AZIENDA TERRITORIALE PER L'EDILIZIA RESIDENZIALE
DELLA PROVINCIA DI TREVISO

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI

APPROVATO CON
DECRETO DEL DIRETTORE N. 173 DEL 28.02.2023

Sommario

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche autorizzati o Utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Ai fini del presente Regolamento l'Ente si configura quale Titolare del trattamento, ovvero la persona giuridica che determina le finalità e i mezzi del trattamento di dati personali.

Ogni dipendente e collaboratore è tenuto a rispettare il presente Regolamento.

Tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò 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.

Sui sistemi informatici in uso agli Utenti non sono installati o configurati apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1. Oggetto e finalità

1.1 Il presente Regolamento è redatto sulla base delle seguenti fonti di diritto:

- Legge 20 maggio 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*";
- Regolamento Europeo 679/16 "*General Data Protection Regulation*" (di seguito "Reg. 679/16" o "GDPR");
- "*Linee guida del Garante per posta elettronica e Internet*" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- Art. 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act).

1.2 La finalità del presente Regolamento è quella di promuovere in tutto il personale una corretta "cultura informatica", fornendo le informazioni utili e necessarie affinché l'utilizzo degli Strumenti informatici e telematici messi a disposizione dall'Ente, quali la posta elettronica, Internet, i personal computer ed i software, sia conforme alle finalità e nel pieno rispetto della legge. L'obiettivo principale è quello di evitare il verificarsi di qualsiasi abuso o uso non conforme degli Strumenti, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2. Campo di applicazione

2.1 Il presente regolamento 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.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "autorizzato del trattamento".

3. Principi generali e di riservatezza nelle comunicazioni

3.1 I principi a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

- **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);
- **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;

- **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art. 5, co. 1 e 2 del GDPR), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile".

3.2 Il dipendente si attiene alle seguenti regole:

a) è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, sanitari o altri dati, elementi e informazioni 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/ Ufficio.

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;

c) è vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni 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 e di ricezione di Clienti/ assegnatari di alloggi / Fornitori o colleghi di lavoro;

d) per le riunioni e gli incontri con Clienti/ assegnatari di alloggi, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le eventuali zone/ sale dedicate.

4. Gestione, assegnazione e revoca delle credenziali di accesso

4.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'Area/Ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo Utente. Nel caso di collaboratori esterni, la richiesta deve essere inoltrata direttamente dalla Direzione o dal Responsabile dell'Area/Ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali deve essere completa di generalità dell'Utente ed elenco degli Strumenti informatici 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.

4.2 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'Utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e deve essere conservata e custodita dall'Utente con la massima diligenza, senza divulgarla.

4.3 La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili all'Utente (username, nomi o date relative alla persona o ad un familiare).

4.4 È necessario procedere alla modifica della password a cura dell'Utente al primo accesso e, successivamente, almeno ogni tre mesi.

4.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Area/Ufficio di riferimento deve comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali devono essere disabilitate.

5. Utilizzo infrastruttura di rete e *File System*

5.1 Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun Utente deve essere in possesso di credenziali di autenticazione.

5.2 È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

5.3 L'accesso alla rete garantisce all'Utente la disponibilità di condivisioni di rete (cartelle su server), nelle quali vanno inseriti e salvati i file di lavoro, organizzati per Area/Ufficio o per diversi criteri o per obiettivi specifici di lavoro. Ciascun Utente, poi, dispone di un'area riservata e personale denominata "cartella utente". Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. È vietato, pertanto, 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, 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 su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo paragrafo 13 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informatici e Strumenti dell'Ente a device esterni (*hard disk*, chiavette, CD-ROM, DVD e altri supporti).

5.4 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 ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

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

5.6 Su espressa richiesta della Direzione, l'Ente può mettere a disposizione dei propri Utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno, mediante accesso sicuro (o tramite rete VPN oppure tramite protocolli di tipo sicuro quali ad esempio il protocollo HTTPS, 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 l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso dall'esterno dell'Ente dovranno seguire le prescrizioni del paragrafo 4.

5.7 All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tale rete consente l'accesso alle risorse e ad Internet ai 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 necessitino 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. L'impostazione della connessione Wi-Fi sarà effettuata dall'Amministratore di Sistema.

5.8 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.

I log relativi all'uso del *File System* e della *intranet*, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
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.

6. Utilizzo degli Strumenti informatici (PC, notebook e altri strumenti con relativi software e applicativi)

6.1 Il dipendente / collaboratore è consapevole che gli Strumenti forniti sono di proprietà dell'Ente 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 si deve quindi attenere alle particolari regole di utilizzo degli Strumenti di seguito descritte.

6.2 L'accesso agli Strumenti è protetto da password. Per l'accesso devono essere utilizzati username e password assegnate dall'Amministratore di Sistema (cfr. paragrafo 4). A tal proposito si rammenta che essi sono strettamente personali e l'Utente è tenuto a conservarli con la massima segretezza. Nel caso di PC e notebook non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

6.3 Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari, evitando ogni possibile forma di furto, smarrimento, danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni furto, smarrimento, malfunzionamento e/o danneggiamento.

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

6.5 L'Utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) 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.

6.6 Eventuali informazioni archiviate sul PC locale devono comunque essere esclusivamente quelle necessarie all'attività lavorativa svolta.

6.7 La gestione dei dati su PC è demandata all'Utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni i dati che possono essere utilizzati anche da altri Utenti, evitando di mantenere l'esclusività su di essi.

6.8 Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.

6.9 L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file e applicazione che ritenga essere pericolosa per la sicurezza dei PC, per la rete locale e i server, nonché può cambiare tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici. L'Amministratore di Sistema può, inoltre, procedere in qualunque momento alla rimozione di ogni applicazione che riterrà essere non pertinente allo svolgimento delle attività aziendali.

6.10 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 e garantirne il corretto funzionamento.

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

6.12 È vietato l'utilizzo di supporti di memoria (chiavi USB, CD-ROM, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

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

6.14 È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

6.15 Nel caso in cui l'Utente dovesse notare comportamenti anomali del PC, l'Utente è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

6.16 Il datore di lavoro può accedere alle postazioni di PC assegnate ai dipendenti nei casi, con le modalità e per le finalità descritte al punto 9.6 e paragrafo 12.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui server o sui router, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
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 strumento di adeguata informazione sulle modalità d'uso degli Strumenti e di effettuazione dei controlli ai sensi del GDPR.

7. Utilizzo di Internet

7.1 È ammessa la navigazione in siti web considerati correlati con la prestazione lavorativa, ad es. siti istituzionali, siti degli Enti locali, siti Internet di fornitori e partner. L'accesso è consentito dal *proxy* con le relative *policy* di sicurezza debitamente implementate e 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, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

7.3 È vietato a chiunque il download di qualunque tipo di software prelevato da siti Internet, se non espressamente autorizzato dall' Amministratore di Sistema. Del pari è vietato l'upload di qualsivoglia software non autorizzato espressamente dall'Amministratore di Sistema.

7.4 L'Ente si riserva di bloccare l'accesso a siti web considerati "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, l'Utente potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.

7.5 Nel caso in cui, per ragioni di servizio, vi sia l'esigenza di disporre di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una e-mail indirizzata all'Amministratore di Sistema e, in copia, al Responsabile di Area/Ufficio, nella quale devono essere 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 paragrafi 13 e 14 del presente Regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

7.6 È tassativamente 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 dalla Direzione e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

7.7 È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet dai dispositivi informatici assegnati, tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema e della Direzione.

7.8 Con i dispositivi informatici assegnati, sono assolutamente vietate la partecipazione a Forum non professionali e Social Network, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati) e di bacheche elettroniche nonché le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

7.9 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'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 e alle e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Non sono consentiti strumenti di messaggistica istantanea distribuiti da società con sede in Paesi considerati non adeguati dalla Commissione Europea.

7.10 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino la banda in modo rilevante, come ad esempio 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. Utilizzo della posta elettronica certificata

8.1 L'indirizzo di posta elettronica certificata istituzionale dell'Azienda è ater.tv@pecveneto.it.

8.2 Le strutture aziendali utilizzano la casella di PEC quale canale privilegiato per lo scambio di documenti informatici con altri Enti e Amministrazioni, società e professionisti.

8.3 È obbligatorio l'utilizzo della PEC per la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna ai sensi dell'art. 48 del d.lgs. 82/2005.

8.4 Nel rispetto della vigente normativa in materia di appalti pubblici, i dipendenti designati quali Responsabile Unico del Procedimento (RUP) sono muniti di casella PEC da rendere nota all'ANAC per le comunicazioni, prioritariamente in ricezione, attinenti alle procedure di affidamento di lavori, servizi e forniture.

8.5 L'attribuzione e revoca di ulteriori caselle di PEC a uffici o dipendenti aziendali è di competenza del Direttore, tramite l'Ufficio servizi informatici.

8.6 Eventuali modifiche all'assetto organizzativo dell'ATER potranno determinare modifiche nell'elenco delle strutture aventi caselle di PEC con eventuale revoca e/o nuova attribuzione. Resta salvo che per le comunicazioni istituzionali è necessario l'utilizzo della casella di posta elettronica istituzionale.

9. Utilizzo della posta elettronica

9.1 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.

9.2 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.

9.3 Tutte le comunicazioni pervenuti a caselle di posta elettronica e inerenti procedimenti aziendali o che comportano un impegno dell'azienda devono essere protocollate.

9.4 È fatto divieto di utilizzare indirizzi e-mail private per comunicazioni inerenti all'attività aziendale.

9.5 L'iscrizione a *mailing-list o newsletter* esterne utilizzando l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

9.6 L'accesso del datore di lavoro alle e-mail aziendali dei dipendenti è legittimo nel caso in cui si possa ragionevolmente ritenere che il dipendente stia utilizzando le e-mail aziendali di cui ai punti precedenti 9.1 oppure 9.2 per finalità estranee a quelle lavorative e segnatamente per finalità personali o illecite. Rientrano nell'ambito delle finalità illecite anche la raccolta, conservazione, trasmissione o diffusione di informazioni personali o aziendali apprese in occasione del rapporto di lavoro, quando il lavoratore non sia autorizzato a farlo. Nella medesima casistica il datore di lavoro può accedere ad ogni tipo di device aziendale (smartphone, postazione PC, tablet, ecc.) e messaggistica effettuata con dispositivi

aziendali. In tutti i casi menzionati, il datore di lavoro procederà secondo il principio di proporzionalità, così come previsto dal Garante per la protezione dei dati personali, e secondo le modalità meglio descritte al paragrafo 12. Nell'effettuazione di tali verifiche il datore di lavoro potrà avvalersi di sistemisti o tecnici all'uopo incaricati, con formale atto di nomina di soggetto autorizzato al trattamento dei dati personali o con contratto di nomina di responsabile esterno del trattamento. Nello svolgimento di tali attività dovrà essere altresì rispettato il principio di minimizzazione dei dati raccolti, da intendersi in relazione alla natura dell'illecito ricercato. Le informazioni raccolte potranno essere utilizzate ai fini del rapporto di lavoro.

9.7 In caso di controversia giudiziaria o indagine, è possibile che il datore di lavoro debba accedere, tramite l'Amministratore di Sistema o di sistemisti o tecnici all'uopo incaricati, alla corrispondenza e-mail e consegnarla a terzi.

9.8 In casi eccezionali, ad esempio per esigenze tecniche o di sicurezza, o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, il datore di lavoro può accedere in consultazione alla corrispondenza presente nella e-mail disattivata del dipendente cessato, tramite l'Amministratore di Sistema o di sistemisti o tecnici all'uopo incaricati.

9.9 Allo scopo di garantire sicurezza alla rete, deve evitarsi l'apertura di 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 l'Amministratore di Sistema per una valutazione dei singoli casi.

9.10 Non è 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.

9.11 Nel caso fosse necessario inviare allegati "pesanti" (fino a 10 MB), è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalente. Nel caso di allegati ancora più voluminosi, è necessario rivolgersi all'Amministratore di Sistema.

9.12 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, i dati personali e/o particolari di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

9.13 Non è consentito 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 quest'ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office", facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio….@xxxx. Per tale eventualità rivolgersi all'Amministratore di Sistema.

9.14 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 e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta è tenuto a 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. È compito del Dirigente/Responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile.

9.15 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del Dirigente/Responsabile 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.

9.16 È vietato inviare messaggi di posta elettronica in nome e per conto di un altro Utente, salvo sua espressa autorizzazione.

9.17 La casella di posta elettronica personale 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, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

9.18 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico.

9.19 In caso di cessazione del rapporto lavorativo, la e-mail affidata all'Utente viene disattivata nei tempi tecnici necessari. È raccomandabile che nell'ultimo mese di servizio venga inviata una e-mail ai contatti in rubrica per informare della cessazione del rapporto, facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni, oppure indicando un indirizzo e-mail alternativo preferibilmente di tipo collettivo, tipo ufficio….@xxxx. Per tale eventualità rivolgersi all'Amministratore di Sistema. È necessario inoltre impostare nell'ultimo giorno di servizio un messaggio "Out of Office", anche in tal caso facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni, oppure indicando un indirizzo e-mail alternativo preferibilmente di tipo collettivo, tipo ufficio….@xxxx. Per tale eventualità rivolgersi all'Amministratore di Sistema.

9.20 In caso di imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio o per motivi di sicurezza del sistema informatico, l'Ente può, per il tramite dell'Amministratore di Sistema e nel rispetto del principio di proporzionalità disciplinato da questo Regolamento, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. È compito del Dirigente/Responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile.

9.21 Le informazioni eventualmente 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.

10. Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti

10.1 Il telefono 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.

10.2 Quando viene assegnato un cellulare/smartphone di servizio all'Utente, quest'ultimo è responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (v. paragrafo 6), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. Si raccomanda, in particolare, il rispetto delle regole per una corretta navigazione in Internet (v. paragrafo 7), se consentita.

10.3 Con riguardo agli 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.

10.4 È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Area/Ufficio.

10.5 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area/Ufficio.

10.6 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, se possibile.

10.7 Le stampanti e le fotocopiatrici devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

10.8 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.

10.9 Il datore di lavoro può eseguire verifiche sugli smartphone assegnati per finalità di servizio, secondo i principi e con le modalità previste al paragrafo 12.

11. Assistenza agli Utenti e manutenzioni

11.1 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 problemi 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 aggiornamento software e manutenzione preventiva hardware e software.

11.2 Gli interventi tecnici possono avvenire, previo consenso dell'Utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'Utente stesso.

11.3 Qualora l'intervento tecnico in loco o 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.

11.4 L'accesso in teleassistenza sui PC della rete 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.

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

12. Controlli sugli Strumenti (art. 6.1 delle Linee guida del Garante per posta elettronica e internet[1], ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 I controlli sugli strumenti informativi utilizzati dai lavoratori devono rispettare i seguenti criteri:

- **Proporzionalità:** il controllo e l'estensione dello stesso deve rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resta sempre entro i limiti minimi;

[1] Del. n. 13 del 1° marzo 2007.

- **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 I controlli possono avvenire esclusivamente per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia e la manutenzione del sistema informatico e per la salvaguardia delle informazioni personali ed aziendali sensibili.

12.3 In ottemperanza al principio di proporzionalità, viene applicata la seguente procedura:

- 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;
- successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente può autorizzare il personale addetto al controllo, potendo così accedere alle informazioni con possibilità di rilevare file 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 dell'indirizzo IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

12.4 Qualora il rischio di compromissione del sistema informativo sia imminente e grave, così come nel caso in cui l'illecito sia da ritenersi grave e segnatamente in caso di illecita raccolta, trasmissione, conservazione o diffusione di informazioni personali o aziendali sensibili, o se si tratta di prevenire o interrompere la commissione di reati, a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti precedenti, l'Amministratore di Sistema, eventualmente insieme al tecnico nominato responsabile esterno del trattamento, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.5 L'Ente, a mezzo dell'Amministratore di Sistema o di soggetto all'uopo autorizzato o nominato responsabile esterno del trattamento, può altresì accedere agli Strumenti informatici o agli account in dotazione ai lavoratori per improcrastinabili esigenze produttive, ad esempio in caso di assenza o temporanea irreperibilità del lavoratore o di cessazione dello stesso, nel caso in cui quest'ultimo non abbia rimesso a disposizione dell'Ente le informazioni stesse. In tal caso si osserva la seguente procedura:

- redazione di un atto da parte del Direttore e/o Responsabile dell'Area/Ufficio che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
- 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;
- redazione di un verbale che riassuma i passaggi precedenti.

12.6 In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

12.7 Qualora indirettamente si riscontrino file o informazioni anche personali, esse possono 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, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16.

12.8 In caso di nuovo accesso da parte dell'Utente allo Strumento informatico oggetto di controllo, lo stesso deve avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

13. Conservazione dei dati

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/16 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*), la cui conservazione non sia necessaria, sono cancellati entro dodici mesi dalla loro produzione.

13.2 In casi eccezionali, ad esempio per 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, è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate e qualora i mezzi tecnici lo consentano.

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

14. Partecipazioni a Social Media

14.1 L'utilizzo a fini promozionali e commerciali 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 specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli Utenti o collaboratori.

14.2 È vietata la partecipazione agli stessi social media durante l'orario di lavoro. Il divieto deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi.

14.3 Anche al di fuori dell'orario di lavoro, la condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza delle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, le informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in corso di svolgimento presso gli uffici. Ogni comunicazione e divulgazione di contenuti, inoltre, deve 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 può quindi inserire il nominativo e il logo dell'Ente, né può pubblicare disegni, modelli od altro, connesso ai citati diritti. Ogni deroga a quanto sopra disposto può, peraltro, avvenire solo previa specifica autorizzazione della Direzione.

14.4 L'Utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non può 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 d'Area/Ufficio.

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

15. Sanzioni disciplinari

15.1 Il presente Regolamento è stato approvato dal Direttore e, pertanto, è vincolante per tutti coloro che operano all'interno dell'Ente.

15.2 La violazione delle disposizioni previste dal presente Regolamento costituisce illecito disciplinare.

15.3 La sua pubblicizzazione avviene a cura del Responsabile dell'Ufficio sistemi informatici e dell'Amministratore di Sistema nelle seguenti forme:

- trasmissione per posta elettronica interna a tutti i Dirigenti e Responsabili e a tutto il personale provvisto di e-mail;
- attraverso la rete informatica interna;
- mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.

15.4 Tutti gli Utenti possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente Regolamento tramite comunicazione al Responsabile del personale o all'Amministratore di Sistema, il quale, dopo attenta valutazione, se ritenute conferenti, le sottoporrà al Direttore per l'eventuale approvazione.