REGOLAMENTO
PER L'UTILIZZO DEI
SISTEMI INFORMATICI
DEL COMUNE DI GRAVINA DI CATANIA

REGOLAMENTO
PER L'UTILIZZO DEI SISTEMI INFORMATICI
DEL COMUNE DI GRAVINA DI CATANIA

Indice

PREMESSA

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

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Gravina di Catania.

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

Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 2016/679 sulla protezione dei dati personali.

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

1. Oggetto e finalità

Il presente 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 n. 2016/679 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 della Privacy**);
- 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";

- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità dell'Ente e 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.

2. Principi generali e di riservatezza nelle comunicazioni

2.1. Il presente Regolamento, in materia di protezione dei dati personali, rinvia interamente alle disposizioni di cui al GDPR e, precisamente:

a) il principio di necessità, secondo cui i sistemi informatici e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);
b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2. Il dipendente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, o altri dati, elementi e informazioni dell'Ente dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere

comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.

b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office.

3. Tutela del lavoratore

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

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

4. Campo di applicazione

4.1. Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.

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

5. Gestione, assegnazione e revoca delle credenziali di accesso

5.1. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal personale del Servizio Sistemi Informativi, previa formale richiesta del Responsabile del Servizio nel quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile di Servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei servizi informatici per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente al Servizio Sistemi Informativi dal Responsabile di riferimento.

5.2. Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dal Servizio Sistemi Informativi, ed una

relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e non divulgata.

5.3. La password deve essere di adeguata robustezza, conforme ai criteri di complessità stabiliti e comunicati dal Servizio Sistemi Informativi. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare).

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

5.5. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente al Servizio Sistemi Informativi la data effettiva a partire dalla quale le credenziali saranno disabilitate.

6. Utilizzo della rete del Comune di Gravina di Catania

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

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

6.3. L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto, è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema o dal Servizio Sistemi Informativi a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 15 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse dell'Ente, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

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

6.5. Senza il consenso del Servizio Sistemi Informativi è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

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

6.7. Il Comune di Gravina di Catania mette a disposizione dei propri dipendenti che necessitino di svolgere compiti specifici, pur non essendo presenti in sede, 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. Le richieste di abilitazione all'accesso mediante VPN dovranno essere autorizzate dal Segretario Generale previo accordo individuale con il lavoratore che preveda durata, modalità e obiettivi.

I consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di Gravina di Catania necessitino di accedere a determinate risorse informatiche dovranno essere autorizzati dal Servizio Sistemi Informativi.

6.8. 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 Sistemi Informativi si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

6.9 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, nonché i file salvati o trattati su Server o unità di rete condivise (es. NAS), saranno registrati e potranno essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. I controlli possono avvenire secondo le disposizioni previste al successivo punto 15 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 679/16 "General Data Protection"

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

7.1. Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Gravina di Catania 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.

7.2. L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dal Servizio Sistemi Informativi (punto n. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

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

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

7.5. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

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

7.7. Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.

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

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

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

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

7.12. 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 dal Servizio Sistemi Informativi. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

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

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

7.15. Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente al Servizio Sistemi Informativi.

7.16. Al fine di evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità degli applicativi, non è consentito installare programmi provenienti dall'esterno. In caso di introduzione di virus, trojan o programmi che possono rappresentare un rischio per la sicurezza del computer e/o di qualsiasi altro dispositivo in uso si deve contattare l'Ufficio Sistemi Informativi, astenendosi dal risolvere il problema per conto proprio.

Si rammenta inoltre quanto segue:

a) Non è consentito l'uso di programmi non autorizzati dall'Ufficio Sistemi Informativi;
b) Non è consentito scaricare alcun software se non con l'autorizzazione dell'Ufficio Sistemi Informativi;
c) Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
d) Non è consentito modificare le configurazioni impostate sul proprio PC rispetto a quelle autorizzate e predisposte;
e) Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come, ad esempio, modem Wi-Fi e memorie esterne);
f) Non sono consentiti la visualizzazione e il salvataggio di testi, immagini o registrazioni a carattere razzista, pornografico, pedopornografico, sessuale, violento, osceno o di natura simile, indipendentemente da quale ne sia la fonte e/o comunque di qualsiasi materiale che sia vietato dalle norme penali.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

I controlli possono avvenire secondo le disposizioni previste al successivo punto 15 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 679/16 "General Data Protection Regulation".

8. Utilizzo di supporti magnetici e/o ottici

8.1 I dati devono essere salvati sulle cartelle presenti sul server.

L'utilizzo di supporti magnetici (es. hard-disk esterni, chiavette usb) e/o ottico (es. DVD, CD) non è consentito.

Solo in casi eccezionali e su autorizzazione del Servizio Sistemi Informativi deve avvenire secondo le seguenti modalità:

a) il supporto non potrà fuoriuscire dai locali comunali e dovrà essere custodito in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato, alterato e/o distrutto;

9. 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.

9.1. 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, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente.

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

9.3. 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.

9.4. 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 Sistemi Informativi per uno sblocco selettivo.

9.5. 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 mail indirizzata al Servizio Sistemi Informativi, 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 il

punto 15 del presente Regolamento. Al termine dell'attività gli addetti del Servizio Sistemi Informativi ripristineranno i filtri nella situazione iniziale.

9.6. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dal Servizio Sistemi Informativi, con il rispetto delle normali procedure di acquisto.

9.7. 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 e della Direzione Generale previo parere tecnico degli stessi Amministratori.

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

9.9. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dal Servizio Sistemi Informativi. 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. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni del punto n.15 del presente Regolamento.

9.10. 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.

Si informa che l'Ente, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informatici, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, l'Ente registra per un massimo di 365 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 potrà trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate al successivo punto 15 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 679/16 "General Data Protection Regulation".

10. Obblighi di pubblicazione

10.1 Tutti dipendenti autorizzati a pubblicare sul sito istituzionale, amministrazione trasparente, albo pretorio, notizie, informazioni ed atti amministrativi, sono tenuti al rispetto delle disposizioni di legge in materia ed in particolare al rispetto dei tempi di pubblicazione, di protezione dei dati personali ed altresì a rendere i documenti accessibili.

10.2 Non è ammessa, la pubblicazione di documenti-immagine (scansioni digitali di documenti cartacei) senza che si sia provveduto a opportuna digitalizzazione del testo ivi contenuto. Per ottemperare alla normativa è necessario, pubblicare sui siti web solo documenti derivanti da Word/Excel/OpenOffice, grazie al semplice salvataggio del file in formato .pdf (funzionalità disponibile all'interno dei programmi stessi) e dove richiesto firmati digitalmente.
Sull' Accessibilità dei documenti si richiama:

- la legge 4/2004 "**Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici"** che pone l'obbligo per le pubbliche amministrazioni di garantire *"il diritto di accesso ai servizi informatici e telematici della pubblica amministrazione e ai servizi di pubblica utilità da parte delle persone disabili";*

- **Il Decreto Ministeriale 20 marzo 2014** che recita: "*Il formato digitale dei documenti pubblicati necessari a fornire informazioni o a erogare servizi deve essere utilizzabile con tecnologie compatibili con l'accessibilità. Il contenuto dei documenti deve essere conforme ai requisiti tecnici di accessibilità. Se un documento non risponde a queste caratteristiche, per sua natura o perché è disponibile solo in formato non compatibile con l'accessibilità, allora deve essere soddisfatto almeno uno dei seguenti punti:*

  a) *il formato ed i contenuti dei documenti devono essere resi disponibili nella loro completezza anche in modalità adatta ad essere fruita mediante le tecnologie compatibili con l'accessibilità ed essere conformi ai requisiti tecnici di accessibilità;*
  b) *per i documenti resi disponibili in formato digitale non utilizzabile con tecnologie compatibili con l'accessibilità, oppure che abbiano contenuti non conformi ai requisiti tecnici di accessibilità, devono essere forniti sommario e descrizione degli scopi dei documenti stessi in forma adatta ad essere fruita con le tecnologie compatibili con l'accessibilità e devono essere indicate in modo chiaro le modalità di accesso alle informazioni equivalenti a quelle presentate nei documenti digitali non accessibili.*

11. 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.

11.1. Ad ogni utente viene fornito un account e-mail dell'Ente nominativo, generalmente coerente con il modello *inzialenome_cognome@comune.gravina-di-catania.ct.it* (ad esempio *m_rossi@comune.gravina-di-catania.ct.it*); l'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi dell'Ente, 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.

11.2. L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente.

11.3. 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.

11.4. Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare gli Amministratori di Sistema o il Servizio Sistemi Informativi per una valutazione dei singoli casi.

11.5. 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.

11.6. Nel caso fosse necessario inviare allegati "pesanti" (fino al 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 al Servizio Sistemi Informativi.

11.7. 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 o Enti – qualificati e competenti.

11.8. 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 "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo

ufficio@comune.gravina-di-catania.ct.it. Rivolgersi al Servizio Sistemi Informativi per tale eventualità.

11.9. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;

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

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

11.12 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.

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

11.14 Non vengono effettuati backup periodici della posta elettronica personale, pertanto è compito del singolo utente, se lo ritenesse necessario, gestire in autonomia queste attività. La posta elettronica può essere gestita sia dalla postazione di lavoro in dotazione che da qualsiasi dispositivo connesso ad internet, utilizzando il portale raggiungibile all'indirizzo https://intranet.comune.gravina-di-catania.ct.it:7000 e le credenziali personali della casella.

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

Si informa altresì che l'Ente, per il tramite del Servizio Sistemi Informativi, 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 Sistemi Informativi può, secondo le procedure indicate successivo punto 15 del presente Regolamento, accedere all'account di posta elettronica dell'Ente, prendendo visione dei messaggi, salvando o cancellando file.

Si informa che, in caso di cessazione del rapporto lavorativo, la mail dell'Ente affidata all'incaricato verrà sospesa per un periodo di 6 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Il sistema in ogni caso genererà una risposta automatica al mittente.

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 costituiscono adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

12. Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

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

12.2. 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.

12.3. Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. punto n. 7 "Utilizzo degli Strumenti elettronici"), 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.

12.4. 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 dal Servizio Sistemi Informativi.

12.5. È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.

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

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

12.7. Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli ufficio in caso di inutilizzo prolungato.

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

13. Cessazione del rapporto di lavoro

13.1 Quando un dipendente cessa il rapporto di collaborazione (sia esso dipendente, collaboratore a progetto o stagista), l'incaricato è obbligato a consegnare all'Ufficio di appartenenza gli strumenti aziendali e i dispositivi messi a disposizione, inclusi i supporti di memoria esterni.

13.2 L'Ufficio Sistemi Informativi, su segnalazione dell'Ufficio del Personale, provvederà a disattivare l'accesso ai corrispondenti archivi presenti sul server, alla casella di posta elettronica, e a tutti gli applicativi e servizi web messi a disposizione dall'Ente. Per consentire la continuità operativa, sulla casella di posta dell'incaricato dimissionario sarà impostato un messaggio automatico che avvisa della disattivazione della casella e-mail. Ricordando che la posta elettronica e tutti gli strumenti sono di proprietà dell'Ente, si ritiene necessario ricordare che a cessazione del rapporto di lavoro è obbligatorio restituire integri e completi tutti gli strumenti che il Comune ha messo a disposizione, in particolare:

a) la casella di posta elettronica ed i messaggi e documenti in essa contenuti devono essere messi a disposizione dell'Ente per consentire la continuità operativa;
b) eventuali messaggi privati o non pertinenti l'attività operativa devono essere eliminati;
c) PC portatili e smartphone devono essere tempestivamente consegnati, senza che il collaboratore ne effettui backup o copie per uso personale;
d) eventuali schede sim devono essere restituite.
e) entro 15 giorni dal termine della collaborazione tutto l'hardware sarà formattato in modo da essere illeggibile e non più recuperabile, secondo gli standard internazionali più recenti.

14. Assistenza agli utenti e manutenzioni

14.1. Il Servizio Sistemi Informativi 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 aggiornamento software e manutenzione preventiva hardware e software.

14.2 Al fine di una gestione più efficiente e tempestiva, tutte le richieste di intervento da parte dei dipendenti devono avvenire tramite l'apertura di un ticket di assistenza da inoltrare tramite e-mail interna dell'Ente esclusivamente al seguente indirizzo *supporto@gravinanet.it*. Il personale del Ced prenderà in carico il ticket nel più breve tempo possibile. Le richieste di supporto inoltrate tramite ticket avranno la priorità rispetto a quelle fatte tramite altri canali.

14.3. 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.

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

14.5. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o gli Amministratori di Sistema devono 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.

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

15.1. Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, 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 dei punti n. 2, 3 e n. 4 del presente Regolamento e dei seguenti principi:

a) 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.

b) Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
c) 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 analiticamente spiegato ai punti 6 – 7 – 8 – 9 – 11 – 12 del presente Regolamento.

Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente , per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti ai punti 15.2 e 15.3) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

15.2. *Controlli per la tutela del patrimonio dell'Ente, per la sicurezza e la salvaguardia del sistema informatico, nonché 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 6 – 7 – 8 – 9 – 11 – 12 il Responsabile 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).

a) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
b) 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 6 – 7 – 8 – 9 – 11 – 12 con possibilità di rilevare file trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
c) Qualora il rischio di compromissione del sistema 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 del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

15.3. *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 file 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 6 – 7 – 8 – 9 – 11 – 12 il Responsabile del trattamento dei dati personali, per il tramite del Servizio Sistemi Informativi, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

a) Redazione di un atto da parte del Responsabile di Servizio che comprovi le necessità organizzative che richiedano l'accesso allo Strumento.
b) Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
c) Redazione di un verbale che riassuma i passaggi precedenti.
d) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
e) Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

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 Trattamento 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). 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 "General Data Protection".

16. 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:

- Accesso alla propria postazione di lavoro da parte di persone non autorizzate
- Accesso alla propria casella di posta elettronica da parte di persone non autorizzate
- Accesso alla rete dati dell'Ente da parte di terzi con dispositivi non autorizzati
- Perdita o sottrazione di dispositivi di memorizzazione esterni contenenti dati personali
- Installazione di software malevolo o comunque non autorizzato che possa compromettere la sicurezza e l'integrità degli Strumenti

17. Conservazione dei dati

17.1. In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy e/o firewall), la cui conservazione non sia necessaria, saranno cancellati entro i termini indicati nel presente Regolamento, 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.

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

18. Partecipazioni a Social Media

18.1. 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.

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

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

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

19. Sanzioni disciplinari

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

20. Deroghe e modifiche al presente Regolamento

Il presente documento è pubblicato sul sito web istituzionale, adeguatamente diffuso a tutto il personale dell'Ente e ai collaboratori esterni e regolarmente aggiornato. L'ufficio competente provvederà a notificare a collaboratori e dipendenti la presenza di una eventuale versione aggiornata. Il presente documento viene regolarmente revisionato e approvato dall'Ente. Deroghe o modifiche di uno o più punti del presente Regolamento, non rendono invalidi gli altri punti.