CITTÀ DI PORTO SAN GIORGIO

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DEL COMUNE DI PORTO SAN GIORGIO

Sommario

Art.1 - Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche *incaricati o utenti*, del Comune di Porto San Giorgio, le indicazioni per una corretta ed adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni software e strumenti informatici dell'Ente.

Si specifica che tutti gli Strumenti utilizzati dal lavoratore, intendendo con ciò le postazioni di lavoro (PDL, ovvero PC, notebook, tablet, smartphone,..), risorse fisiche (es: server, NAS, stampanti, scanner, plotter, dischi esterni o chiavette USB, armadi dati o locali adibiti a datacenter) o logiche (es: aree di lavoro condivise, aree dati personali e condivise, dati e informazioni presenti nei sistemi

gestionali, connessioni di rete), caselle di posta elettronica (e-mail istituzionali o personali) ed altri strumenti con relativi software e applicativi (di seguito più semplicemente indicati come "Strumenti"), **sono messi a disposizione dall'Ente per rendere la prestazione lavorativa**. Gli Strumenti, nonché le relative reti di trasmissione dati dell'Ente a cui è possibile accedere tramite gli stessi, **sono domicilio informatico del Comune di Porto San Giorgio**.

I dati personali e le altre informazioni dell'utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.

Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente.

Tali dati personali ed informazioni sono altresì utilizzabili **a tutti e soli i fini connessi al rapporto di lavoro**, visto 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 sulla protezione dei dati personali.

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, ma solo per il monitoraggio del sistema informativo ai fini di garantirne la sicurezza (es: antivirus, firewall, proxy, sistemi di inventario).

Eventuali attività di assistenza remota sugli strumenti informatici in uso agli utenti vengono effettuate solo dopo l'assenso da parte degli stessi.

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n.300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti **Reg. 679/16** o **GDPR**);
- in attuazione del D. Lgs. n. 196 del 2003, modificato dal D.Lgs. n.101 del 2018 (d'ora in avanti **Codice Privacy**);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- nel rispetto delle funzioni ed indirizzi del "*Responsabile per la transizione al digitale*" (**RTD**) così come definito dall'art.17 del Codice dell'Amministrazione Digitale (D.Lgs.82/2005 e ss.mm.ii., d'ora in avanti **CAD**);
- in attuazione della circolare AGID 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni";
- alla luce dell'articolo 23 del D.Lgs. n.151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa».*

La finalità del Regolamento 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, ad esempio, la posta elettronica, internet e le postazioni di lavoro (PDL), con i relativi software, **sia conforme alle finalità dell'Ente e nel pieno rispetto della legge**.

Si vogliono fornire a tutto il personale le informazioni e le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, che potrebbe comportare delle conseguenze in materia di sicurezza e privacy, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

All'interno dell'Ente è stato istituito un apposito Servizio denominato "Sistema Informatico Comunale" per la gestione degli Strumenti informatici ed il supporto agli utenti. Inoltre è presente il Responsabile per la transizione al digitale, con funzioni di indirizzo, coordinamento, pianificazione e monitoraggio, particolarmente per quanto riguarda il rispetto degli adempimenti normativi relativi alla corretta e adeguata gestione delle informazioni, la sicurezza e la tutela del sistema informatico.

Il presente regolamento recepisce inoltre quanto indicato nelle Misure minime di sicurezza informatica che tutte le pubbliche amministrazioni sono tenute ad attuare e mantenere nel tempo.

Art.2 - Principi generali e di riservatezza nelle comunicazioni

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

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

Il dipendente/collaboratore si attiene alle seguenti regole di trattamento:
a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dell'Ente dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di Settore.
b) È vietata l'estrazione di originali e/o copie cartacee e informatiche per uso personale di documenti, manuali, fascicoli, lettere, dati e informazioni presenti nei sistemi informatici 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 responsabilità del dipendente/collaboratore proteggere le informazioni di carattere istituzionale di cui viene a conoscenza, ed è fatto esplicito divieto di 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.
d) Quando un utente si allontana dalla propria postazione di lavoro deve bloccare la propria sessione di lavoro (o, al limite, terminarla) in modo che la postazione sia protetta dall'accesso di altri soggetti. Lo sblocco deve essere protetto da password;
e) È vietato lasciare in evidenza o comunicare a terzi (es: colleghi) le proprie credenziali di autenticazione ai Sistemi Informatici dell'Ente o il proprio badge per la registrazione delle presenze (anch'esso considerato dispositivo di autenticazione). Sono fatti salvi gli utilizzi da parte di dipendenti per specifiche attività operative agli stessi affidate con il provvedimento di nomina in qualità di incaricati al trattamento.
f) Per le riunioni e gli incontri con Utenti, cittadini, Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate, e rispettare le distanze di cortesia.

Art.3 - Tutela del lavoratore

Alla luce dell'art.4, comma 1, Legge.n.300/1970, la regolamentazione della materia indicata nel presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare i Sistemi Informativi per 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. 679/16.

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/dispositivi di autenticazione.

Tale figura potrà anche venir indicata, ai sensi del GDPR, come "*incaricato del trattamento*".

Art.5 - Gestione, assegnazione e revoca delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alle risorse informatiche (postazioni di lavoro, applicativi, posta elettronica, accesso alle reti) **vengono assegnate dal personale del Servizio "Sistema Informatico Comunale", previa formale richiesta scritta** (tramite nota interna di protocollo indirizzata all'Ufficio SIC) **del Responsabile del Settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente**, ovvero sulla base delle funzioni attribuite secondo la struttura organizzativa dell'Ente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata

direttamente dalla Segreteria dell'Ente o dal Responsabile del Settore con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco delle risorse informatiche per le quali deve essere abilitato l'accesso.

Ogni successiva variazione delle abilitazioni di accesso ai sistemi informatici dovrà essere richiesta formalmente al Servizio "Sistema Informatico Comunale" dal Responsabile del Settore.

Alcuni principi generali:
a) Le credenziali di autenticazione verranno comunicate direttamente all'utente con sistemi che garantiscano la riservatezza.
b) Le credenziali di autenticazioni consistono in un **codice nominativo per l'identificazione dell'utente** (altresì nominato username, nome utente o user id, generalmente coerente con il modello *nome.cognome*), assegnato dal Servizio "Sistema Informatico Comunale", ed una relativa **password.** La password è personale e riservata, e dovrà essere conservata e custodita dall'incaricato con la massima diligenza, e non divulgata a terzi.
c) 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 famigliare).
d) È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni tre mesi. È fatta salva la possibilità che il cambio password sia reso obbligatorio e abbia scadenze diverse (più brevi) in base alle politiche di gestione dei singoli sistemi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili, è obbligatorio il cambio password almeno ogni tre mesi.
e) **Non sono ammesse password vuote**, per cui si invitano tutti gli utenti ad assicurarsi della presenza di una password di accesso, ovvero ad impostarla al più presto.
f) Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile del Settore sulla base delle funzioni attribuite, secondo la struttura organizzativa dell'Ente, dovrà comunicare formalmente e preventivamente al Servizio "Sistema Informatico Comunale", la data effettiva a partire dalla quale le credenziali saranno disabilitate.

Art.6 - Utilizzo della rete e delle risorse logiche

Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale od internet (es. per applicativi gestionali software o cloud), ciascun utente deve essere in possesso di credenziali di autenticazione.

Le credenziali sono strettamente personali. È proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre utenti.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server/NAS) nelle quali vanno inseriti e salvati i documenti informatici (files) di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Ciascun utente, poi, dispone di norma di un'area riservata e personale denominata con il proprio cognome o numero di interno. **Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali**. Pertanto **è vietato il salvataggio sulle condivisioni di rete dell'Ente, ovvero sugli Strumenti in generale, 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 dal personale del Servizio "Sistema Informatico Comunale", a seguito di interventi di analisi della sicurezza informatica ovvero di manutenzione/aggiornamento verrà rimosso secondo le regole previste nel capitolo "Controlli sugli Strumenti" del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte ad attività di controllo regolare e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali delle PdL, la cartella "Download" o "Desktop" dell'utente (presente nella postazione di lavoro dove normalmente opera), gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o chiavette USB ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse dell'Ente, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita o sottrazione di dati. Pertanto la responsabilità dei salvataggi dei dati in questi dispositivi è a carico del singolo utente.

- Senza il consenso del Titolare (vds informativa Privacy sul sito), è vietato trasferire documenti informatici dai Sistemi Informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
- Senza il consenso del Titolare (vds informativa Privacy sul sito), è vietato salvare documenti informatici dell'Ente su unità di memorizzazione esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, WeTransfer, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.
- Il consenso del Titolare si ritiene implicito se il salvataggio o trasferimento di documenti informatici dell'Ente viene effettuato attraverso gli Strumenti Informatici in dotazione (ad es.:procedure gestionali, posta elettronica) nell'ambito di un procedimento amministrativo, utilizzando i canali di comunicazione istituzionali.
- Senza il consenso del Titolare (vds informativa Privacy sul sito) non è permessa la connessione di dispositivi personali alla rete dell'Ente, sia essa cablata o wireless.

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi informatici in sua gestione, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante. L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno delle proprie strutture, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso a tecnici, fornitori od altri Enti che nell'ambito di un rapporto contrattuale o convenzione con il Comune di Porto San Giorgio necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune di Porto San Giorgio che necessitino di svolgere compiti specifici, pur non essendo presenti in sede.

All'interno delle sedi del Comune di Porto San Giorgio potranno essere rese disponibili delle reti senza fili (wireless), c.d. "Wi-Fi". Tali reti consentono l'accesso ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso a queste reti verrà concesso ad amministratori, dipendenti, consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di Porto San Giorgio necessitino di accedere a determinate risorse informatiche. Verrà concesso, altresì, a dipendenti e funzionari del Comune di Porto San Giorgio che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse.

La richiesta per l'accesso alla rete tramite VPN o tramite WIFI verrà fatta con le stesse modalità descritte al capitolo "Gestione, assegnazione e revoca delle credenziali di accesso".

Ogni utente che avrà accesso alla rete dell'Ente attraverso dispositivi personali avrà cura di garantire l'aggiornamento e la protezione degli stessi in termini di sicurezza. Il Servizio "Sistema Informatico Comunale" si riserva la facoltà di negare o interrompere l'accesso alla rete – anche senza preavviso - di dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

I locali od armadi tecnici adibiti alla gestione di apparati di rete e Sistemi Informatici sono accessibili soltanto al personale tecnico e di norma vengono mantenuti chiusi a chiave.

I log relativi all'accesso alla rete ed agli archivi elettronici condivisi, possono essere registrati attraverso sistemi automatici di monitoraggio, e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Servizio "Sistema Informatico Comunale" dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. I controlli possono avvenire secondo le disposizioni previste nel 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 679/16 "GDPR".

Art.7 - Utilizzo degli Strumenti (PDL ed altri strumenti con relativi software ed applicativi)

Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Porto San Giorgio e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione o che comunque utilizza. 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.

L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Codice Utente e password assegnate dal Servizio "Sistema Informatico Comunale" secondo le modalità indicate ai capitoli precedenti. A tal proposito si rammenta che queste credenziali sono strettamente personali e che l'utente è tenuto a conservarli nella massima diligenza e segretezza.

Il Personal Computer, notebook, tablet, e tutti gli accessori forniti (webcam, casse audio, cuffie, microfoni, adattatori, cavi, mouse, tastiere, etc) in generale qualsiasi Postazione di Lavoro (PdL), ed ogni altro hardware, deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale del Servizio Sistema Informatico Comunale ogni malfunzionamento e/o danneggiamento.

- Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, se non previa richiesta e intervento (o eventuale autorizzazione) da parte del personale del Servizio Sistema Informatico Comunale.

- 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 (PDL) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare una PdL incustodita connessa alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso, che verrà in ogni caso attribuito al detentore delle credenziali di accesso. Di norma le PdL vengono configurate con un blocco automatico dopo un certo tempo di inattività.

- Salvo casi eccezionali, da comunicare al Servizio Sistema Informatico Comunale, **è vietato lasciare accese le PdL al di fuori dell'orario di lavoro**.

- Le informazioni archiviate sulla PDL locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata ed in ogni caso, come esplicitato precedentemente, non sono soggette ad attività di backup periodico.

- Costituisce buona regola la pulizia periodica degli archivi memorizzati sulla propria PDL, con cancellazione dei file obsoleti o non più utili.

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

- Non è consentita l'installazione autonoma di programmi nelle PdL, ed in ogni caso di programmi diversi da quelli autorizzati dall'Ente e sprovvisti di adeguata licenza di utilizzo.

Tutte le richieste di risorse hardware e software dovranno essere inoltrate al Servizio "Sistema Informatico Comunale" per le opportune valutazioni tecniche. In particolar modo, questo vale anche per l'approvvigionamento di strumenti hardware o software complessi (portali web, gestionali etc): il SIC darà il proprio parere rispetto alla fornitura, e, qualora questa sia adeguata e compatibile tecnicamente con la infrastruttura informatica, sarà compito dell'Ufficio interessato (del Settore/Servizio richiedente) procedere con gli adempimenti amministrativi e finanziari.

Gli operatori del Servizio "Sistema Informatico Comunale" potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza delle PDL, 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 la PdL sempre protetta.

- È vietato utilizzare la PDL 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, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti dell'Ente, salvo che il

supporto utilizzato sia stato fornito ed autorizzato dall'Ente. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative e nell'ambito di un procedimento amministrativo.

- È vietato connettere alla PdL qualsiasi dispositivo o periferica personale (ad es. Smartphone) o comunque non autorizzata preventivamente dall'Ente.

- È vietato connettere alla rete locale qualsiasi dispositivo (notebook, tablet, dispositivi di rete, router, switch, modem, etc.) non autorizzato preventivamente dall'Ente.

- È vietato modificare il cablaggio delle postazioni (cavi di rete, usb, di alimentazione, etc).

Nel caso in cui l'utente dovesse notare comportamenti anomali della PdL, l'utente stesso è tenuto a comunicarlo tempestivamente al Servizio "*Sistema Informatico Comunale*".

I log relativi all'utilizzo di Strumenti ed applicativi, reperibili nella memoria degli Strumenti stessi, ovvero sui Server o sui dispositivi di rete dell'Ente, nonché i file con essi trattati possono essere registrati attraverso sistemi automatici di monitoraggio e possono essere oggetto di controllo da parte del Titolare del trattamento 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 nel 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 679/16 "GDPR".

Art.8 - Utilizzo di internet

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

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

a) È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito dai sistemi di filtraggio implementati dall'Ente con le sue policy di sicurezza, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente.

b) È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente (sovraccarico della rete, introduzione di virus informatici), 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.

c) **È vietato a chiunque il download di qualunque tipo di software gratuito** (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dal Servizio "*Sistema Informatico Comunale*".

d) 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 il Servizio "Sistema Informatico Comunale" per uno sblocco selettivo (ced@comune-psg.org).

e) Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera da filtri, è necessario richiedere lo sblocco mediante una mail indirizzata a ced@comune-psg.org, ed in copia al Responsabile di Settore, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, ed eventualmente intervallo di tempo richiesto per completare l'attività.

f) È vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dall'Ente o comunque nell'ambito di un procedimento amministrativo che preveda dei movimenti finanziari.

g) È vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet dalla propria postazione, utilizzando dispositivi personali.

h) 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'Ente. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed alle e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del presente regolamento.

i) 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, così come effettuare download o aggiornamenti massivi, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei Sistemi Informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, l'Ente registra per 7 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 secondo le disposizioni e le forme previste nel 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 679/16 "GDPR".

Art.9 - Utilizzo della posta elettronica

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

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

Ad ogni utente viene fornito un account e-mail nominativo nel dominio dell'Ente, generalmente coerente con il modello *nome.cognome@comune_psg.org*; 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 e di conservare e modificare frequentemente la password secondo le medesime indicazioni fornite per la gestione dell'account di accesso alle PdL.

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 o operatività dell'Ente.

Si ricorda altresì che tutta la corrispondenza con cittadini, imprese ed altra amministrazione relativa a procedimenti amministrativi è opportuno transiti attraverso il protocollo dell'Ente e venga gestita con i canali telematici ufficiali (Sportello telematico polifunzionale).

- L'iscrizione a mailing-list o newsletter esterne con il proprio indirizzo dell'Ente 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, con i quali non sussiste alcun rapporto lavorativo o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.xlse, *.xlsx e *.pif e altri in aggiornamento in base alle necessità.

- È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing, frodi informatiche, o installazione involontaria di software malevolo. In qualunque situazione di incertezza, prima di eseguire qualsiasi azione, contattare il Servizio "Sistema Informatico Comunale" 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 vietata la diffusione di messaggi pubblicitari di prodotti di qualsiasi tipo.

- Nel caso fosse necessario inviare allegati "pesanti" (oltre i 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 al personale del Servizio "Sistema Informatico Comunale" per la valutazione delle soluzioni.

- Non è consentito l'invio automatico di e-mail all'indirizzo email 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 preferibile utilizzare l'inoltro automatico ad

altre caselle dell'Ente e/o un messaggio di autoreply "Fuori Ufficio/Out of Office", facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo.

- 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 Responsabile di Settore quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

- Sarà compito dello stesso assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile. Si ricorda comunque della possibilità di accesso alla propria casella di posta elettronica da qualsiasi dispositivo connesso ad internet e dotato di browser.

- La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, e su autorizzazione del responsabile di Settore 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. Si ricorda che vi sono comunque dei limiti all'invio massivo di messaggi dalla casella di posta e che è possibile utilizzare il servizio di invio newsletter, più idoneo a gestire comunicazioni/avvisi/inviti ad una pluralità di soggetti.

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

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. In ogni caso, va preferito il salvataggio dei dati sulle condivisioni dell'Ente.

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

Si ricorda che non vengono effettuati backup periodici della posta elettronica personale, pertanto è compito del singolo utente, se lo ritenesse necessario, gestire in autonomia queste attività.

In casi particolari e su esplicita richiesta al Sistema Informatico Comunale, possono essere configurati ed utilizzati dispositivi personali (es. smartphone/tablet) per la gestione della posta elettronica.

Si informa che le comunicazioni, anche elettroniche, ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente. Si informa altresì che l'Ente 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 del Servizio "Sistema Informatico Comunale" può, secondo le procedure indicate nel presente Regolamento, accedere all'account di posta elettronica del dipendente dell'Ente, prendendo visione dei messaggi, salvando o cancellando file e modificandone la configurazione (ad esempio per impostare il messaggio di "Fuori Ufficio").
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 "GDPR".

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

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono in dotazione, sono di proprietà del Comune di Porto San Giorgio 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 all'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 all'utente un cellulare dell'Ente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente si applicano le medesime regole 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, la gestione della posta elettronica e la connessione di dispositivi non autorizzati.

- Per gli Smartphone e Tablet dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate.

- È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali.

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

o Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative,
o Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili),
o Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.

- Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera, prima di lasciare gli uffici o in caso di inutilizzo prolungato.

- Nel caso in cui si renda necessaria la stampa di informazioni riservate o dati sensibili l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

- Le stampanti multifunzione con possibilità di scannerizzazione salvano i documenti in una condivisione di rete accessibile agli utenti; si raccomanda di spostare i documenti immediatamente dopo l'attività di scansione, soprattutto se trattasi di documenti contenenti dati sensibili o giudiziari. Trattandosi di aree di memorizzazione temporanee un automatismo provvederà ad una cancellazione periodica di tali file.

Art.11 - Assistenza agli utenti e manutenzioni

Il Servizio "Sistema Informatico Comunale" e le Aziende incaricate di effettuare attività di manutenzione sul software e sui Sistemi in generale, possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:
- verifica e risoluzione di problemi sistemistici ed applicative, su segnalazione dell'utente finale.
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- richieste di 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, i soggetti sopra indicati sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'accesso in teleassistenza sulle PdL della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Ente e soggetto alle verifiche, da parte del Servizio "Sistema Informatico Comunale", 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 o suo delegato deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento, ed assicurarsi della corretta disconnessione al termine dell'intervento.

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

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 del presente Regolamento e l'integrità del proprio Sistema Informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art.4, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la

raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

I controlli devono essere effettuati nel rispetto del presente Regolamento e dei seguenti principi:

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

L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come spiegato nei riquadri di cui ai punti precedenti del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite del Servizio Sistemi informativi ed Innovazione Tecnologica, 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, oppure per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.).

Gli interventi di controllo sono di tre tipi, come di seguito specificato, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti messi a disposizione degli utenti: controlli per la tutela del patrimonio dell'Ente, 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, ecc.).

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

I. 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.
II. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti precedenti, con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
III. 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 precedenti, il Titolare del Trattamento, unitamente all'Ufficio Sistemi Informativi ed Innovazione Tecnologica, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

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 descritte ai punti precedenti il Titolare del trattamento dei dati personali, per il tramite del Servizio "Sistema Informatico Comunale", si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).
i. Redazione di un atto/comunicazione da parte del Titolare del trattamento che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
ii. Incarico al Servizio "Sistema Informatico Comunale" 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.
iii. Redazione di un verbale che riassuma i passaggi precedenti.
iv. In ogni caso l'accesso ai documenti/informazioni presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

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 Titolare del trattamento e dal tecnico incaricato 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). 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 679/16 "GDPR".

Art.13 - Violazione Privacy e Data Breach

Premesso che l'art. 32 del Reg. 679/16 affidi al Titolare del trattamento ed al Responsabile esterno del trattamento il compito di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei dati personali adeguato al rischio, ed al Responsabile per la Transizione al digitale la responsabilità sull'attuazione delle Misure minime di sicurezza, **eventuali violazioni dei dati personali rilevate da qualsiasi dipendente dell'Ente o collaboratore esterno, nonché dai responsabili esterni, vanno immediatamente segnalate**, in riferimento all'art.33 del Reg. 679/16, **al Titolare del trattamento**, al quale spetta il compito di valutare l'impatto e la gravità della violazione ed eventualmente avviare una procedura di notifica all'autorità di controllo.

Fatte salve le raccomandazioni contenute in questo regolamento relative alla protezione dei dati personali, all'utilizzo dei Sistemi e degli strumenti messi a disposizione degli utenti, si riporta un elenco, esemplificativo e non esaustivo, delle possibili violazioni:
1. Accesso alla propria postazione di lavoro da parte di persone non autorizzate;
2. Accesso alla propria casella di posta elettronica da parte di persone non autorizzate;
3. Accesso alla rete dati dell'Ente da parte di terzi con dispositivi non autorizzati;
4. Perdita o sottrazione di dispositivi di memorizzazione esterni contenenti dati personali;

5. Installazione di software malevolo o comunque non autorizzato che possa compromettere la sicurezza e l'integrità degli Strumenti;

Art.14 - Conservazione dei dati

In riferimento agli articoli 5 e 6 del Reg. 679/16, ed in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico (es. log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro i termini previsti dalla normativa, salvo esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In caso di cessazione del rapporto lavorativo, incarico politico e/o istituzionale, le cartelle personali presenti nelle condivisioni di rete, la casella di posta elettronica, i dati presenti nella PdL del soggetto verranno resi inaccessibili, conservati al massimo per un periodo di **6 mesi** e successivamente eliminati.
Ogni ufficio o servizio può disporre di una o più caselle email non nominative (ad es. tributi@comune-psg.org). Al fine di garantire l'operatività e la continuità del servizio, per queste caselle non è prevista la cancellazione dei dati in caso di avvicendamento del personale dell'Ufficio.

Nell'ambito della normale operatività, gli amministratori dei sistemi possono disporre o operare autonomamente la cancellazione di contenuti presenti nella PDL non conformi al presente regolamento.

Art.15 - Partecipazione a Social Media

L'utilizzo, a fini promozionali, 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.

Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri cittadini e fornitori, gli altri enti, 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 e con gli Strumenti messi a disposizione dall'Ente.

Le presenti disposizioni devono essere osservate dall'utente sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente, se non espressamente autorizzato. 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.16 - Sanzioni disciplinari

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

In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

L'Ente di riserva, in caso di inosservanza rilevata in seguito ai relativi controlli e verifiche, di procedere con i relativi provvedimenti in relazione alla gravità del danno. La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt.2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art.7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).