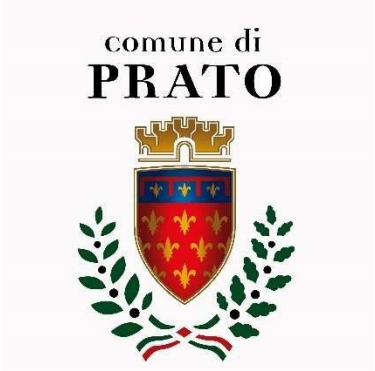

REGOLAMENTO SULL'UTILIZZO DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE DEL COMUNE DI PRATO

Approvato con DGC 125 del 15.06.2021

Modificato con DGC 207 del 14.06.2022

Sommario

Titolo I - PREMESSE

Art. 1. Definizioni

1. Nell'ambito del presente Regolamento si applicano le seguenti definizioni:

a) "*Amministrazione*" – L'*Amministrazione* Comunale di Prato.
b) "*Dotazioni*" – Si intendono i sistemi hardware, i sistemi software ed i servizi meglio specificati al successivo Art. 4.
c) "*Utenti*" – I soggetti di cui all'art. 4 comma 2.
d) "*Responsabili di struttura*" – I dirigenti del servizio di riferimento.
e) "Sistema Informativo" Il servizio dell' "*Amministrazione*" che ha la responsabilità della realizzazione e gestione delle infrastrutture informatiche, telematiche e telefoniche.
f) "Servizio *Accessi"* – Addetti alle gestione delle abilitazioni *Utenti* presso il servizio "Sistema Informativo" dell'*Amministrazione.*
g) "GDPR" - Regolamento UE 2016/679

Art. 2. Scopo del Regolamento

2. L'*Amministrazione* definisce, anche per il tramite del presente Regolamento, le modalità di utilizzo, da parte degli *Utenti*, ed il controllo, da parte degli addetti al sistema informatico dell*'Amministrazione*, delle *Dotazioni* informatiche messe a disposizione degli *Utenti*. Ciò allo scopo di:

    a. garantire il corretto utilizzo delle stesse;

    b. garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

    c. garantire la continuità dei servizi dell'*Amministrazione*;

    d. evitare che gli *Utenti* possano esporre sé stessi e/o l'*Amministrazione* a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito delle *Dotazioni*, nonché esporre l'*Amministrazione* a conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine.

3. Il presente Regolamento costituisce altresì un insieme di misure di sicurezza ai fini dell'art. 32 del GDPR[1].

4. Non rientra tra gli scopi del presente Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non

[1] Art. 32 comma 1 GDPR: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio….."

consentiti. Pertanto, nel rispetto delle previsioni di cui agli artt. 4[2] e 8[3] della Legge 20 maggio 1970, n. 300 (di seguito anche solo "Statuto dei Lavoratori"), l'*Amministrazione* intende anche disciplinare, con il presente Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite le *Dotazioni*, informando circa l'esercizio dell'eventuale potere disciplinare dell'*Amministrazione* nei confronti dei dipendenti, qualora si verificasse ed accertasse - secondo le procedure di cui al presente Regolamento - un uso improprio e/o non autorizzato delle *Dotazioni*.

5. Il presente Regolamento e le previsioni ed indicazioni in esso contenute sono richiamate anche all'interno dei seguenti atti:

   a) Art. 57 CCNL – "Obblighi del dipendente" comma 3 punti g) h) j) e k);
   b) Codice di comportamento dei dipendenti dell'*Amministrazione*[4];
   c) Nota informativa resa ai neo-assunti;
   d) Nomine degli Autorizzati ai vari trattamenti.

Art. 3. Riferimenti Normativi

1. Il presente Regolamento si ispira ed attua le seguenti norme:

   a) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("GDPR");

   b) Decreto legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016";

   c) Opinion 2/2017 del cd. "Article 29 Data Protection Working Party" dell'8 Giugno 2017, "on data processing at work";

   d) Provvedimento del Garante del 1° marzo 2007, "Lavoro: le linee guida del Garante per posta elettronica e Internet", pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

   e) Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato in Gazzetta Ufficiale n. 300 del 24 dicembre 2008;

---

[2] L. 300/1970 – art. 4 :
"1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ……."

[3] L. 300/1970 – Art. 8 :
"E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore."

[4] Al momento quello vigente è stato approvato con DGC n. 12/2014 - si vedano di esso gli art. 11 comma 4, art. 12 comma 6, art. 15 comma 1 ed art. 16

f) Legge 20 maggio 1970, n. 300 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale, nei luoghi di lavoro e norme sul collocamento” ("Statuto dei Lavoratori");

g) Legge 22 aprile 1941 n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (di seguito anche solo "Legge sul Diritto d'Autore");

h) Decreto Legislativo 10 febbraio 2005, n. 30 (di seguito anche solo "Codice della proprietà industriale");

i) I vigenti Contratto Collettivo Nazionale di Lavoro e Contratto Collettivo Decentrato Integrativo.

Art. 4. Ambito di applicazione

1. Sono oggetto del presente Regolamento i seguenti elementi sintetizzati con il termine “*Dotazioni*”:

   a) i sistemi hardware di elaborazione personali (quali PC, tablet, etc.) messi a disposizione del dell’*Amministrazione* per lo svolgimento del lavoro d’ufficio;
   b) I sistemi hardware ad uso condiviso fra più utenti (es. Stampanti dipartimentali, fax, ecc.)
   c) i Software di base ed applicativi installati sui componenti hardware di cui al punto a), sui server presso la sala macchine dell’*Amministrazione* nonché i servizi in cloud messi a disposizione degli *Utenti*;
   d) i servizi di rete utilizzabili per lo svolgimento del lavoro di ufficio e l’accesso ai dati e documenti immagazzinati sui sistemi informatici, locali o remoti, dell’*Amministrazione*;
   e) il servizio di accesso alla rete mondiale Internet;
   f) i dispositivi e le utenze telefoniche fornite dall’*Amministrazione* per lo svolgimento del lavoro d’ufficio.

2. Il Regolamento si applica ai seguenti soggetti di seguito complessivamente denominati “U*tenti*”:

   a) tutti coloro ai quali l’*Amministrazione* fornisce una “matricola” personale, ovvero:

      a.a) tutti i dipendenti, indipendentemente dalla modalità di svolgimento dell’attività lavorativa (solo a titolo d’esempio: telelavoro, smart working, ecc.),

      a.b) i titolari di cariche politiche;

   b) tutti coloro che svolgono attività per l’*Amministrazione*, quali:

      b.a) collaboratori e prestatori di lavoro autonomo a prescindere dal rapporto intrattenuto con l’*Amministrazione*;

      b.b) in generale, a chiunque sia, in qualunque modo ed a qualunque titolo, autorizzato all’utilizzo delle *Dotazioni* dell’*Amministrazione* nello svolgimento delle proprie funzioni istituzionali.

3. Rimane ferma, in ogni caso, l’inapplicabilità, agli *Utenti* che non rientrano nella categoria dei dipendenti di cui al precedente punto a.a), di ogni riferimento relativo ai profili disciplinari e, più in generale, di ogni ulteriore previsione e/o normativa richiamata nel Regolamento che presupponga lo svolgimento di attività in regime di subordinazione.

Titolo II - ASSEGNAZIONE DELLE DOTAZIONI

Art. 5. Consegna delle Dotazioni

1. L’*Amministrazione*, ove necessario, mette a disposizione degli *Utenti* delle *Dotazioni* di tipologia e capacità correlate all’attività da svolgere.

2. Le assegnazioni delle *Dotazioni* e l'accesso al Sistema informatico dell'*Amministrazione* sono effettuate nei confronti degli *Utenti* sulla base delle esigenze generali espresse dall'*Amministrazione* o da esigenze specifiche espresse dai *Responsabili di struttura*.

3. All'inizio del rapporto di lavoro o di collaborazione, su richiesta del *Responsabile di struttura* presso la quale l'*Utente* deve svolgere la propria attività, ed in funzione delle specifiche esigenze di servizio che devono essere espletate, a cura del *Servizio Accessi*, si procederà a:

    a. Creare il nuovo utente all'interno dei sistemi di autenticazione interessati;

    b. Consegnare all'*Utente* le credenziali di accesso ai sistemi interessati;

    c. Impostare i diritti di accesso alle varie risorse informatiche di rete;

    d. Ad impostare i profili autorizzatori richiesti, dal *Responsabile di struttura* all'interno della varie procedure informatiche interessate;

    e. A creare, ove necessario, le credenziali per l'utilizzo del sistema di accesso da remoto (VPN).

    Diritti di accesso e/o profili di autorizzazione potranno variare al cambio di mansione o ufficio come meglio descritto all'Art. 21.

4. Sempre su richiesta del *Responsabile di struttura* presso la quale l'*Utente* deve svolgere la propria attività, ed in funzione delle specifiche esigenze di servizio che devono essere espletate, ove la richiesta sia giustificata e compatibilmente con le disponibilità di magazzino, a cura degli addetti alla gestione della manutenzione delle postazioni di lavoro dell'*Amministrazione* si procederà a:

    a. Installare, se non già presente e se necessaria, una postazione di lavoro presso l'ufficio sede dell'attività;

    b. A consegnare all'*Utente* un eventuale computer portatile per il lavoro a distanza;

    c. A configurare come necessario, e secondo le direttive del servizio sistema Informativo a garanzia della sicurezza ed integrità del sistema informatico, le apparecchiature consegnate per il loro proficuo utilizzo da parte dell'*Utente*.

    d. A configurare, ove necessario, sulla strumentazione mobile, il sistema di accesso da remoto (VPN) con le quantità di sicurezza di cui al punto 3 e) precedente.

5. Tenuto conto, infine, delle richieste del *Responsabile di struttura* presso la quale l'*Utente* deve svolgere la propria attività, delle specifiche esigenze di servizio da espletate e delle disponibilità di magazzino, a cura degli addetti alla gestione del sistema telefonico dell'*Amministrazione* si procederà a:

    a. Installare, ove non presente, e configurare apparecchiature telefoniche fisse;

    b. A consegnare all'*Utente* eventuali telefoni mobili e/o tablet con relativa utenza.

Art. 6. Caratteristiche della postazione di lavoro

1. Di norma a ciascun *Utente* viene assegnata una sola postazione fissa, mentre il computer portatile è assegnato solo ad *Utenti* autorizzati a prestazioni in modalità a distanza, secondo la regolamentazione dell'*Amministrazione*. Richieste di ulteriori assegnazioni, in quanto deroganti al suddetto principio, devono essere motivate a cura del *Responsabile di struttura* presso la quale l'*Utente* deve svolgere la propria attività e saranno gestire sulla base delle disponibilità e tenuto conto di priorità e valutazione di effettiva necessità accertate a cura servizio Sistema Informativo.

2. La riassegnazione di una stazione di lavoro non più utilizzata a diverso soggetto nell'ambito della stessa struttura può avvenire anche a cura dello stesso *Responsabile di struttura.* Quest'ultimo è comunque tenuto a comunicare agli addetti alla gestione della manutenzione delle postazioni di lavoro tale riassegnazione ai fini della rettifica dell'inventario informatico e di eventuali interventi di configurazione e messa a punto necessari.

3. Le apparecchiature inventariate presenti nei vari uffici e non assegnate ad alcun *Utente* saranno poste, a livello di inventario, a carico del *Responsabile di struttura* a cui appartiene l'ufficio in cui si trovano.

4. L'utilizzo di una stessa postazione da parte di più *Utenti* è consentito solo tramite profilazione degli *Utenti* e lo stretto utilizzo, da parte di ciascun *Utente*, delle proprie credenziali di sicurezza personali; l'assegnazione di una postazione ad un utente non implica quindi l'esclusività di utilizzo della stessa, sulla base delle disposizione organizzative del *Responsabile di struttura* di appartenenza. Tale tipologia di stazioni è attribuita, a livello di inventario, al *Responsabile di struttura*.

5. Gli *Utenti* che svolgono funzioni che non richiedono un'assegnazione puntuale della postazione (ad esempio: agenti di Polizia Municipale, docenti Nidi e Materne, ispettori, ecc.) utilizzano postazioni in condivisione con altri *Utenti* sulla base dell'organizzazione definita dalle rispettive strutture di appartenenza; anche tali postazioni sono formalmente assegnate, a livello di inventario, al responsabile della struttura.

6. Presso alcune sedi lavorative possono essere realizzati spazi di co-working, attrezzati con postazioni di lavoro utilizzabili da qualsiasi utente per favorire il lavoro in mobilità. Tali postazioni sono formalmente assegnate al *Responsabile di struttura* press cui si trova lo spazio di co-working.

7. In caso di trasferimento dell'*Utente* ad altro ufficio o ad altra sede dell'*Amministrazione*, di assenza o di trasferimenti temporanei di lunga durata ad altri enti, le apparecchiature della postazione fissa, che non siamo immediatamente attribuite a nuovi *Utenti* della stessa struttura, sono immediatamente disinstallate a cura degli addetti alla gestione della manutenzione delle postazioni di lavoro per poter essere riutilizzate. I *Responsabili di struttura* sono tenuti a notificare tempestivamente tale evenienza agli addetti alla manutenzione.

8. Nel caso di dotazione di computer portatile, a norma del precedente comma 1, l'*Amministrazione* potrà richiedere, ai fini dell'ottimizzazione delle risorse informatiche impiegate, che contemporaneamente venga revocata, allo stesso utente, l'assegnazione della postazione fissa, chiedendo al dipendente di utilizzare il computer portatile anche in ufficio. In tale evenienza l'*Amministrazione* si riserva anche di valutare l'installazione, nella postazione d'ufficio, di periferiche aggiuntive al computer portatile al fine di facilitare il lavoro dell'utente.

Art. 7. Uso di computer di proprietà dell'Utente (BYOD)

1. Ai fini dello svolgimento di attività lavorativa a distanza, o per consentire a personale non dipendente che ha rapporti di collaborazione con l'*Amministrazione*, è consentito l'utilizzo di dispositivi personali connessi alla rete telematica dell'*Amministrazione*, sia direttamente presso gli uffici che mediante utilizzo di sistemi VPN. Ciò comunque nel rispetto del presente Regolamento.

2. l'uso di tali dispositivi personali è consentito esclusivamente previa autorizzazione da parte dei tecnici del servizio Sistema Informativo, i quali potranno impartire prescrizioni tecniche obbligatorie finalizzate alla salvaguardia della sicurezza ed integrità delle infrastrutture telematiche ed informatiche oltre ai dati dell'*Amministrazione*.

Art. 8. Dispositivi di stampa, fotocopia e fax

1. Ai fini del contenimento dei costi e in considerazione degli obblighi di dematerializzazione in atto nella Pubblica *Amministrazione*, nonché dell'impatto ambientale derivante dalle stesse, le stampanti locali assegnate a singoli *Utenti* sono progressivamente dismesse a vantaggio dell'utilizzo di stampanti di rete dipartimentali collocate in aree comuni e utilizzabili da gruppi definiti di *Utenti* (non legate quindi a singole strutture organizzative).

2. Possono essere previste eccezioni alla regola precedente, su richiesta dei *Responsabili di struttura* interessati e compatibilmente con le disponibilità di magazzino, che dovranno essere di volta in volta autorizzate dal servizio Sistema Informativo e dal Servizio Patrimonio.

3. Le stampanti potranno essere configurate in modo da totalizzare i volumi di stampa per *Utente* e/o postazione di lavoro che le ha effettuate, ciò al fine di poter consentire una corretta contabilità per centri di costo dei relativi oneri di utilizzo.

4. Le stampanti condivise tra più *Utenti* saranno assegnate al *Responsabile di struttura*, mentre quelle personali ancora in funzione saranno assegnate al relativo *Utente* utilizzatore.

5. Le stampanti condivise tra *Utenti* di più strutture organizzative saranno comunque assegnate, a livello di inventario, ad uno dei *Responsabili di Struttura* interessati all'utilizzo.

Art. 9. Dispositivi di Telefonia fissa

1. La postazione di lavoro è di norma corredata da uno più dispositivi di telefonia fissa. Le assegnazioni di linee telefoniche, utenze, apparati e abilitazioni, vengono attribuite dal servizio Sistema informativo sulla base di motivate esigenze espresse dagli *Utenti*, approvate dai relativi *Responsabili di struttura*.

2. I dispositivi di telefonia fissa in uso a più *Utenti* sono formalmente assegnati al *Responsabile di struttura*.

3. Su specifica richiesta del *Responsabile di struttura,* possono essere creati, su gruppi di apparecchi telefonici fissi, servizi di risposta del tipo "call center" per i quali le telefonate indirizzate ad un unico un mero interno sono servite, secondo regole di assegnazione prestabilite, da uno degli apparecchi del gruppo. Sulle linee telefoniche gestire mediante un tale servizio di call center può essere attivata, sempre su richiesta del Responsabile di struttura, la funzionalità di registrazione delle conversazioni.

4. L'attivazione della funzionalità di cui al punto precedente (call center) è soggetta al rispetto del GDPR, le azoni necessarie (Registro trattamenti, informative, Analisi d'impatto, etc.) devono essere intraprese a cura del Responsabile di struttura richiedente prima dell'avvio del servizio.

Art. 10. Dispositivi di telefonia mobile

1. I dispositivi di telefonia mobile si compongono di SIM e apparati (cellulare, smartphone, router wifi, tablet, ecc.).

2. I dispositivi di telefonia mobile, di proprietà o il cui costo del dispositivo è a carico dell'*Amministrazione*, sono assegnati all'*Utente* utilizzatore su specifica richiesta del *Responsabile di struttura* presso cui l'*Utente* presta servizio .

3. I dispositivi assegnabili, di cui al comma precedente, sono esclusivamente quelli disponibili nell'ambito dei contratti di fornitura del servizio di telefonia mobile gestiti dal servizio Sistema informativo.

4. Per particolari esigenze di servizio, gli apparati possono essere messi a disposizione di più *Utenti* e sono, in tal caso, formalmente assegnate al *Responsabile della struttura*.

5. È consentito agli utenti di utilizzare per scopi di servizi propri dispositivi di telefonia mobile, facendosi assegnare, con le procedure di cui ai commi precedenti, soltanto la l'utenza e relativa SIM da parte dell'*Amministrazione*.

6. Inoltre è anche consentito che, mediante procedura di portabilità del proprio numero, l'*Utente* trasferisca la titolarità della propria utenza all'*Amministrazione* esclusivamente nel rispetto di quanto stabilito all'Art. 23.

7. Infine è possibile, in caso di cessazione del rapporto o della prestazione con l'*Amministrazione* da parte dell'Utente, che l'utenza in capo all'*Amministrazione* venga volturata a favore dell'Utente dietro richiesta esplicita di quest'ultimo.

Art. 11. Dotazioni mobili

1. Tutte le attrezzature mobili (PC portatili, Telefoni mobili, tablet, ecc..), di proprietà o il cui costo è a carico dell'*Amministrazione*, possono essere trattenute dall'*Utente* se questo è destinato ad altra mansione, all'interno dell'*Amministrazione*, che necessitava del loro uso a norma dell'Art. 5. In caso ciò non si verifichi, o nel caso di cessazione della prestazione o di assenza o di trasferimenti temporanei di lunga durata ad altri enti, queste sono immediatamente restituite, a cura dell'*Utente* assegnatario, agli addetti alla gestione della manutenzione delle postazioni di lavoro ed agli addetti alla gestione del sistema telefonico dell'*Amministrazione* per poter essere riutilizzate.

Art. 12. File server

1. I sistemi di file server centralizzati prevedono spazi di memorizzazione dedicati al singolo *Utente* e spazi condivisi tra gli *Utenti* di strutture organizzative e progetti.

2. Le abilitazioni all'utilizzo degli spazi di memorizzazione condivisi rispecchiano generalmente la struttura organizzativa di appartenenza di ciascun *Utente* o la partecipazione a progetti trasversali o comunque sono configurati su richiesta dei *Responsabili di struttura*.

Art. 13. Connessioni di rete presso la postazione d'ufficio

1. Le postazioni di lavoro fisse sono di norma interconnesse alla rete telematica cablata di edificio dell'*Amministrazione*.

2. Per tali postazioni è da utilizzarsi esclusivamente tale connessione di rete anche se dotate di altri sistemi di connettività.

Art. 14. Connessioni di rete per lavoro a distanza

1. Per la connessione da remoto, utilizzando dispositivi computer portatili, si potrà utilizzare qualunque tipo di connessione fissa o mobile, privata del dipendente o messa a disposizione dall'*Amministrazione*, purché di caratteristiche minime che saranno raccomandate da parte dei tecnici del servizio Sistema Informativo.

2. Il lavoro da remoto sarà possibile o in modalità "disconnessa", mediante lavoro in locale e scambio di informazione con il resto della struttura utilizzando:

    a. I pacchetti software accessibili in sicurezza da internet,

    b. La posta elettronica istituzionale dell'*Amministrazione* ed accessibile anche da internet.

3. Il lavoro da remoto sarà altresì possibile o in modalità "connessa" mediante connessione sicura all'infrastruttura telematica dell'*Amministrazione* realizzata attraverso lo strumento VPN dato in dotazione come indicato all'Art. 5. commi 3 lett. e) e 4 lett. d). In tal caso saranno utilizzabili anche tutte le risorse informatiche accessibili solo dalla intranet dell'*Amministrazione*; possono fare eccezione alcune risorse particolarmente critiche per le quali, dietro valutazione del dirigente del servizio Sistema Informativo, si ritiene sicuro solo l'accesso dalla rete intranet e non tramite VPN.

4. La modalità "connessa" di cui al comma precedente sarà attivabile solamente in caso di dotazione di computer portatile dell'Amministrazione. In caso invece di lavoro da remoto svolto con l'utilizzo di computer privato del dipendente sarà messa a disposizione un'altra modalità di lavoro, sempre di tipo "connessa", ma che consentirà esclusivamente l'accesso al desktop di un computer fisso connesso alla rete dell'ufficio per lo svolgimento del proprio lavoro da tale computer.

Art. 15. Servizio di Posta elettronica

1. Per lo scambio di messaggi di posta elettronica, finalizzati all'espletamento delle attività previste dal rapporto contrattuale con l'*Amministrazione*, saranno assegnati, all'*Utente*, uno o più caselle di posta elettronica, con associati uno o più indirizzi elettronici, accessibili con le credenziali consegnate come indicato all'Art. 5. comma 3 lett. b).

2. Le caselle di posta elettronica assegnate saranno accessibili in sicurezza sia dall'intranet che da qualunque postazione internet anche pubblica in modalità web.

Art. 16. Pacchetti applicativi

1. Sulla base delle esigenze operative dell'*Utente* e sulla base di specifiche richieste da parte del *Responsabile di struttura* presso la quale l'*Utente* presta servizio, sono resi disponibili, da parte del servizio Sistema Informativo, ed accessibili con le credenziali di cui all'Art. 5. comma 3 lett. b), vari pacchetti software.

2. Sui pacchetti applicativi saranno organizzate periodicamente attività di formazione al fine di un loro corretto e sicuro utilizzo.

Art. 17. Accesso ad internet

1. Dalle postazioni di lavoro, sia fisse che mobili, messe a disposizione dell'*Amministrazione* sarà possibile la navigazione nella rete internet ma solo sulla base di opportuni profili autorizzatori basati sulla tipologia di sito acceduto, di protocollo di rete utilizzato, di tipologia di postazione di lavoro dalla quale si effettua l'accesso e di profilo *Utente*.

2. L'assegnazione base, al momento dell'attivazione dell'*Utente*, sarà quella corrispondente al profilo più restrittivo. Il profilo potrà essere modificato in senso più permissivo esclusivamente sulla base di motivata richiesta da parte del *Responsabile di struttura* presso la quale l'*Utente* presta servizio.

Art. 18. Servizio WI-FI

1. Nei locali dell'*Amministrazione* possono essere realizzate varie infrastrutture di rete WI-FI sia ad accesso pubblico che per esclusivo utilizzo a fini specifici scopo di servizio.

2. Le regole di utilizzo di tali infrastrutture sono definite:

    a. per le reti ad accesso pubblico, dagli specifici regolamenti di servizio,

    b. per le reti aventi scopo specifico, da specifiche disposizioni emanate a cura del dirigente del servizio Sistema Informativo.

Titolo III - NORME DI UTILIZZO DELLE DOTAZIONI

Art. 19. Norme generali di comportamento

1. Costituisce regola generale che l'utilizzo delle *Dotazioni* deve essere limitato esclusivamente alle esigenze derivanti dalle proprie funzioni lavorative; non è ammesso l'uso a scopi privati. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza di cui gli *Utenti* rispondono; pertanto tale comportamento potrà essere perseguibile nelle opportune sedi.

2. Gli *Utenti* sono tenuti ad utilizzare le *Dotazioni* messe a loro disposizione con diligenza, adottando comportamenti idonei a non causare danni alle stesse.

3. Gli *Utenti* dovranno osservare gli obblighi specifici di seguito riportati:

    a. è fatto divieto di cedere, anche temporaneamente, a terzi le *Dotazioni*, o loro componenti, e comunque di consentirne l'utilizzo da parte di terzi non specificatamente autorizzati dall'*Amministrazione*;

    b. è fatto divieto di manomettere in qualsiasi modo sia l'hardware che il software delle *Dotazioni* assegnate o di installare componenti hardware e software aggiuntivi non forniti dall'*Amministrazione*;

    c. è fatto divieto di rimuovere o rendere illeggibile il codice identificativo di inventario delle *Dotazioni, ove presente*;

    d. è fatto divieto di impiegare le *Dotazioni* per finalità diverse da quelle per le quali sono state progettate o utilizzarle per compiere azioni illecite verso altri sistemi, sia interni che esterni, all'organizzazione;

    e. nel caso sia necessario portare qualsiasi *Dotazione* fuori della sede di lavoro (ad es. in caso di lavoro a distanza, eventi, corsi, laboratori formativi, ecc.) è fatto obbligo agli *Utenti* di prendere tutte le precauzioni affinché non venga smarrita, danneggiata o rubata, nonché di prestare la massima attenzione a non lasciarla mai incustodita e di conservarla in luoghi protetti;

    f. è fatto obbligo di segnalare tempestivamente eventuali furti o smarrimenti comunicando l'evento al servizio Sistema Informativo;

    g. è fatto obbligo di segnalare ogni anomalia o malfunzionamento riguardante le *Dotazioni* secondo le procedure indicate dal servizio Sistema informativo;

    h. è fatto obbligo effettuare il log-out dalla propria postazione di lavoro al termine della giornata lavorativa e bloccarla in caso di allontanamento dalla stessa;

    i. ai fini del contenimento della spesa energetica, della riduzione dell'impatto ambientale, della necessità di prolungare la vita dei dispositivi, è fatto obbligo di:

        i. spegnere il monitor in caso di temporanea inattività,

        ii. spegnere la postazione al termine della giornata di lavoro (salvo diversa indicazione da parte del servizio Sistema Informativo),

        iii. limitare al minimo indispensabile la produzione di stampe.

4. L'obbligo di cui al comma 3. punti i. e ii. (spegnimento della stazione) è da considerarsi non applicabile quando l'*Utente* deve effettuare attività di lavoro a distanza nella modalità che prevede il collegamento in desktop remoto al proprio PC fisso in ufficio.

5. Gli utenti dovranno rispettare le prescrizioni relative al risparmio energetico di cui all'Art. 39.

Art. 20. Norme generali per e la sicurezza e la protezione dei dai personali

1. E' fatto obbligo agli *Utenti* di archiviare le informazioni e i dati in forma digitale esclusivamente necessari all'attività lavorativa. Costituisce buona regola la pulizia periodica degli archivi, da eseguirsi almeno ogni 6 (sei) mesi, con cancellazione dei file obsoleti o inutili. Particolare attenzione va prestata ad evitare la duplicazione dei dati, al fine di evitare un'archiviazione ridondante ed inutilmente costosa.

2. In caso di trasferimento ad altra struttura o modifica delle proprie mansioni l'*Utente* è tenuto ad eliminare dalla postazione, dalle cartelle di rete personali e dalla posta elettronica eventuali file contenenti dati che non è più autorizzato a trattare; Ove tali dati siano ancora di qualche utilità per altri *Utenti* o strutture dell'*Amministrazione* gli stessi vanno immediatamente passati, senza distruggerli, agli *Utenti* o strutture interessati; il *Responsabile di struttura* è tenuto a revocare le abilitazioni all'uso dei software gestionali e delle risorse condivise (cartelle di rete, liste di distribuzione, ecc.) dell'*Utente*;

3. Più in generale, si ricorda inoltre l'obbligo, al termine dell'orario di lavoro, di:

    a. garantire che materiale informatico rimovibile contenente dati o informazioni relative all'*Amministrazione* siano conservati in appositi cassetti e/o armadi;

    b. ove possibile, chiudere a chiave cassetti, porte degli uffici o di aree ad accesso limitato;

    c. raccogliere tutti i documenti stampati e i documenti che non sono più richiesti/necessari e provvedere alla loro definitiva eliminazione. In ogni caso, tali documenti non devono essere depositati integralmente nei normali cestini da ufficio, ma distrutti precedentemente con l'apposita attrezzatura.

4. Qualora si verificasse il furto o lo smarrimento di una *Dotazione* informatica o di telecomunicazione l'*Utente* è tenuto, immediatamente e comunque entro 24 ore dalla scoperta dell'accaduto a darne comunicare al servizio Sistema Informativo, fornendo tutte le opportune informazioni e chiarimenti in merito, e, se richiesto dal servizio Sistema Informativo, sporgere denuncia alle autorità competenti inviandone copia al servizio Sistema Informativo stesso.

Art. 21. Norme per l'accesso ai sistemi mediante credenziali

1. L'accesso ai sistemi informatici dell'*Amministrazione* è sottoposto a procedure di identificazione personale (log-in) basate sull'utilizzo di credenziali composte, al minimo, da un identificativo univoco (User ID) e di una parola segreta (Password) necessari al riconoscimento della identità degli *Utenti* da parte dei vari componenti informatici.

2. Le credenziali sono rilasciate dal *Servizio Accessi*, dietro specifica delle seguenti informazioni personali:

    a. Nome e Cognome,

    b. Codice Fiscale,

    c. Data del termine del rapporto di lavoro/collaborazione (se conosciuto).

3. Al rilascio della credenziali, il *Responsabile della struttura* presso o per la quale il soggetto svolge la propria attività, deve specificare al *Servizio Accessi* i profili di accesso alle varie procedure e sistemi informatici che saranno utilizzati dall'*Utente* per lo svolgimento della propria attività. Per alcuni sistemi e/o procedure l'impostazione nei conforti degli *Utenti* dei diritti di accesso potrà avvenire, mediante apposita procedura informatica, direttamente a cura del *Responsabile di struttura* cui tali sistemi e/o procedure fanno riferimento, in termini di responsabilità, ai sensi del GDPR.

4. Sono vietati la richiesta ed il rilascio di credenziali d'accesso ai componenti del sistema informatico dell'*Amministrazione* associate ad *Utenti* generici (ufficio, progetto) e non nominativi, cioè non collegati ad un codice fiscale di un *Utente*.

5. In base ad esigenze tecniche potranno essere rilasciate ai soggetti più credenziali di accesso da utilizzarsi ciascuna per parti differenti del sistema informatico dell'*Amministrazione*.

6. Al variare della mansione o ufficio i diritti di accesso ed i profili autorizzatori relativi alle varie *Dotazioni* e sistemi informatici dell'*Utente* dovranno essere variati con procedure simili a quelle adottate all'inizio del rapporto di lavoro o collaborazione, ad iniziativa e cura del *Responsabile di struttura* di destinazione.

7. Le credenziali sono segrete e strettamente personali; l'*Utente* è tenuto :

    a. a mantenere la riservatezza delle proprie credenziali d'accesso alle *Dotazioni*, consegnate come indicato all'Art. 5. comma 3 lett. b). evitando di comunicarle ad altri soggetti e pertanto:

        i. a non inserirle in messaggi di posta elettronica o trasmetterle attraverso qualsiasi altra forma di comunicazione elettronica (anche se cifrata);

        ii. a non salvarle su strumenti o documenti informatici che non siano protetti a loro volta da apposite chiavi strettamente personali;

        iii. a non trascriverle su fogli, biglietti, post-it o su oggetti, soprattutto se posti nelle vicinanze del PC.

    b. A non attivare sistemi di memorizzazione di password durante l'utilizzo di strumenti informatici specie durante la navigazione web anche su pagine e applicativi web dell'*Amministrazione*.

    c. A modificare la password al momento del primo utilizzo (se questa è pre-impostata in modo da essere conosciuta ad altri) e ogniqualvolta richiesto dalle procedure automatiche di cambio password impostate nei sistemi, nonché tutte le volte ritenga siano venuti meno i requisiti di riservatezza;

    d. A scegliere ogni nuova password rispettando i vincoli imposti dalle singole procedure e/o dalle regole tecniche decise dal responsabile del servizio Sistema Informativo;

    e. A bloccare l'accesso, ove previsto, ai dispositivi mobili con PIN o altro sistema disponibile ;

8. I servizi utilizzabili per il cambio password e le regole in vigore per la scelta di nuove password sono rese disponibili sulle pagine del portale intranet dell'*Amministrazione*.

9. E' assolutamente proibito entrare nella rete e nei programmi con credenziali attribuite ad altro *Utente*.

10. L'*Utente* è responsabile di qualsiasi azione o attività svolta tramite l'utilizzo delle credenziali personali a lui assegnate, anche se usate da altro soggetto se le stesse non sono state conservate secondo le norme di cui al presente Regolamento.

11. Per ragioni di sicurezza i tecnici del servizio Sistema Informativo possono disattivare temporaneamente l'accesso alla postazione, alla rete o ad alcuni o tutti gli strumenti informatici cui risulta abilitato un *Utente* fino al ripristino delle condizioni di sicurezza.

Art. 22. Utilizzo della postazione di lavoro

1. I componenti hardware e software delle postazioni di lavoro fisse e mobili vengono installati, configurati e aggiornati dai tecnici incaricati dal servizio Sistema Informativo secondo configurazioni di riferimento predefinite. Installazioni di hardware e software diverse dalla configurazione iniziale sono autorizzate ed eseguite esclusivamente dai tecnici del servizio Sistema Informativo, ciò risulta vero anche per gli applicativi per i quali non sono richiesti, per la loro installazione, i privilegi di amministratore di sistema.

2. L'accesso alle *Dotazioni* è configurato in modo specifico per ciascun *Utente* e non prevede la concessione a quest'ultimo di privilegi di amministratore di sistema. Casi particolari, legati a vincoli e/o limiti del singolo pacchetto software, saranno valutati a cura dei tecnici del servizio Sistema informativo al fine di poter concedere, anche solo temporaneamente, i privilegi di amministratore di sistema, ma a valere solo sulla singola risorsa informatica interessata. Ciò avverrà comunque solo dopo che i tecnici del servizio Sistema Informativo avranno informato l'*Utente* dei rischi e precauzioni che comporterà agire con questo tipo di privilegi. La concessione di privilegi di amministratore di sistema locale non pregiudica comunque il rispetto degli obblighi di cui all'Art. 19. e del presente Regolamento.

3. Le seguenti attività sono espressamente proibite agli *Utenti*:

    a. utilizzare e/o installare apparati di telecomunicazione diversi da quelli forniti in dotazione;

    b. qualora la postazione informatica sia dotate di connessione di rete aggiuntiva, wired o wireless, che possa consentire la connessione ad altre reti pubbliche, attivare tali connessioni aggiuntive quando la postazione sia contemporaneamente connessa alla rete fissa o mobile dell'*Amministrazione*; l'accesso con tali modalità alternative dovrà avvenire disattivando ogni altro dispositivo di connessione alla rete comunale;

    c. modificare la configurazione hardware e/o software in dotazione, installare/effettuare download di software/applicativi non autorizzati, anche se ritenuti dallo stesso necessari alla propria attività. L'installazione di software non autorizzato dal servizio Sistema Informativo viene considerato come manomissione del sistema;

    d. eliminare un programma o file installato legalmente in modo tale da impedire od ostacolare le normali operazioni, ivi inclusa la disattivazione dei sistemi di sicurezza;

    e. acquisire, utilizzare, duplicare software illegalmente;

    f. effettuare qualsiasi attività finalizzata a mettere alla prova la sicurezza del sistema informatico, salvo esplicita autorizzazione fornita dal servizio Sistema Informativo.

4. I tecnici del servizio Sistema Informativo sono autorizzati a rimuovere, anche mediante procedura automatizzata da remoto, ogni anomalia introdotta dagli *Utenti* sulla postazione di lavoro.

5. Nel caso in cui gli *Utenti* vengano a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi, dovranno darne tempestivamente comunicazione al servizio Sistema informativo.

Art. 23. Utilizzo delle dotazioni di telefonia fissa e mobile

1. L'assegnazione delle *Dotazioni* di telefonia è finalizzata allo svolgimento dell'attività lavorativa. L'*Utente* sarà ritenuto esclusivo responsabile per ogni eventuale danno nei confronti dell'*Amministrazione* o di terzi che dovesse derivare dall'utilizzo improprio dei dispositivi. Ogni utilizzo non inerente all'esercizio delle funzioni assegnate all'*Utente* può infatti contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza; pertanto nel caso in cui l'*Amministrazione* dovesse sostenere costi dovuti a un uso improprio del dispositivo di telefonia mobile assegnato o all'inosservanza del presente Regolamento, essi potranno essere addebitati all'assegnatario.

2. L'utilizzo dell'apparato di telefonia mobile di servizio per telefonate personali è consentito esclusivamente quando l'assegnatario accetta la fatturazione separata a proprio carico di tali telefonate, con un contratto di tipo "dual billing"[5], qualora disponibile nel profilo tariffario della SIM assegnata e dal contratto con l'operatore di telefonia.

3. Nell'utilizzo delle *Dotazioni* di telefonia è fatto divieto all'*Utente*:

    a. di chiamare numeri a pagamento, salva preventiva autorizzazione del proprio *Responsabile di Struttura* e per soli scopi di servizio;

    b. di attivare servizi di deviazione da numerazione fissa a numerazione esterna e da numerazione fissa a numerazione mobile. Eventuali deroghe vanno motivate e devono essere autorizzate dal proprio *Responsabile di Struttura* o essere necessarie per l'espletamento della propria attività in modalità remota;

    c. di utilizzare le SIM assegnate dall'*Amministrazione* su apparati diversi da quelli assegnati;

    d. di utilizzare SIM personali in apparati mobili forniti dall'*Amministrazione*.

4. Nell'utilizzo delle *Dotazioni* di telefonia mobile è fatto obbligo di bloccare l'accesso al dispositivo mobili con PIN o altro sistema disponibile;

5. Le apparecchiature utilizzate per l'allestimento di servizi di "call center", come descritto all' Art. 9. Non consentono comunque di eseguire analisi dell'attività dei singoli operatori, ma solo statistiche complessive del servizio connesso alle linee entranti e ciò al fine di scongiurare qualunque forma di controllo a distanza dei lavoratori interessati.

Art. 24. Utilizzo delle stampanti, fotocopiatrici e fax

1. Gli *Utenti* sono tenuti ad effettuare stampe, fotocopie e fax esclusivamente per esigenze di servizio. E' fatto divieto di effettuare stampe e fotocopie di materiale di utilità personale.

2. Durante l'effettuazione delle stampe, fotocopie, scansioni ed invio via fax di documenti, al fine di impedire la volontaria o accidentale diffusione di dati personali o la perdita di riservatezza sulle informazioni contenute nei documenti che vengono stampati, l'*Utente* che effettua l'operazione è tenuto a presidiare l'intero processo di stampa, fotocopia, scansione o trasmissione via fax di

[5] Regime contrattuale che prevede una fatturazione separata, direttamente in capo all'*Utente*, delle telefonate personali identificate mediante un opportuno sistema indicato dal gestore al momento della chiamata.

documenti, evitando che soggetti non autorizzati possano entrare in possesso o prendere visione degli stessi.

3. Nel caso di scansioni con invio del file scansionato in una cartella di rete condivisa con altri Utenti, l'utente che effettua la scansione deve provvedere a prelevare il file con il risultato della scansione nel più breve tempo possibile per depositarlo nello spazio disco adatto a proteggerne la riservatezza.

4. In ogni caso in contenuto delle cartelle di rete dedicate alla ricezione di file relativi a scansioni da apparecchiature multifunzione sarà inesorabilmente cancellato in automatico ogni notte.

Art. 25. Utilizzo dello spazio disco

1. L'integrità e la disponibilità delle informazioni e dei dati, ivi inclusi i dati personali, sono garantite solo quando gli stessi sono memorizzati nei file server di rete (i c.d. dischi di rete) e/o dispositivi di memorizzazione messi a disposizione dall'*Amministrazione*, e che sono oggetto di misure di protezione, monitoraggio e backup. Gli *Utenti* devono pertanto salvare documenti e dati, relativi alla propria attività lavorativa, esclusivamente sui sistemi di memorizzazione di cui sopra, utilizzando gli spazi opportuni ed in base strettamente al tipo di accesso che deve essere garantito ad altri *Utenti* della struttura e/o dell'*Amministrazione*.

2. Non è consentito il salvataggio di dati, inerenti l'attività lavorativa su spazi di memorizzazione localizzata sui dischi interni alle postazioni di lavoro (incluso lo spazio sul desktop virtuale – schermo - del computer), né su memorie esterne rimovibili (hard disk esterni, chiavette USB, ecc.).

3. Qualora, per specifiche eccezionali esigenze e nel rispetto delle normative in tema di protezione dei dati personali, sia autorizzato in sicurezza dal servizio Sistema informativo l'utilizzo di memorie esterne, è fatto obbligo all'*Utente* di conservare tali dispositivi di memora esterni in luoghi da lui protetti (ad es. armadi e cassettiere chiusi a chiave con accesso a riservato esclusivamente a chi è autorizzato al relativo trattamento), verificare il loro contenuto informativo prima della loro eventuale consegna a terzi e prima della loro eliminazione/distruzione o sostituzione, nonché procedere alla cancellazione dei dati in essi contenuti quando non più necessari.

4. Salvo che la procedura informatica messa a disposizione dall'*Amministrazione* preveda strutturalmente il salvataggio dei dati sullo spazio disco all'interno della postazione di lavoro o su supporti rimuovibili, eventualità che sarà stata dunque valutata nell'ambito delle procedure di valutazione del rischio sul relativo trattamento, ogni altra costituzione di archivio dati personali all'interno di dotazioni hardware dell'Utente o su supporti rimuovibili costituirà trattamento dati non di pertinenza dell'*Amministrazione* e del quale sarà pienamente titolare, ai sensi di legge, l'*Utente* che ha costituito tale archivio dati. Sarà dunque quest'ultimo a dover valutare i rischi relativi e ad assumere in proprio le opportune misure di contrasto per tali rischi. L'Utente sarà dunque anche responsabile del pieno rispetto delle prescrizioni sui trattamenti dati di cui al GDPR.

Art. 26. Utilizzo delle connessioni di rete

1. La rete telematica dell'*Amministrazione* si basa principalmente su un'infrastruttura cablata e proprietaria che fa uso di collegamenti cittadini proprietari e/o affittati da operatori di telecomunicazione privati. Tale infrastruttura serve tutte le postazioni di lavoro presso gli uffici serviti dal sistema informatico dell'*Amministrazione*.

2. L'infrastruttura telematica comunale è dunque principalmente basata su connessioni di rete "wired", ma possono essere presenti zone coperte mediante connessioni "wireless" (es.: tecnologia WI-FI).

3. L’accesso alla rete telematica comunale può avvenire anche mediante tecniche VPN in caso di attività svolta da remoto, ciò esclusivamente mediante le tecniche, *Dotazioni* e regole di sicurezza definite dal presente Regolamento.

4. La rete telematica è gestita dagli addetti del servizio Sistema Informativo dell’*Amministrazione* o da soggetti esterni da quest’ultimo incaricati. Dagli stessi soggetti è esclusivamente curata la configurazione degli apparti informatici che utilizzano della rete telematica.

5. È vietato collegare alla rete telematica comunale apparati non forniti dell'*Amministrazione* e comunque senza l’intervento del tecnici all’uopo incaricati, salvo che ciò sia esplicitamente e preventivamente autorizzato dal servizio Sistema Informativo.

6. È fatto divieto di estendere, modificare o alterare la struttura della rete telematica comunale intervenendo sui suoi apparati costitutivi o aggiungendone altri senza l’intervento diretto degli addetti del servizio Sistema Informativo o di loro incaricati.

Art. 27. Utilizzo dei wi-fi

7. E’ fatto divieto agli *Utenti*, ed è considerata grave violazione della sicurezza dell’infrastruttura telematica dell’*Amministrazione*, la realizzazione di infrastrutture Wi-Fi diverse da quelle realizzate dalla stessa *Amministrazione*.

8. È anche vietato realizzare infrastrutture di rete personali che consentano la condivisione dei dati accessibili dai propri dispositivi in dotazione (es.: Tethering, Bluetooth).

Art. 28. Utilizzo dell’acceso ad internet

1. Agli *Utenti* dell’infrastruttura telematica comunale è consentito l’accesso alla rete internet per esclusivi scopi lavorativi.

2. L’accesso ad internet avviene attraverso apparati di controllo della navigazione i quali registrano ogni accesso tenendo traccia delle attività di ciascun *Utente* e di ciascuna postazione informatica. Le attività di navigazione sulla rete internet sono in tal modo tracciate su un sistema di “log”, comunque nel rispetto di quanto stabilito dalla L. 300/1970 e dal GDPR.

3. Per ridurre il rischio di usi impropri e/o pericolosi della navigazione in Internet, vengono implementate misure di accesso filtrato mediante strumenti che inibiscono l'accesso a specifici siti o pagine ritenuti non inerenti l’attività lavorativa e che analizzano i contenuti acceduti per verificare l’assenza di malware conosciuti.

4. Gli eventuali controlli, circa l’uso improprio del servizio di navigazione internet, possono avvenire mediante accesso al sistema di log di cui sopra, nel rispetto del successivo Art. 36. Il controllo sui file di log non è continuativo e sistematico, ma viene effettuato soltanto dietro motivata richiesta del *Responsabile di struttura* a cui l’*Utente* individuato è assegnato. In ogni caso, i file vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità dell’Ente e nel rispetto delle disposizioni di legge sulla materia.

5. I log raccolti con il sistema di controllo della navigazione Internet possono essere utilizzati anche per individuare tentativi, reali o potenziali, di accesso non autorizzato o fraudolento al sistema informatico comunale.

6. Al fine di garantire un appropriato utilizzo della rete internet, gli *Utenti* devono rispettare le seguenti regole:

a. è consentita la navigazione in internet solo su siti contenenti informazioni necessarie o utili all'attività lavorativa o, comunque, all'acquisizione di notizie utili alla propria formazione/informazione professionale;

b. l'*Utente* non è mai autorizzato all'installazione di programmi o software particolari per la fruizione di servizi e contenuti e non è altresì autorizzato ad effettuare il download di software, file musicali, video etc. con finalità estranee all'attività lavorativa;

c. deve rispettare le norme in materia di diritto di autore e altri diritti connessi e di utilizzo della rete;

d. non è autorizzato ad accedere a servizi di condivisione di file in modalità peer-to-peer;

e. non deve utilizzare sistemi per l'offuscamento della connessione con la finalità di rendere nascosta la propria identità nella rete, in particolare è vietato l'utilizzo di servizi/software di anonimizzazione della navigazione;

f. durante il servizio non è permesso, salvo che per motivi lavorativi, professionali, formativi, specificatamente autorizzati dal proprio *Responsabile di Struttura*, partecipare a forum, utilizzare chat line o bacheche elettroniche, social network (quali Facebook, Instagram, Twitter, ecc.), anche usando pseudonimi;

7. l'*Utente* è personalmente responsabile della propria condotta nell'utilizzo delle reti e dei servizi di telecomunicazione.

Art. 29. Servizi cloud

1. E' vietato all'*Utente* utilizzare, di propria iniziativa, qualsiasi servizio di cloud pubblico quali, a titolo puramente esemplificativo e non esaustivo, Google drive, Apple iCloud, Dropbox, Microsoft drive, WeTransfer, e simili, che prevedano la memorizzazione e/o lo scambio, anche solo temporaneo, di dati e documenti di proprietà dell'*Amministrazione,* ed in particolare che contengano dati personali facendoli transitare da sistemi informatici e spazi di memorizzazione dati di proprietà di terzi.

2. E' fatto salvo l'utilizzo di servizi del cloud pubblico specificatamente indicati dall'*Amministrazione* purché ciò avvenga secondo le indicazioni e le modalità specificatamente indicate da parte del servizio Sistema Informativo.

3. Ove si renda necessario accedere ad un servizio del cloud pubblico per vincoli imposti dall'esterno, l'*Utente* deve preventivamente ricevere autorizzazione da parte del servizio Sistema Informativo e seguire le indicazioni ed istruzioni di sicurezza eventualmente indicate da quest'ultimo.

4. Per lo scambio da e per l'esterno di file di grosse dimensioni è a disposizione un sistema di deposito temporaneo accessibile anche dall'esterno e nel pieno rispetto di quanto sopra indicato, ed utilizzabile all'indirizzo indicato dal servizio Sistema Informativo[5].

Art. 30. Utilizzo di servizi di connettività fuori dall'ufficio

1. L'utilizzo, dai dispositivi avuti in dotazione dall'*Amministrazione*, di servizi di connettività diversi da quelli forniti all'interno degli uffici Comunali, è consentito solo rispettando le regole ed impostazioni di sicurezza configurate, sui dispositivi in dotazione, a cura dei tecnici del servizio Sistema Informativo.

2. E' fatto divieto di disattivare o disinstallare tali impostazioni di sicurezza.

Art. 31. Lavoro da Remoto

1. L'attività lavorativa da remoto è consentita esclusivamente o mediante l'accesso ai servizi applicativi dell'*Amministrazione* disponibili in internet e/o mediante l'interconnessione alla infrastruttura intranet dell'*Amministrazione* utilizzando esclusivamente le modalità di cui ai commi 3 e 4 del precedente Art. 14. messi a disposizione dai tecnici del servizio Sistema Informativo e così come attivati con le procedure di cui all' Art. 5. Comma 3 lett. e) e comma 4 lett. d).

2. Le limitazioni all'uso di internet e dei servizi cloud di cui agli articoli precedenti è applicabile anche al lavoro da remoto se è eseguito utilizzando *Dotazioni* dell'*Amministrazione*.

3. E' vietato accedere ad internet ed ai servizi cloud per scopi personali quando si è connessi alla rete intranet dell'*Amministrazione* mediante la VPN.

Art. 32. Utilizzo della posta elettronica

1. Agli *Utenti* del sistema informatico comunale è consentito l'utilizzo della posta elettronica per esclusivi scopi lavorativi.

2. Gli *Utenti* assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse, nonché di garantire la riservatezza delle credenziali di accesso.

3. Ad ogni *Utente* del sistema informatico dell'*Amministrazione* è attribuita una o più caselle di posta e uno o più indirizzi di posta elettronica associati ad esse.

4. Alla casella di posta elettronica di base è sempre assegnato un indirizzo di posta che richiama le generalità dell'*Utente*.

5. Per un miglior coordinamento del lavoro di ufficio possono essere create caselle ed indirizzi di posta condivisi tra più *Utenti* con diritti di accesso differenziati in base alle richieste dei relativi *Responsabili di Struttura*.

6. Per un più agevole inoltro dei messaggi di posta elettronica possono essere create liste di distribuzione in entrata e/o in uscita, con associato un indirizzo impersonale. L'invio di messaggi a tale tipologia di indirizzi provocherà l'invio dello stesso messaggio a tutta la lista di indirizzi o caselle inserite nella lista.

7. Gli indirizzi di posta elettronica associati alle caselle di posta non strettamente personali, potranno richiamare il nome dell'ufficio o del servizio a cui si riferiscono.

8. Gli indirizzi di posta elettronica, anche personali, potranno essere pubblicati, ove necessario, nelle pagine dei siti internet gestiti dall'*Amministrazione*.

9. Per un corretto utilizzo della posta elettronica vanno rispettate le seguenti indicazioni:

    a. Spam: i messaggi di posta elettronica ricevuti, per loro natura, possono contenere informazioni o richieste anche non veritiere, e anche l'indirizzo stesso del mittente può essere falsificato. I messaggi di posta sono analizzati e filtrati con un sistema automatico antispam ed anti-malware. È fatto comunque obbligo agli *Utenti* di non aprire documenti, eseguire programmi, seguire link a siti internet, contenuti in messaggi di provenienza incerta, ed è fatto divieto di rispondere a tali messaggi, che vanno invece segnalati agli addetti del servizio Sistema Informativo. In caso di dubbi sull'autenticità di messaggi richiedere il supporto tramite inoltro della mail sospetta ad un indirizzo che sarà reso noto dagli addetti al servizio Sistema Informativo;

b. Allegati: va controllata la dimensione degli allegati, inviando allegati di grandi dimensioni solo quando effettivamente necessario, e che le dimensioni non superino i limiti imposti dal sistema di posta trasmittente e/o ricevente e dopo aver verificato se non sia possibile un loro ridimensionamento, effettuando delle conversioni di formato o compressioni. Preferire, ogni volta che sia possibile, una delle seguenti tecniche alternative:

    i. Indicare un percorso di rete accessibile al destinatario in cui il documento da trasmettere è depositato;

    ii. Depositare il documento sul sistema di deposito temporaneo accessibile anche dall'esterno[6] e, nel pieno rispetto del precedente Art. 29. , quindi creare un link anonimo a tale deposito temporaneo, ed infine comunicare al corrispondente tale link, preoccupandosi di cancellare il documento dallo spazio temporaneo creato dopo lo scarico avvenuto da parte del corrispondente;

    iii. Annunciare via mail la spedizione del documento da effettuarsi mediante consegna separata di supporto di memorizzazione di massa rimovibile.

c. Firme e Conferme di lettura: non vanno impostate automaticamente per tutti i messaggi, ma inserite al bisogno in fase di composizione del singolo messaggio; Sono fatti salvi gli eventuali messaggi automatici di cui al successivo comma 19.

d. Manutenzione: è necessario verificare periodicamente l'archivio della propria casella di posta elettronica conservando solo la corrispondenza strettamente necessaria alla propria attività; gli *Utenti* sono tenuti a mantenere in ordine la propria casella di posta elettronica, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego delle risorse informatiche;

e. Invio "massivo": i messaggi di posta elettronica vanno inviati solo ai destinatari oggettivamente interessati alla comunicazione cercando di limitarne il più possibile il numero, in particolare è vietata la diffusione di "catene" di ogni genere e tipo; si informa che invii massivi possono causare il blocco, per motivi di sicurezza, dell'account di posta elettronica; per l'invio di messaggi periodico a liste di indirizzi di notevoli dimensioni utilizzare i servizi di newsletter messi a disposizione dal servizio Sistema Informativo e non il normale servizio di posta elettronica;

f. liste di distribuzione esterne: evitare di iscriversi a mailing list esterne salvo che queste non siano utili per l'espletamento della propria attività lavorativa ed in ogni caso dopo aver accuratamente verificato in anticipo se tali servizi siano affidabili;

g. Uso del proprio indirizzo: non utilizzare l'indirizzo di posta elettronica dell'*Amministrazione* per la partecipazione a dibattiti, chat, forum, social network o mailing-list o per l'iscrizione a servizi di qualunque genere per uso privato, nemmeno utilizzando pseudonimi.

10. Si precisa che le caselle di posta elettronica non sono da considerarsi archivi ed il contenuto deve essere considerato esclusivamente temporaneo e non destinato alla conservazione nel tempo. L'archiviazione di documenti digitali nel tempo può avvenire esclusivamente mediante gli appositi applicativi e nel rispetto, ove necessario, delle norme del D.Lgs 82/2005 (CAD) in merito all'archiviazione sostituiva.

[6] Per lo scopo è disponibile uno spazio "cloud" dell'Amministrazione che può essere liberamente utilizzato dagli Utenti all'indirizzo http://dropbox.comune.prato.it

11. Le caselle di posta dell'*Amministrazione* possono pertanto anche essere soggette a cancellazioni massive automatiche ai fini della razionalizzazione delle risorse informatiche utilizzate. L'Utente risponde della perdita di documenti a causa della mancata loro memorizzazione secondo i principi del precedente punto 10.

12. La casella di posta elettronica anche personale, è da intendersi ad esclusivo uso per scopi d'ufficio e non può pertanto essere utilizzata per comunicazioni di tipo personale. Dato lo scopo della stessa, e nei soli casi stabiliti dal presente Regolamento, sarà dunque possibile un accesso a tale casella da parte dell'*Amministrazione* o da soggetti terzi legittimati secondo la casistica sotto riportata.

13. Al fine di assicurare la disponibilità del contenuto di una casella di posta elettronica personale, in caso di improvvisa o prolungata assenza degli *Utenti*, di un loro impedimento o a seguito di cessazione del rapporto di lavoro/collaborazione, l'accesso alla predetta casella di posta elettronica potrà essere effettuato per il tramite di persona fiduciaria nominata dall'*Utente* o, in caso di impossibilità di tale nomina, dall'Amministratore di Sistema, su richiesta del *Responsabile di struttura* di appartenenza dell'*Utente*. Di tale attività sarà redatto apposito verbale e, ove possibile, informato l'*Utente* interessato alla prima occasione utile[7].

14. Una volta disattivato l'account di posta elettronica, copia dei messaggi di posta elettronica sarà conservata entro i termini previsti dalle regole di "retention", salvo che vi siano elementi che inducano l'*Amministrazione* a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

15. In caso di disabilitazione dell'*Utente*, per la casella di posta elettronica personale, potrà essere attivato un servizio di risposta automatica per un congruo periodo di tempo da definirsi con il servizio Sistema informativo.

16. Le politiche di attivazione e disattivazione delle caselle e/o indirizzi di posta elettronica, i tempi di "retention", nonché le modalità e tempi di attivazione di messaggi di risposta automatica, sono stabiliti da provvedimenti dei Dirigente del Servizio Sistema Informativo.

17. Oltre al caso di cui al precedente comma 13, non è consentito ad alcuno l'accesso alle caselle di posta elettronica personali dell'*Utente*, fatte salve le richieste dell'Autorità Giudiziaria e le esigenze dell'*Amministrazione* nel rispetto di quanto previsto dai provvedimenti del Garante della Privacy e dalle norme vigenti.

18. Per combattere i fenomeni dello Spamming e del Phishing è utilizzato apposito sistema per l'analisi automatica dei messaggi di posta in transito. Tale analisi genera opportune registrazioni ("log") che possono essere analizzati anche in differita con le limitazioni di cui all' Art. 36.

19. Nei messaggi di posta elettronica inviati dalle caselle postali dell'*Amministrazione* potranno essere inseriti, anche in automatico, messaggi relativi sia alla riservatezza che ai diritti di quest'ultima sul contenuto dei messaggi, nonché avvertimenti ai destinatari relativi alla natura non personale del messaggio ed alla possibilità che le risposte potranno essere conosciute nell´ organizzazione di appartenenza del mittente[7].

[7] C.f.r. punto II disposizione delle "le linee guida del Garante per posta elettronica e internet – Del. n. 13 del 1° marzo 2007.

Art. 33. Utilizzo del software applicativo

1. Ciascun *Utente* deve far uso esclusivamente dei pacchetti applicativi strettamene necessari alla propria attività d'ufficio e secondo le indicazioni del proprio *Responsabile di Struttura*.
2. Per ciascun software applicativo, ogni *Utente* deve utilizzare esclusivamente le credenziali personali che gli sono state allo scopo rilasciate per quell'applicativo.
3. E' fatto divieto di continuare ad accedere a pacchetti software, quando questi non sono più necessari alla propria attività anche se si permane in possesso di credenziali valide.
4. Cessata la necessità di utilizzo di un pacchetto software, e se ciò non avvenisse d'ufficio per qualunque ragione, l'*Utente* deve chiedere l'immediata disabilitazione all'uso di quel pacchetto comunicando tale evenienza agli addetti alla gestione degli accessi presso il servizio Sistema Informativo.

Art. 34. Software anti-malware

1. Le postazioni sono dotate di strumenti antivirus aggiornati centralmente con strumenti di distribuzione automatica del software.
2. Le postazioni possono essere dotate di strumenti per la raccolta di eventi, operazioni e situazioni, utili ad indentificare ogni possibile tentativo di operazione malevola o dannosa ad opera sia degli *Utenti* che di terzi. Tali eventi saranno raccolti in appositi "log" trattati nel rispetto del successivo Art. 36. e delle disposizioni vigenti in materia.
3. È vietato disattivare gli strumenti di cui ai punti precedente presenti sulla *Dotazione* informatica, modificarne la configurazione o usare strumenti similari differenti da quelli forniti dall'*Amministrazione*.

Titolo IV - REVOCA DELLE ASSEGNAZIONI DELLE DOTAZIONI

Art. 35. Conclusione del rapporto

1. Alla conclusione del rapporto di lavoro o allo scadere del rapporto di collaborazione cessano l'assegnazione delle *Dotazioni*, l'accesso al sistema informatico dell'*Amministrazione* ed ai software applicativi.
2. Contestualmente, i dispositivi mobili (ad es. cellulari, tablet, notebook, ecc.) devono essere riconsegnati al servizio Sistema informativo.
3. Le abilitazioni dell'*Utente* vengono disattivate con riferimento:
    a. Per i di pendenti: alla data di cessazione resa evidente dai sistemi di gestione del personale;
    b. Per i collaboratori ad altro titolo: alla data indicata nella richiesta di abilitazione e comunque della notifica di cessazione del rapporto con l'*Amministrazione* o su richiesta del *Responsabile di struttura*.
4. Non è consentito ad alcuno l'accesso ai dati dell'*Utente* salvati nelle caselle di posta elettronica personale, fatte salve le richieste dell'Autorità Giudiziaria e le esigenze dell'*Amministrazione* nel rispetto di quanto previsto dal GDPR e dalle norme vigenti ed esplicitamente definite dal presente Regolamento.
5. Quando il rapporto di lavoro o collaborazione venga a cessare, è fatto divieto all'*Utente* di conservare, duplicare, comunicare o diffondere informazioni e dati di proprietà dell'*Amministrazione*.

6. In qualunque momento è facoltà dei *Responsabili di struttura* disporre la revoca dell'assegnazione dei dispositivi mobili.

Titolo V - ALTRE DISPOSIZIONI

Art. 36. Controlli

1. L'*Amministrazione*, per motivi organizzativi o di sicurezza si riserva la facoltà di effettuare, per il tramite dei tecnici del servizio Sistema Informativo, controlli saltuari e occasionali, garantendo agli *Utenti* il rispetto dei principi di liceità, pertinenza e non, eccedenza previsti dalla normativa applicabile, di quanto previsto dai provvedimenti del Garante della Privacy, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.
2. L'*Amministrazione* si riserva, in particolare, di monitorare le reti e le *Dotazioni* nei seguenti casi:
    a. necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
    b. monitorare i livelli di utilizzo delle stesse ai fini di una loro ottimizzazione
    c. constatazione di utilizzo indebito della posta elettronica e della rete Internet;
    d. necessità di effettuare verifiche tese alla protezione del patrimonio dell'*Amministrazione*;
    e. presenza di casi di abusi da parte di singoli o reiterati abusi;
    f. presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.
3. Su richiesta dell'Autorità giudiziaria l'*Amministrazione*, per il tramite dei tecnici del servizio Sistema Informativo o di incaricati della stessa Autorità Giudiziaria, è tenuto ad effettuare qualsiasi controllo sull'utilizzo delle *Dotazioni*.
4. Controlli periodici possono essere effettuati, anche a campione, su:
    a. volume dei messaggi scambiati,
    b. formato e dimensione dei file allegati,
    c. durata dei collegamenti ad Internet (globale, per funzione, per gruppi o tipologia di *Utenti*),
    d. siti visitati più frequentemente (globale, per funzione, per gruppi o tipologia di *Utenti*),
    e. informazioni raccolte dai dispositivi di sicurezza (firewall, antivirus, IDS, IPS, ecc.).
5. Le modalità con cui verranno effettuati i controlli saranno le seguenti:
    a. i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di *Utenti*, su dati aggregati e anonimi tramite l'analisi di statistiche generali;
    b. successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate;
    c. in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.
6. In ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail, ivi inclusi i salvataggi periodici dei dati (c.d. "back up"); inoltre non si procede alla

riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'*Utente*, né alla lettura o alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo.

7. L'effettuazione di tali controlli, che non hanno lo scopo di monitorare l'attività degli *Utenti*, bensì di verificare la sicurezza del sistema e per effettuarne la manutenzione, avverranno nel pieno rispetto della Normativa Applicabile.

8. Con particolare riferimento all'utilizzo dei telefoni, sempre nel rispetto della normativa applicabile, l'*Amministrazione* effettua verifiche periodiche volte a verificare la coerenza dei costi derivanti dalle utenze telefoniche associate con i suddetti apparecchi. A tal proposito verranno segnalati agli *Utenti* eventuali discrepanze o problemi che dovessero essere riscontrati nel corso di tali controlli.

9. Tutti i log raccolti dai vari componenti del sistema informatico dell'*Amministrazione* sono conservati e trattati secondo quanto stabilito al successivo Art. 37.

10. Allo scopo di garantire i diritti degli *Utenti* i dati prodotti dai monitoraggi di cui ai commi precedenti non possono essere oggetto di elaborazioni volte a definire il profilo o la personalità dell'*Utente* ovvero ad individuarne loro dati sensibili e/o giudiziari.

11. I tecnici del servizio Sistema Informativo o loro incaricati possono, in qualunque momento, procedere alla rimozione di ogni file o applicazione che si riterrà essere pericoloso per la sicurezza dei sistemi informatici dell'*Amministrazione* o che possano causare danni a terzi, sia sui dispositivi d'*Utente* che sulle unità di rete.

12. I tecnici del servizio Sistema Informativo o loro incaricati possono inoltre procedere, in qualunque momento, alla rimozione di ogni file contenente dati non pertinenti all'attività d'ufficio, sia sui dispositivi d'*Utente* che sulle unità di rete.

13. Con il presente Regolamento è fornita informativa agli *Utenti*, anche ai sensi dell'art. 13 del GDPR, in merito ai controlli e al relativo trattamento dati; l'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità organizzative e di sicurezza, ed in linea con le eventuali prescrizioni di legge.

Art. 37. Tracciamento operazioni e copie di sicurezza

1. Tutti i componenti del sistema informatico dell'*Amministrazione* producono, durante il loro funzionamento, informazioni di tracciatura dei vari eventi corredate di dettagli, circa le operazioni effettuate, utili a ricostruire, anche successivamente, quanto accaduto. Tali informazioni sono registrate in appositi file all'interno dei sistemi e sono genericamente indicate come "log".

2. Sulla raccolta e conservazione dei vari file di log, prodotti dai diversi componenti del sistema informatico dell'*Amministrazione,* saranno applicate le disposizioni di cui provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e sue successive modifiche, integrazioni e precisazioni.

3. Stante la continua evoluzione della normativa in materia, le continue innovazioni tecnologiche ed il mutare delle esigenze di controllo della integrità e funzionamento dei sistemi, le tipologie dei vari file di log ed il loro ciclo di vita, ivi inclusi i tempi massimi di conservazione, sono stabiliti con provvedimenti del Dirigente del Servizio Sistema informativo. Tali provvedimenti sono resi noti agli *Utenti* dei servizi informatici comunali anche attraverso il sito intranet dell'*Amministrazione*.

4. Nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati nei file di log con riferimento all'esercizio o alla difesa di un diritto in sede

giudiziaria (azioni da parte di terzi verso l'*Amministrazione* o viceversa, o in caso di verifiche relative ad un presunto comportamento illecito), oppure si debba ottemperare all'obbligo di custodire o consegnare i dati per specifica richiesta dell'Autorità Giudiziaria, i periodi massimi di tempo per la loro conservazione stabiliti di provvedimenti del dirigente del servizio Sistema Informativo di cui al comma precedente verranno prolungati secondo le necessità del caso e nel pieno rispetto delle finalità esclusive sopra descritte;

5. Il contenuto dei dispositivi di memorizzazione, delle cartelle dei file server, delle caselle di posta elettronica sono soggetti a copie periodiche salvate su dispositivi anche rimovibili al fine di garantire il loro recupero in caso di perdita o disastro.

6. Stante la continua evoluzione della normativa in materia, le continue innovazioni tecnologiche ed il mutare delle esigenze di rispristino di perdite casuali o accidentali di dati, le modalità e le tempistiche con cui tali copie sono effettuate e conservate, nel rispetto della normativa vigente in tema di protezione dei dati personali, sono stabilite con provvedimenti del Dirigente del servizio Sistema Informativo.

7. I tempi di conservazione delle copie effettuate, stabiliti dai provvedimenti dei Dirigente del Servizio Sistema Informativo di cui al comma precedente, potranno variare anche in aumento per eventuali esplicite richieste delle Autorità competenti e/o in caso vi siano elementi che inducano l'*Amministrazione* stesso a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), ciò comunque previa eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Art. 38. Assistenza da remoto

1. Il personale incaricato dal servizio Sistema informativo ed i tecnici di fornitori esterni di servizi e prodotti informatici, esplicitamente autorizzati dal servizio Sistema Informativo all'assistenza e alla manutenzione hanno la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni *Utente* al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento è effettuato su chiamata dell'*Utente*.

2. Il personale dal servizio Sistema informativo incaricato può compiere, di propria iniziativa, interventi anche da remoto, con il solo fine di garantire la sicurezza e l'integrità del sistema informatico dell'*Amministrazione*, in caso di comprovata ed imminente minaccia, che possono comportare anche l'accesso ai dati trattati da ciascun *Utente*, ivi compresi gli archivi di posta elettronica, nonché procedere alla verifica sui siti internet acceduti dagli *Utenti* abilitati alla navigazione esterna. La facoltà si applica anche in caso di assenza prolungata od impedimento dell'*Utente*. Di tale attività, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, e posto che ciò sia possibile, è data preventiva comunicazione all'*Utente.* Al termine di tale attività sarà redatto apposito verbale e, ove possibile, sarà informato l'*Utente* interessato alla prima occasione utile.

3. Per impedire l'accesso illegittimo a dati personali presenti in cartelle o spazi di memoria assegnati agli *Utenti*, le attività di cui ai precedenti punti potranno essere condotte esclusivamente nei seguenti casi:

    a. se i sistemi di controllo remoto sono installati e configurati sulle postazioni *Utente* in modo da richiedere necessariamente all'*Utente* una cosciente e volontaria azione di abilitazione sul proprio computer a tale connessione;

    b. oppure se la connessione avviene in assenza di una sessione *Utente* aperta con applicativi in esecuzione.

4. L’abilitazione di cui al precedente punto a) dovrà essere obbligatoriamente temporanea e valere esclusivamente per il tempo strettamente necessario all'esecuzione dell'intervento e comunque fino alla disconnessione;

Art. 39. Norme per la gestione del servizio di “call center” telefonico

1. Nel caso di utilizzo della configurazione di tipo “call center” di cui all’Art. 9. Ultimi commi, i controlli effettuati sul servizio saranno tesi esclusivamente alla valutazione delle prestazioni complessive del servizio senza possibilità di poter effettuare statistiche riferite ai singoli operatori e/o alla loro specifica attività in modo che non possa configurarsi qualsiasi forma di controllo a distanza ai sensi del Art. 4 della L.300/1970

Art. 40. Norme per il risparmio energetico e la sostenibilità ambientale

1. Salvo che la postazione di lavoro non debba essere utilizzata da remoto per scopi lavorativi e non sia possibile successivamente procedere alla sua accensione in tempo utile per il suo utilizzo da remoto, la stessa postazione di lavoro deve essere sempre spenta prima di lasciare gli uffici o in caso di assenze prolungate dall’ufficio o in caso di suo inutilizzo.

2. E’ fatto divieto di disabilitare, in tutte le *Dotazioni*, le funzionalità di “stand-by” e/o di autospegnimento. L’operazione è consentita limitatamente all’unità centrale per i computer fissi ed esclusivamente nella stessa casistica di cui al punto precedente.

Art. 41. Ulteriori prescrizioni

1. La sicurezza dei sistemi informatici è soggetta a costante evoluzione dovuta al continuo mutare delle minacce informatiche, il che comporta l'adozione di contromisure, anche temporanee e/o urgenti, sempre nuove e specifiche al verificarsi minacce potenziali, attacchi effettivi o eventi particolari. A tal fine il servizio Sistema Informativo, al verificarsi della necessità di adozione urgente di ulteriori misure, rispetto a quanto stabilito dal presente Regolamento, provvederà ad informare gli *Utenti* tramite la intranet comunale e/o tramite anche altri canali ditali ulteriori misure.

Art. 42. Inosservanza del Regolamento

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

Art. 43. Pubblicità

2. Dell’approvazione del presente Regolamento viene data diffusione ai dipendenti tramite la intranet comunale e/o posta elettronica.

Art. 44. Disposizioni finali

Con l’approvazione del presente Regolamento viene abrogato l’analogo regolamento approvato con DGC 545/2008.

Il presente testo sostituisce, quello approvato con DGC 125/2021.