Comune di Alassio

Regolamento per l'utilizzo degli strumenti informatici

Versione 1.0 – Novembre 2021

Sommario

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Alassio 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 del Comune stesso. Da ciò deriva la necessità, raccomandata anche dal Garante per la protezione dei dati personali, di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare, conseguentemente, eventuali usi scorretti che possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli articoli 2104 e 2105 del codice civile.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Comune di Alassio adotta il presente Regolamento diretto ad evitare che determinati comportamenti possano innescare problemi o minacce alla sicurezza nel trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo le dotazioni oggetto del presente regolamento strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale ed il conseguente diritto alla riservatezza ed alla dignità, così come sanciti dallo Statuto dei Lavoratori e dalla normativa, nazionale e comunitaria, applicabile in materia di protezione dei dati personali.

Questo Regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dalla normativa italiana ed europea in materia, dalle Linee Guida del Garante della Privacy per Posta Elettronica ed Internet (Delibera n. 13 del 01/03/2007) e dalla legislazione vigente in materia di responsabilità amministrativa delle persone giuridiche (D.Lgs. 231/01 e s.m.i.) e fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Si precisa che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

Il presente Regolamento opera in sinergia con il *Piano di protezione dei Dati Personali e gestione del rischio di violazione* ed ai relativi allegati che contengono le procedure e le policy aziendali definite nell'ambito della sicurezza informatica e delle modalità di utilizzo degli strumenti e di gestione dei dati e del patrimonio documentale dell'Ente.

PARTE I

Art. 1 – Oggetto e finalità

Il presente Regolamento è redatto sulla base dei seguenti riferimenti normativi:

- **Legge 20.5.1970, n. 300** recante "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" con particolare riferimento all'art. 4, comma 1, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- **D.Lgs. 30/06/2003 n. 196** recante "*Codice in materia di protezione dei dati personali*" (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs. n. 101/18);
- **Regolamento Europeo 679/16** "*General Data Protection Regulation*" (d'ora in avanti Reg. 2016/679 o GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- **"Linee guida del Garante per posta elettronica e internet"** in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- **D.Lgs. n. 151/2015** (c.d. *Jobs Act*) recante "*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183.",* con particolare riferimento all'art. 23 che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;
- **D.Lgs. 10/08/2018 n. 101** recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).*";
- **C.C. Art. 2104 "Diligenza del prestatore di lavoro"**, *il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*;
- **C.C. Art. 2105 "Obbligo di fedeltà"**, *il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio*;
- **C.C. Art. 2106 "Sanzioni disciplinari"**, *l'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione*.

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

Art. 2 – Principi generali e riservatezza nelle comunicazioni

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

a) *Liceità e correttezza*, secondo cui il trattamento di dati personali è lecito solo quando previsto da procedimenti amministrativi che rientrano nelle funzioni istituzionali dell'Ente, quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o ancora quando il trattamento è necessario per adempiere un obbligo legale a cui è soggetto l'Ente. In tutti gli altri casi l'interessato dovrà aver espresso il proprio consenso (un consenso informato) al trattamento dei propri dati;

b) *Trasparenza*, secondo cui devono essere trasparenti le modalità con cui sono raccolti e utilizzati i dati personali e devono essere facilmente accessibili e comprensibili le informazioni e comunicazioni relative al trattamento (identità del titolare del trattamento, finalità del trattamento, diritti degli interessati…);

c) *Limitazione delle finalità*, secondo cui i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente devono essere trattati in una modalità che sia compatibile con tali finalità. Il trattamento dei dati per finalità diverse da quelle per le quali sono stati inizialmente raccolti è consentito solo se compatibile con tali iniziali finalità;

d) *Minimizzazione dell'uso*, secondo cui i dati personali devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati;

e) *Esattezza*, secondo cui i dati personali devono essere sempre esatti e aggiornati. Eventuali inesattezze devono essere tempestivamente rettificate ovvero i dati inesatti devono essere cancellati;

f) *Limitazione della conservazione*, secondo cui i dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati. Valgono in ogni caso le disposizioni legislative e regolamentari in materia di documentazione amministrativa ed è poi possibile l'ulteriore trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici.

Il dipendente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali, gli elementi e le 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 Dirigente responsabile;

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 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 lavoratori con mansioni di front office;

d) Per le riunioni e gli incontri con utenti, cittadini, fornitori, consulenti e collaboratori dell'Ente è necessario porre particolare attenzione alla riservatezza, utilizzando apposite sale dedicate e/o evitando la presenza di soggetti non interessati.

Art. 3 – Tutela del lavoratore

Alla luce dell'art. 4, comma 1, L. n. 300/1970, 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 sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

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

Art. 4 – Campo di applicazione

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 lo stesso intrattenuto.

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 "incaricato del trattamento".

PARTE II

Art. 5 – Utilizzo delle postazioni di lavoro

Il dipendente/collaboratore è consapevole che gli strumenti informatici forniti sono di proprietà del Comune di Alassio 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 seguenti regole di utilizzo degli strumenti informatici.

L'accesso alle dotazioni dell'Ente è protetto da password; per l'accesso devono essere utilizzate le credenziali assegnate dagli Amministratori di Sistema. A tal proposito si rammenta che esse sono strettamente personali e l'utente è tenuto a conservarle nella massima segretezza. Qualora l'utente abbia il dubbio che le proprie credenziali non siano più riservate ha facoltà di rinnovarle in ogni momento. L'accesso al sistema da parte di persone non autorizzate per mezzo di credenziali custodite in modo incauto può esporre l'utente titolare delle stesse a conseguenze disciplinari, civili e penali.

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

Non è consentito all'utente modificare le caratteristiche hardware e software impostate sulle dotazioni assegnate, salvo preventiva autorizzazione da parte degli Amministratori di Sistema. In particolare non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Ufficio Informatica. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.

Gli operatori dell'Ufficio Informatica sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Detti interventi potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata o impedimento dell'utente e non sia possibile procedere altrimenti.

Il personale dell'Ufficio Informatica ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

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 postazione 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. A maggior tutela degli utenti dovrà essere impostato lo screen saver a tempo con l'obbligo di reintrodurre le credenziali per lo sblocco del terminale. Se più utenti utilizzano la stessa postazione di lavoro per trattare dati personali di terzi, effettuano il "log out" (scollegamento dalla rete) ogni volta che un diverso utente deve utilizzare la propria postazione abituale. Al termine della giornata lavorativa i PC dovranno essere spenti salvo sia necessario che la postazione debba rimanere accesa per permettere il collegamento da remoto in regime di smart working: in tal caso l'utente dovrà effettuare il "log out" prima di allontanarsi dalla postazione.

Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.

La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle cartelle di rete dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

Gli operatori dell'Ufficio Informatica o gli Amministratori di Sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

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.

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

È vietato l'utilizzo di supporti di memoria (chiavi USB, dischi fissi esterni, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti informatici dell'Ente, salvo che il supporto utilizzato sia stato autorizzato dall'Ufficio Informatica. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Ufficio Informatica.

È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Ufficio Informatica.

Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente all'Ufficio Informatica. Nel caso vengano rilevati dei virus dovranno essere seguite le indicazioni di cui all'art. 13 del presente Regolamento.

I log relativi all'utilizzo di strumenti informatici, reperibili nella memoria degli strumenti stessi ovvero sui server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso gli Amministratori di Sistema, 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 articolo 21 del presente Regolamento.

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 2016/679 "General Data Protection Regulation".

Art. 6 – Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dell'Ufficio Informatica, previa formale richiesta del Dirigente dell'Ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente o il nuovo collaboratore.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Ufficio Informatica, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Ad eccezione delle sole utenze di servizio per sistemi software centralizzati, tutte le user id dovranno essere nominative e riconducibile ad una persona fisica.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi. Il sistema avvertirà l'utente della scadenza della password e della necessità di modifica della stessa.

La parola chiave, formata da lettere (maiuscole o minuscole), numeri e caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato. Per le utenze amministrative le password dovranno avere una lunghezza minima di 14 caratteri. Tutte le password dovranno rispettare alcuni requisiti minimi di robustezza e non potranno essere riutilizzate prima di 6 mesi dall'ultimo utilizzo. Tali limitazioni saranno gestite direttamente dal sistema. Le presenti disposizione tengono conte delle vigenti linee guida dell'AgID in materia di sicurezza informatica. Laddove nuove versioni di tali linee guida dovessero introdurre misure diverse e/o più stringenti, le stesse dovranno essere osservate in sostituzione di quelle attuali.

Qualora la parola chiave dovesse venir sostituita in quanto abbia perduto la propria riservatezza, l'Ufficio Informatica provvederà ad impostare una nuova password provvisoria concordata con l'utente impostando a sistema l'obbligo di modifica della stessa al primo utilizzo.

Poiché l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, il titolare può assicurare come segue la disponibilità dei citati dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. Gli Amministratori di Sistema attiveranno, su formale richiesta del Dirigente competente, un profilo di accesso temporaneo, da utilizzarsi esclusivamente per il periodo necessario. Al termine di tale periodo, il profilo temporaneo verrà eliminato.

Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Dirigente di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Informatica la data effettiva a partire dalla quale le credenziali saranno disabilitate.

È assolutamente vietata, e punita ai sensi dell'art. 615 quater c.p. al ricorrere delle condizioni di legge, la detenzione abusiva, la diffusione e l'indebita appropriazione di credenziali di autenticazione.

Art. 7 – Utilizzo della rete

Per l'accesso alle risorse informatiche del Comune di Alassio attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 6.

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

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 Ufficio. Tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sui dischi locali delle postazioni di lavoro, 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 dagli Amministratori di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sulle postazioni di lavoro viene rimosso, 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 degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo (se autorizzati dall'Ufficio Informatica). 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.

Poiché l'accesso alle cartelle di rete è differenziato in base agli Uffici di appartenenza, è disponibile una cartella libera denominata "Scambio" ed organizzata in sottocartelle nominative che gli utenti posso utilizzare per scambiarsi documenti. Tale struttura di cartelle deve essere utilizzata come mero luogo di interscambio di files da spostare tempestivamente nelle cartelle di rete degli Uffici. È pertanto vietato lasciare in deposito documenti per lungo tempo in tali cartelle in quanto, oltre a non essere oggetto di

backup, non verrebbe garantito il rispetto della riservatezza degli stessi. Peraltro il contenuto della cartella "Scambio" può essere cancellato in qualsiasi momento dagli Amministratori di Sistema, anche senza preavviso, in caso di emergenza dovuta all'esaurimento dello spazio di archiviazione di rete.

L'acceso alle risorse condivise ed ai software gestionali dell'Ente con le credenziali di cui all'art. 6 è legato ad un sistema di autorizzazione dove vengono definiti dei profili che permettono di definire i diritti e le limitazioni di ogni singolo utente in merito alle operazioni che lo stesso può effettuare sui vari dispositivi e sui vari sistemi software. I profili di autorizzazione, per ciascun utente/incaricato o per classi omogenee di utenti/incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

È fatto obbligo agli utenti di assicurarsi di non lasciare le proprie stampe, anche qualora siano semplici bozze o stampe errate, presso le stampanti dipartimentali del palazzo comunale essendo le stesse posizionate ad ogni piano in zone di passaggio con libero accesso del pubblico, e di ritirare celermente dette stampe con particolare riguardo a quelle contenenti dati personali e/o sensibili. In caso di malfunzionamento degli apparati gli utenti dovranno contattare il personale dell'Ufficio Informatica ed attendere fino alla risoluzione del problema o alla cancellazione della coda di stampa.

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

Senza il consenso del Dirigente competente è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul server o sul PC in dotazione) su repository esterni (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

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.

Il Comune di Alassio mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna o tramite analoga connessione realizzata tramite il client di accesso al firewall dell'Ente. L'accesso viene concesso a consulenti e tecnici che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso da remoto dovranno seguire le prescrizioni dell'articolo 6.

All'interno delle sedi del Comune possono essere rese disponibili anche reti senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse dell'Ente e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti e tecnici che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'accesso alla sola rete internet in modalità Wi-Fi viene anche concessa ad utenti esterni generici, laddove ne facciano richiesta, tramite l'emissione di un voucher, ovvero di credenziali monouso a tempo.

Gli Amministratori di Sistema si riservano 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.

I log relativi all'uso del File System e della intranet dell'Ente, nonché i file salvati o trattati su Server o PC, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso gli Amministratori di Sistema, 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 art. 21 del presente Regolamento.

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 2016/679 "General Data Protection Regulation".

Art. 8 – Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti di memorizzazione rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili o comunque di carattere riservato, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale dell'Ufficio Informatica e seguire le istruzioni da questo impartite.

In ogni caso, i supporti contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

Non è consentita l'uscita dalle sedi comunali di hardware e supporti magnetici, ottici o di altra natura e cartacei, se non preventivamente autorizzati.

È vietato l'utilizzo di supporti rimovibili personali.

L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

È interdetta l'installazione o l'uso di supporti rimovibili sulle stazioni di lavoro. Per eventuali necessità in proposito occorrerà farsi autorizzare dall'Ufficio Informatica.

Art. 9 – Utilizzo dei dispositivi mobili - Precauzioni nello Smart Working

L'Ufficio Informatica fornisce su richiesta dispositivi mobili quali notebook, cellulari, internet key; fornisce inoltre il necessario supporto agli utenti per il corretto utilizzo di essi.

L'utente è responsabile del dispositivo mobile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

A tali dispositivi si applicano le regole di utilizzo previste dal presente regolamento con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

Anche per tali dispositivi l'installazione di programmi dovrà essere effettuata a cura dell'Ufficio Informatica, al fine di garantire il rispetto dei criteri di sicurezza informatica nell'uso della rete.

I dispositivi mobili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Gli utenti devono inoltre comunicare all'Ufficio Informatica eventuali guasti o anomalie, riscontrate nell'uso dei dispositivi, e informare tempestivamente di eventuali smarrimenti o furti.

L'utilizzo di tali dispositivi è limitato all'utente o agli utenti assegnatari; è quindi vietato cederne l'uso, anche temporaneo, a terzi se non preventivamente autorizzato.

I dati personali e riservati di norma non possono essere registrati su tali dispositivi mobili; diversamente devono essere gestiti con la supervisione dell'Ufficio Informatica.

Tali disposizioni si applicano anche nei confronti di eventuali incaricati esterni.

Smart working: le precauzioni Privacy

Il lavoro agile (o smart working) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli spaziali.

Tale modalità aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività.

La definizione di smart working, contenuta nella Legge n. 81/2017, pone l'accento sulla flessibilità organizzativa, sulla volontarietà delle parti e sull'utilizzo di strumentazioni che consentano di lavorare da remoto (come ad esempio: pc portatili, tablet e smartphone).

Nell'ambito della gestione in deroga alla normativa ordinaria per fronteggiare l'emergenza sanitaria dovuta al Covid-19 valgono le norme straordinarie emesse dal Governo e dal Parlamento nei limiti di natura organizzativa, giuridica e temporale in esse contenuti e si evidenzia l'importanza di tale modalità lavorativa a tutela della salute del dipendente ed a garanzia della continuità operativa dell'Ente.

Il dipendente che sia stato autorizzato allo svolgimento di attività lavorativa in regime di smart working verrà dotato in via temporanea, se non già precedentemente assegnata, della strumentazione necessaria. Tale strumentazione consiste indicativamente in un pc portatile/postazione fissa configurata per l'accesso sicuro alla rete ed ai sistemi gestionali comunali. Tali dotazioni permetteranno al dipendente di lavorare da remoto con le stesse modalità del lavoro eseguito in ufficio, salvo l'impossibilità di stampare in loco i documenti (rimangono disponibili le stampanti di rete presso gli uffici comunali). Qualora il dipendente voglia attivare il trasferimento di chiamata dall'ufficio verso il proprio recapito telefonico o verso il cellulare aziendale, egli dovrà, previa formazione, attivare tale funzionalità sul proprio telefono fisso il giorno precedente a quello previsto per lo smart working e disattivarla il giorno successivo. Le chiamate in entrata pervenute al centralino e destinate all'operatore in Smart working saranno trasferite al recapito telefonico impostato.

Alla strumentazione fornita si applicano tutte le norme già previste ai punti precedenti.

In particolare, in conformità al Regolamento UE 2016/679 in materia di protezione del dato personale, il dipendente che lavora in smart working dovrà prestare particolare cautela nella conservazione dei dispositivi a lui assegnati. L'eventuale perdita o sottrazione di uno di detti dispositivi costituisce una forma di "data breach", ovvero di violazione dei dati personali e potrebbe costituire un serio rischio per la conoscibilità a terzi non autorizzati dei dati personali in esso contenuti.

Nel caso di smarrimento o sottrazione di uno dei dispositivi concessi in uso al dipendente in smart working, lo stesso sarà tenuto a darne immediata comunicazione telefonica e scritta al proprio Dirigente ed all'Ufficio Informatica entro 24 ore dalla conoscenza del fatto (sottrazione o perdita).

Il dipendente non potrà mai lasciare incustodito il bene a lui assegnato proprio per evitare un'eventuale sottrazione dello stesso.

Si ricorda, inoltre, che nessun soggetto terzo oltre al dipendente autorizzato allo smart working potrà conoscere il contenuto dei documenti di lavoro siano essi in forma cartacea che elettronica; pertanto il dipendente nell'esercizio della sua attività di smart working dovrà prestare ogni cautela in modo che terzi o familiari o conviventi non possano venire a conoscenza di detti dati personali utilizzati o di informazioni riservate nei luoghi ove si esercita lo smart working.

Art. 10 – Utilizzo dei telefoni, fax, fotocopiatrici e stampanti dell'Ente

Il dipendente è consapevole che gli strumenti di stampa, così come anche il telefono ed il fax dell'Ente, sono di proprietà del Comune di Alassio e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.
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 l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.
Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici 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, se consentita.
Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Ufficio Informatica.
È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Settore.
Per quanto concerne l'uso delle stampanti e degli apparati multifunzione 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.

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 caso di inceppamento o malfunzionamento del dispositivo di stampa l'utente dovrà contattare tempestivamente l'Ufficio Informatica ed assicurarsi che detta stampa venga rimossa dalla coda di stampa del dispositivo o attendere presso il dispositivo stesso fino alla risoluzione del problema.

PARTE III

Art. 11 – Utilizzo di Internet

Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.
È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa.
L'accesso è consentito dal firewall dell'Ente con le sue policy di sicurezza debitamente implementate e aggiornate.
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.
È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema.
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 gli Amministratori di sistema per uno sblocco selettivo.
Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto firewall, è necessario richiedere lo sblocco mediante una nota protocollata e sottoscritta dal Dirigente competente indirizzata all'Ufficio Informatica nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare l'art. 14 del presente regolamento. Al termine dell'attività saranno ripristinarti i filtri nella situazione iniziale.
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 dal Dirigente competente, con il rispetto delle normali procedure di acquisto.
È assolutamente 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.
È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network (salve esigenze d'ufficio), l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali.
Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda come, a titolo esemplificativo, filmati (tratti da youtube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.
L'Ente, per il tramite degli Amministratori 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. 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 registra per 180 giorni 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.
In tali casi i controlli avverranno nelle forme indicate al successivo articolo 21 del presente Regolamento.
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 2016/679 “General Data Protection Regulation”.

Art. 12 – Utilizzo della posta elettronica

La casella di posta elettronica assegnata all’utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Ad ogni utente viene fornito un account e-mail istituzionale nominativo nel formato *nome.cognome*@comune.alassio.sv.it. L’utilizzo dell’e-mail deve essere limitato esclusivamente a scopi dell’Ente ed è assolutamente vietato ogni utilizzo di tipo privato; la “personalizzazione” dell’indirizzo non comporta il suo carattere “privato”, in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

L’Ente fornisce, altresì, degli indirizzi di posta elettronica associati 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.

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

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 l’Ufficio Informatica per una valutazione dei singoli casi.

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.

Nel caso fosse necessario inviare allegati “pesanti” (sopra i 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi, almeno un giorno prima, all’Ufficio Informatica. Nei casi in cui detti allegati siano stati realizzati da professionisti esterni, come nel caso dei progetti, è opportuno prevedere, già all’atto dell’affidamento dell’incarico, la richiesta di produrre documenti già ottimizzati in modo da avere dimensioni contenute e realizzati in formati adatti alla conservazione sulla base delle vigenti linee guida AgID, senza contenuti dinamici (es. file CAD incapsulato in un file PDF) se non strettamente necessari e con immagini esportate a risoluzioni non superiori a quelle necessarie per la consultazione o la stampa.

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

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 questa ultima ipotesi, è raccomandabile utilizzare un messaggio “Fuori sede” 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. Rivolgersi all’Ufficio Informatica per tale eventualità.

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 Dirigente competente quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente competente assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.

Qualora non sia possibile acquisire ordinariamente informazioni o comunicazioni che, se non ricevute o recepite con ritardo, potrebbero arrecare un evidente danno alla società, e nel caso non sia stato nominato il fiduciario di cui al punto precedente, sarà consentito al superiore gerarchico dell'utente, tramite il personale dell'Ufficio Informatica e previa informativa al DPO, di accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario e non sia possibile procedere altrimenti cambiando la password e informando il lavoratore interessato alla prima occasione utile. Quest'ultimo accesso deve essere formalmente motivato e sottoscritto dal superiore gerarchico. Il provvedimento di cui sopra e il verbale a rappresentazione delle operazioni eseguite sono poi inviati via mail al lavoratore interessato e per conoscenza al DPO.

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

E' inoltre espressamente vietato, salvo autorizzazione espressa del proprio Responsabile, salvare/stampare/inoltrare e portare fuori dai luoghi di lavoro documentazione istituzionale. A titolo esemplificativo e non esaustivo è vietato:

- stampare e-mail istituzionali per scopi personali;
- inviare informazioni sensibili ad indirizzi di posta personali;
- fotocopiare/scansionare documentazione istituzionale per scopi personali;
- inoltrare a terzi estranei all'Ente documentazione interna/informazioni ricevute per mezzo di strumenti informatici o via cartacea, salvo che non sia funzionale allo svolgimento di prestazioni professionali a favore dell'Ente stesso.

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 dell'Ente.

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.

Le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.

L'Ente, per il tramite degli Amministratori 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 degli Amministratori di sistema può, secondo le procedure indicate successivo punto 21 del presente Regolamento, accedere all'account di posta elettronica dell'Ente, prendendo visione dei messaggi, salvando o cancellando file.

In caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà sospesa per un periodo di 2 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 di natura procedimentale) ovvero cancellandolo (se il messaggio non ha contenuto di interesse per l'Ente, come, ad esempio, la mail di tipo Spam). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail dell'Ente.

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 2016/679 "General Data Protection Regulation".

Art. 13 – Protezione antivirus

Il sistema informatico del Comune di Alassio è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file non autorizzati, etc.). È fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale dell'Ufficio Informatica.

Ogni dispositivo di memorizzazione 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 dell'Ufficio Informatica.

PARTE IV

Art. 14 – Partecipazioni a Social Media

L'utilizzo a fini promozionali di Facebook, Twitter, Instagram, 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.

Pur garantendo il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare la propria immagine ed il patrimonio, anche immateriale, 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 salvo che per il personale espressamente autorizzato.

A tal fine si richiamano le norme in materia di diritti e doveri del pubblico dipendente, con particolare riferimento al D.P.R. 16 aprile 2013 n. 62 "Codice di comportamento dei dipendenti pubblici", ed il vigente Regolamento per la disciplina dell'informazione sull'attività comunale.

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.

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

Art. 15 – Open Government

Il Comune di Alassio riconosce ed incoraggia modalità di esercizio delle proprie funzioni basate su modelli, strumenti e tecnologie che consentono all'Amministrazione di essere "aperta" e "trasparente" nei confronti dei cittadini.

Ferme restando le disposizioni di legge in materia di Open Government l'incaricato dovrà porre particolare attenzione nella pubblicazione e divulgazione di documenti contenenti dati personali, facendo riferimento ai seguenti principi:

- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principi di necessità, pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione on line. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti;
- è, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale o l'orientamento sessuale" (art. 9 del GDPR).

Art. 16 – Videosorveglianza

Il Comune di Alassio utilizza sistemi di videosorveglianza a garanzia dei luoghi pubblici per una serie di finalità tra cui la sicurezza pubblica, la tutela del patrimonio pubblico ed il monitoraggio del traffico.

Ferme restando le disposizioni del Garante della Privacy in materia di Videosorveglianza dovranno essere rispettati i seguenti principi:

- le finalità e le modalità di gestione del sistema di videosorveglianza cittadina sono definite nel vigente Regolamento per l'utilizzo degli impianti di videosorveglianza;
- il periodo di conservazione non deve superare 7 giorni, fatte salve esigenze di ulteriore conservazione in relazione a indagini da parte delle forze dell'ordine o della magistratura;

- le immagini possono essere visionate solo da responsabili o incaricati del trattamento dei dati ai sensi della vigente normativa in materia di protezione dei dati personali.

Art. 17 – Pubblicazione notizie ed eventi sui canali elettronici del Comune

Il comune di Alassio dispone di un proprio portale web istituzionale per la diffusione di informazioni riguardanti gli Organi di governo dell'Ente, gli Uffici, le notizie, gli eventi promossi dall'Amministrazione, etc., oltre a svolgere le funzioni di pubblicità legate all'albo pretorio ed alla sezione trasparente con i contenuti previsti dal D.Lgs. 14 marzo 2013 n. 33 in materia di trasparenza.

A tale strumento si affiancano il portale turistico per la promozione del territorio e per la pubblicazione di eventi e manifestazioni di tipo turistico, un portale informativo di carattere giornalistico con tutte le notizie riguardanti la città di Alassio ed una serie di canali social.

Come già indicato all'articolo 14, l'Ente gestisce ed organizza il piano editoriale legato alla promozione della città ed ai contenuti di carattere informativo, sia turistico che istituzionale, sui portali e sui canali social.

Relativamente alle pagine istituzionali legate agli Uffici ed ai relativi servizi, alla sezione trasparente ed ai servizi on line, gli Uffici sono abilitati ad operare in autonomia per il caricamento e l'aggiornamento dei contenuti, e ne sono responsabili.

Al fine di dare uniformità e correttezza, sia formale che giuridica, del materiale pubblicato, gli utenti dovranno attenersi alle linee guida definite dall'Ufficio Informatica, allegate al Piano di protezione dei dati personali e di gestione del rischio di violazione, e pubblicate sul sito intranet aziendale.

PARTE V

Art. 18 – Assistenza agli utenti e manutenzioni

L'Ufficio Informatica e gli Amministratori di sistema possono accedere ai dispositivi informatici dell'Ente 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 installazione/aggiornamento software e manutenzione preventiva hardware e software.

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

Gli Amministratori di sistema sono altresì autorizzati ad effettuare interventi di tipo emergenziale senza il consenso dell'utente cui la risorsa è assegnata in caso di osservazione di potenziali pericoli per i sistemi informatici dell'Ente, come, ad esempio, il rilevamento di un virus da parte del sistema antivirus centralizzato, o il rilevamento di attività di rete di tipo malevolo da parte di sistemi di intrusion detection o sulla base dell'analisi dei log del firewall. Gli Amministratori di Sistema potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza del sistema informativo e dei dati, sia sui PC assegnati agli utenti sia sulle unità di rete.

L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Ufficio Informatica, 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.

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

Art. 19 – Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza ai sensi del D.Lgs. n. 196/2003, del regolamento europeo UE 2016/679 e della circolare Agid 18 aprile 2017 n. 2/2017, ed in generale a quanto indicato nella lettera di designazione ad incaricato del trattamento dei dati.

In adempimento del provvedimento generale del Garante per la Protezione dei Dati Personali del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e internet" e ai sensi dell'articolo 13 del regolamento europeo UE 2016/679 vengono di seguito indicate alcune informazioni relative al trattamento dei dati personali dei propri dipendenti e/o collaboratori raccolti in esecuzione del presente Regolamento contenente le regole sull'utilizzo degli strumenti informatici, di internet e della posta elettronica.

I dati raccolti saranno trattati esclusivamente per le finalità elencate nel presente regolamento (fra le quali si ricordano a titolo esemplificativo i dati raccolti a seguito di manutenzione degli strumenti informatici nonché quelli raccolti a seguito di controlli per verificare il rispetto da parte degli utenti delle regole qui riprodotte) e saranno trattati con modalità telematiche e/o su supporto cartaceo. Si ricorda agli utenti che il conferimento dei dati per le finalità sopra citate è necessario ai fini dell'utilizzo degli strumenti elettronici forniti in uso all'utente e che di conseguenza l'eventuale rifiuto di fornire tali dati impedirà al Comune di Alassio di garantire agli utenti l'uso stesso degli strumenti. I dati personali raccolti dall'Ente non saranno oggetto di diffusione e potranno essere comunicati esclusivamente a personale di fiducia dello stesso (come ad esempio società di servizi che forniscono supporto nella manutenzione degli strumenti informatici) legati al Comune da vincoli contrattuali che garantiscono la riservatezza e l'integrità delle informazioni trattate. Tutti i dipendenti e/o collaboratori sono titolari dei diritti previsti all'articolo 13 del

regolamento europeo EU 2016/679 che possono essere esercitati con richiesta rivolta al Titolare (Comune di Alassio) o al relativo Responsabile per la Protezione dei Dati (RPD/DPO).

Art. 20 – Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione del rinnovo tecnologico del parco macchine aziendale comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Dirigenza, tramite il personale dell'Ufficio Informatica o di addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Art. 21 – Sistema di controlli graduali e conservazione dei dati

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, comma2), 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 dell'art. 2 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.

L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite degli Amministratori 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, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

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

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni il Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite dell'Ufficio Informatica, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo):

1) 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;
2) Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni contenute negli

strumenti informatici 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 dell'indirizzo IP dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;

3) Qualora il rischio di compromissione del sistema informativo 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 Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, unitamente agli Amministratori di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Controlli per esigenze produttive e di organizzazione.

Per esigenze produttive e di organizzazione si intendono – 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 Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite dell'Ufficio Informatica, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo).

1) Redazione di un atto da parte del Responsabile di Settore che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo strumento;
2) Incarico agli Amministratori di sistema di accedere alla risorsa con credenziali di amministrazione 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;
3) Redazione di un verbale che riassuma i passaggi precedenti;
4) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
5) 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, sempre nel rispetto di quanto disposto dal Regolamento Europeo EU 2016/679 "GDPR".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Settore e dall'Amministratore di Sistema che ha svolto l'attività.

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

Art. 22 – Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. La mancata osservanza delle presenti modalità di utilizzo degli strumenti informatici può dar luogo a procedimenti di carattere disciplinare, fatto salvo che le violazioni non comportino più gravi sanzioni ai sensi della vigente normativa.

PARTE V

Art. 23 – Entrata in vigore del regolamento e pubblicità

Il presente Regolamento entrerà in vigore con la pubblicazione della Deliberazione di approvazione, salvo successive modifiche ed integrazioni.

Tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento, oltre ad essere pubblicato sul sito web istituzionale dell'Ente, sarà disponibile sul sito intranet aziendale http://alassioinside.

Art. 24 – Norme finali

Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'ufficio (ad esempio: collegamento da casa).

Per le attività svolte in regime di smart working si richiama quanto indicato al precedente art. 9.