'informazione in particolar modo intende perseguire i seguenti obiettivi:

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;

- garantire il rispetto della normativa in materia;

- 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;

1.3 Contesto Normativo

Questo documento fa riferimento al seguente quadro normativo:

- "*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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");

- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"(d'ora in poi "Codice Privacy") integrato con le modifiche introdotte dal *D.Lgs 10 agosto 2018, n. 101, 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE(regolamento generale sulla protezione dei dati).*

- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008).

- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007 pubblicato in Gazzetta Ufficiale n. 5 del 10 marzo 2007.
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".
- Legge 20 maggio 1970, n. 300 "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" (Statuto dei Lavoratori); Modificata dall'articolo 23 D.lgs. 14 settembre 2015 n. 151 (così detto *"Decreto sulle semplificazioni"* attuativo della Legge delega 10.12.2014 n. 183, anche nota come *"legge di riforma del diritto del lavoro"* o *"Jobs Act"*).
- I vigenti Contratto Collettivo Nazionale di Lavoro e Contratto Collettivo Decentrato Integrativo.

1.4 Ambito di applicazione

Il presente Regolamento si applica ai soggetti di seguito indicati di seguito complessivamente denominati "utenti":

a) Amministratori e dipendenti, a qualsiasi titolo inseriti nell'organizzazione dell'Ente, senza distinzione di ruolo e/o livello;
b) Consulenti e collaboratori dell'Ente, a prescindere dal rapporto contrattuale intrattenuto con la stessa;
c) Dipendenti e collaboratori di società che hanno un contratto in essere con l'Ente e che utilizzano risorse ICT della stessa;
d) Ospiti dell'Ente, per l'eventuale uso delle risorse ICT della stessa;
e) Enti e Agenzie attestati alla rete Intranet, per quanto applicabile.

1.5 Contesto Normativo

a) Alla luce dell'art. 4, comma , Legge n. 300/970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, 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 i sistemi informativi per far fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
b) E' garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. UE 679/2016.

2. Principi generali di riservatezza nelle comunicazioni

2.1 Principi che sono a fondamento del presente Regolamento 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. 679/16);

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 deve attenersi alle seguenti regole di trattamento e protezione dell'informazione:

c) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, 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 dell'area/funzione.

d) È vietato modificare, estrarre originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro, salvo esplicita autorizzazione da parte del Responsabile di riferimento.

e) È vietato alterare l'informazione.

f) 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 la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di personale con mansioni di front office.

g) Per le riunioni e gli incontri con utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell'Ente è necessario utilizzare le apposite sale dedicate.

h) I dispositivi hardware e software ed in generale tutti gli strumenti di lavoro disponibili sono utilizzabili esclusivamente per le attività finalizzate al compimento degli incarichi di lavoro assegnati; altri utilizzi al di fuori di quest'ultimo sono da considerarsi esclusi.

i) I soli dispositivi informatici utilizzabili durante l'attività di lavoro sono quelli consegnati al momento dell'assunzione o al cambio/modifica della propria attività di lavoro.

j) L'utilizzo di apparecchiature hardware e software personali potrà avvenire solo su esplicita autorizzazione da parte del Responsabile di riferimento/Responsabile del Sistema informativo comunale, anche in regime di smart working.

k) E' riconosciuto al datore di lavoro di poter svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

3. <u>Gestione, assegnazione e revoca delle credenziali di accesso</u>

3.1 Le credenziali (nome utente e password) per l'accesso ai servizi informatici vengono assegnate dall'Amministratore di Sistema, previa richiesta del responsabile dell'ufficio/servizio, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal responsabile dell'ufficio/servizio con il quale il

collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed 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'Amministratore di Sistema o al Responsabile di riferimento.

L'Amministratore di sistema provvede inoltre a rigenerare password scadute o dimenticate ovvero a sospenderle in particolari casi.

3.2 Le credenziali di autenticazione consistono in un codice di identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password.

3.3 L'utente assegnatario dovrà modificare alla prima connessione la password attribuita e comunicata dall'Amministratore di Sistema, e successivamente ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.

3.4 La password deve essere di adeguata robustezza: deve essere composta da minimo 8 caratteri alfanumerici, preferibilmente un carattere numerico, uno maiuscolo uno minuscolo e uno speciale; non deve contenere riferimenti agevolmente riconducibili all'incaricato. (username, nomi o date relativi alla persona o da un familiare).

3.5 La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza, senza divulgarla. E' pertanto vietata la trascrizione della stessa su supporti facilmente accessibili a terzi (ad es. foglietti, post-it etc.), ovvero permettere ad altri utenti o colleghi di operare con le proprie credenziali.

3.6 Gli utenti devono proteggere le credenziali memorizzate sugli smartphone, tablet e personal computer utilizzati per fruire dei servizi dell'Ente (ad es. posta elettronica, intranet, ecc.) e, nel caso di furto o smarrimento siano essi personali o dell'Ente, devono cambiare tempestivamente la "password del dominio".

3.7 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il responsabile dell'ufficio/servizio di riferimento dovrà comunicare formalmente e tempestivamente all'Amministratore di Sistema, in modo da consentire la disabilitazione dell'accesso.

3.8 È vietato chiedere o raccogliere, in qualsiasi modo, le password degli utenti a cui l'Ente eroga servizi. Se è necessario accedere alle procedure di un utente che dovesse richiedere assistenza, deve essere invitato a digitare lui stesso la password, sia che l'operazione avvenga presso la sede esterna dell'utente, che presso la sede dell'Ente o in remoto. Qualora durante l'attività di lavoro si venga a conoscenza di una password dell'utente a cui l'Ente eroga servizi, questi deve essere immediatamente informato ed inviato a modificare la stessa il prima possibile.

4. Utilizzo delle infrastrutture di rete e File System

4.1 Per l'accesso alle risorse informatiche del Comune di Meolo, attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 3 del presente Regolamento.

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

4.3 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 settore/ufficio 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, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema, a seguito di interventi di sicurezza informatica, ovvero di manutenzione/aggiornamento sui server, viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell' Amministratore 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.

4.4 Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

4.5 Senza il consenso 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.).

4.6 Con regolare periodicità (almeno una volta ogni sei mesi), ciascun utente provvede alla pulizia delle cartelle di rete di propria competenza, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4.7 L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Organizzazione stessa, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN, limitato al solo RDP (Remote Desktop Protocol) viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici o siano in modalità di lavoro subordinato o smart working, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante tali canali di comunicazione dovranno essere autorizzate dall'Amministratore di Sistema e seguire le regole e le prescrizioni di cui ai punti 2 e 3. Qualora sia necessario l'accesso alla rete dell'Ente attraverso i suddetti strumenti e tecniche di collegamento è necessario prestare la massima attenzione nelle fasi di accesso, proteggendo da occhi o da telecamere presenti la fase di digitazione dell'utente e della password. Una volta aperta la connessione, questa deve rimanere attiva lo stretto necessario all'espletamento delle attività richieste, quindi chiusa. In ogni caso, prima di abbandonare la postazione dalla quale è stata aperta la connessione è bene accertarsi dell'avvenuta chiusura della stessa, eliminando cronologia e file temporanei (ove possibile) ed eventuali altri dati di connessione che l'amministratore di rete potrà indicare all'utente in fase di consegna delle credenziali di accesso.

4.8 L'Amministratore di Sistema 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.

4.9 I log relativi all'uso del File System, nonché i file salvati o trattati su server o strumenti, saranno registrati e potranno essere oggetto di controllo da parte del titolare del trattamento, attraverso l'Amministratore di Sistema dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

4.10 Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection"

5. <u>Utilizzo degli strumenti elettronici (pc, notebook e altri strumenti con relativi software ed applicativi)</u>

5.1 Gli utenti sono consapevoli che gli strumenti forniti sono di proprietà del Comune di Meolo 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 utente si deve quindi attenere alle seguenti regole di utilizzo degli strumenti.

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

5.3 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 preposto ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password d'accensione (Bios), senza preventiva autorizzazione da parte dell'Amministratore di Sistema

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

5.5 L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato il dispositivo (pc, notebook, tablet) o nel caso ritenga di non essere in grado di presidiare l'accesso al medesimo: lasciare un pc, notebook, tablet incustodito, che sia connesso o meno alla rete, può essere causa del suo utilizzo, da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.

5.6 Le informazioni archiviate sul pc locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata nel corso della giornata e pertanto ogni informazione deve essere riposta nella opportuna area del server di archiviazione.

5.7 L'utente deve provvedere, con cadenza periodica (almeno ogni sei mesi) alla pulizia degli archivi presenti sulla propria postazione, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati;

5.8 La gestione dei dati su pc è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni dell'Ente, dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati.

5.9 L'Amministratore di Sistema o gli operatori preposti possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC/notebook, 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.

5.10 La riproduzione o la duplicazione di programmi, può essere effettuata solo nel pieno rispetto della vigente normativa in materia di protezione della proprietà intellettuale.

5.11 E' obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il pc/notebook sempre protetto.

5.12 Non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Amministrazione, salvo specifica autorizzazione.

5.13 Procedere allo spegnimento delle postazioni di lavoro "fisse", al termine dell'orario di lavoro, salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento.

5.14 Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, il Comune utilizza alcuni software (teleassistenza) che permettono all'amministratore di sistema (previo consenso dell'utilizzatore finale) di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente.

6. <u>Utilizzo di telefoni, fax, stampanti, fotocopiatrici, scanner</u>

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, sono di proprietà dell'Ente stesso e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

6.1 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 consentito solo nel caso di comprovata necessità ed urgenza.

6.2 Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smatphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici, 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.

6.3 Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "App" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

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

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

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

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

6.5 Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato, qualora non siano provvisti di spegnimento automatico nel tempo.

6.6 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate, in alternativa, dovrà procedere mediante "stampa riservata/differita" dei documenti.

6.7 È vietato:

a) l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa autorizzazione da parte del Responsabile dell'unità operativa.

b) l'utilizzo delle fotocopiatrici/scanner per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa.

7. Navigazione Internet e utilizzo della rete

ll PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento dell'Ente utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi:

7.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è regolato con policy di sicurezza debitamente implementate ed aggiornate.

7.2 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 e di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

7.3 L'Ente si riserva di bloccare l'accesso a siti "a rischio" 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. In caso di blocco accidentale di siti di interesse dell'Ente, contattare l'Ufficio Sistemi Informativi per uno sblocco selettivo.

7.4 Nel caso in cui, per ragioni d iservizio, necessiti una navigazione libera da filtri, è necessario richiedere lo sblocco mediante una e-mail indirizzata all'Amministratore d iSistema, ed in copia al Responsabile dell'Ufficio/Servizio, nella quale siano indicti 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 il punto 12 del presente regolamento.

7.5 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 dal Responsabile dell'ufficio/Servizio e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

7.6 È vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione degli Amministratori di Sistema e dei responsabili di riferimento previo parere tecnico dello stesso Amministratore di sistema.

7.7 La Rete "Wi-Fi", se presente all'interno dell'Ente, consente l'accesso alle risorse 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 l'Ente per permettergli di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. La gestione della connessione Wi-Fi sarà effettuata dall'Amministratore di sistema.

7.8 E' consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. 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. E' consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del punto 12 del presente regolamento.

7.9 Si informa che l'Ente, per il tramite Amministratore di sistema, 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 esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, l'Ente potrebbe registrare i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.
Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.

8. 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 si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

8.1 Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello xxxxx@nomeEnte.it. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.
8.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro 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.
8.3 L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
8.4 Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. 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 contattare gli Amministratori di Sistema per una valutazione dei singoli casi.
8.5 Non é consentito inviare/partecipare a catene telematiche 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.
8.6 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, questo va fatto soltanto a destinatari - persone o Enti – qualificati e competenti.
8.7 Al fine di garantire la funzionalità del servizio di posta elettronica dell'Ente e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) è predisposto per l'invio automatico di messaggi di risposta (funzione "Autoreply" o "Out of office") contenenti le "coordinate" di posta elettronica di un altro soggetto di riferimento o altre utili informazioni o modalità di contatto della struttura/servizio. Tale funzionalità deve essere attivata dall'utente.
8.8 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile del Servizio assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.

8.9 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio. 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.

8.10 È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

8.11 La casella di posta elettronica, personale e quella relativa al gruppo ufficio, deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, essendo lo spazio di archiviazione limitato, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni/area documentale del server.

8.12 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. In caso di ricezione di *e-mail* non attinenti alle attività di lavoro (spam), queste vanno immediatamente eliminate e non si deve in alcun modo attivare gli allegati di tali messaggi.

8.13 Nel caso in cui l'*e-mail* ricevuta sia destinata ad altre persone è necessario limitare il più possibile la lettura del documento, ovvero facendolo con il solo obiettivo di comprendere che non si tratta di documentazione propria (quindi senza né leggere il contenuto, né cercare di capire a chi appartiene), ma inviare un messaggio al mittente spiegando l'errore. L'*e-mail* ricevuta va immediatamente eliminata, anche dal cestino.

8.14 Si informa inoltre che l'Ente, per il tramite dell'Amministratore di Sistema, 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. 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 può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica dell'Ente, prendendo visione dei messaggi, salvando o cancellando file.

8.15 Si informa infine che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo).

9. Manutenzione, modifiche, furto o smarrimento delle risorse ICT

9.1 L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

a) Verifica e risoluzione di probelmi sistemistici ed applicativi, su segnalazione dell'utente finale ;
b) Verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
c) Richieste di installazione ed aggiornamento del software, ovvero di manutenzione preventiva di hardware e software.

9.2 Gli interventi tecnici possono avenire previso consenso dell'utente, quanto l'intervento spesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco od in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

9.3 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 verifice delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

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

9.5 Il sistema operativo ed il software di base del proprio PC è preimpostato, ed è definito dall'Ente stesso. Non è consentita l'installazione di nessun altro software oltre a quello definito, è vietata la modifica dei parametri di configurazione dei dispositivi assegnati.

9.6 Non è permesso intervenire sul dispositivo togliendo o sostituendo componenti hardware o aggiungendo alla rete locale qualsiasi dispositivo che possa inficiare il corretto funzionamento degli apparati ICT (PC esterni, router, switch…).

9.7 In caso di malfunzionamenti deve essere immediatamente avvertito il personale preposto, ogni eventuale modifica deve essere concordata e autorizzata da parte dell'Amministratore di Sistema.

9.8 In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, l'utente dovrà informare tempestivamente l'Amministratore di Sistema comunicando quali dati erano contenuti all'interno.

10. Protezione Antivirus

10.1 Il sistema informatico dell'Ente è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Ente mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente all'Amministratore di Sistema.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del preposto.

11. Accesso ai locali

11.1 L'accesso è consentito al solo personale autorizzato. Gli utenti possono essere autorizzati all'accesso solo relativamente all'erogazione di servizi ed in presenza degli operatori dell'Ente. Gli operatori esterni che devono entrare nei locali (ad esempio per attività di manutenzione), devono essere espressamente autorizzati dal responsabile di riferimento dell'Ente. Gli operatori esterni, in ogni caso, devono operare in presenza e sotto la supervisione degli operatori dell'Ente.

11.2 Gli operatori esterni all' Ente sono tenuti a svolgere le proprie mansioni senza comprometterne la sicurezza delle risorse e delle informazioni a cui hanno accesso. Qualsiasi intervento che possa anche minimamente compromettere la sicurezza, deve essere preventivamente comunicato al responsabile di riferimento che ne deve concedere autorizzazione scritta.

11.3 In assenza di operatori, tutti i locali devono essere chiusi a chiave. Ogni informazione da proteggere su supporto cartaceo, in carico ai singoli operatori, al termine della giornata lavorativa, o più in generale, quando questi non sono presidiati, vanno chiusi a chiave negli appositi armadi o cassettiere.

12. Controlli

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 verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, c.2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. 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. I controlli devono essere effettuati nel rispetto del presente Regolamento 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 Regolamento 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 L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei punti precedenti del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento – sostituzione - implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai punti 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

12.3 <u>Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento - sostituzione - implementazione di programmi, manutenzione hardware, ecc.).</u>

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti del presente Regolamento il Titolare del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

a) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
b) Dopo un tempo stimato in 72 ore, se il comportamento anomalo persiste, l'Ente potrà accedere alle informazioni necessarie con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
c) Qualora il rischio di compromissione del sistema informatico dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Titolare del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.4 <u>Controlli per esigenze produttive e di organizzazione</u>

Per esigenze produttive e di organizzazione di si ntendono, fra le altre, l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Titolare del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

a) Redazione di un atto da parte del Responsabile dell'Ufficio/Servizio e/o che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
b) Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
c) Redazione di un verbale che riassuma i passaggi precedenti.
d) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
e) Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.

13. Utilizzo dei Social network

13.1 L'utilizzo a fini istituzionali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifico regolamento, direttive ed istruzioni operative, al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

13.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare alcune regole comportamentali al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, utenti esterni, fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

13.3 Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

13.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Responsabile dell'ufficio/servizio.

13.5 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile dell'ufficio/servizio.

13.6 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

14. Conservazione

14.1 I dati personali relativi agli accessi ad Internet ed al traffico telematico ai log di sistema, la cui conservazione non sia necessaria, saranno periodicamente cancellati in modo automatico mediante procedure tecniche adottate dall'Amministratore di sistema, che provvederà a configurare i sistemi in modo che ciò avvenga, in maniera conforme alla vigente normativa.

14.2 L'eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari; all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria. In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità specifiche e comprovate e limitate al tempo necessario e predeterminato al loro raggiungimento.

14.3 L'Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

15. Disposizioni ulteriori

La sicurezza sei sistemi informatici è soggetta a costante evoluzione dovuta al continuo mutare delle minacce informatiche, il che comporta l'adozione di contromisure sempre differenti e specifiche al verificarsi di attacchi o eventi particolari. A tal fine l'Amministratore di Sistema informa gli utenti, tramite posta elettronica e/o tramite altri canali digitali istituzionali, circa le ulteriori prescrizioni da osservare da parte degli utenti.

16. Pubblicità

Viene data diffusione ai dipendenti dell'approvazione del Regolamento tramite posta elettronica e/o altri canali digitali istituzionali e mediante pubblicazione sull'apposita sezione "amministrazione trasparente" del sito istituzionale.

17. Violazioni

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL, ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale.