REGOLAMENTO
PER L'UTILIZZO DEI
SISTEMI INFORMATICI

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.
Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate al punto 15.
Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico dell'Ente.
I dati personali e le altre informazioni dei dipendenti/ collaboratori registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. 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 679/16 "General Data Protection Regulation".
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso ai dipendenti e collaboratori 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:

- in osservanza 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 parziale osservanza (in quanto non direttamente assoggettabile ad Informest) del D.lgs. 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale; ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- in parziale osservanza (in quanto non direttamente assoggettabile ad Informest) del DPR 16 aprile 2013, n. 62 - Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165;
- in osservanza 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»;
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- in parziale osservanza (in quanto non direttamente assoggettabile ad Informest) del DPR 13 giugno 2023, n. 81 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62;

in parziale osservanza delle Linee Guida emanate da AgID che delineano regole e standard per l'attuazione e il rispetto delle norme nell'ambito dell'agenda digitale.

La finalità è quella di promuovere in tutto il personale 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 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. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

a) **il principio di necessità,** secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del 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. È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

2.3. Il dipendente ed il collaboratore si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni 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 quando il dipendente/collaboratore si allontana dalla postazione di lavoro.
d) Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le eventuali /zone sale dedicate.

3. Tutela del lavoratore

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

3.2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 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 intrattenuto con lo stesso.

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 dall'Amministratore di Sistema, previa autorizzazione del dirigente responsabile. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Amministratore di Sistema.

5.2. Le credenziali di autenticazioni consistono in un codice per l'identificazione del dipendente/collaboratore (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla. Si consiglia l'uso di un software per la gestione delle password tra quelli messi a disposizione dell'Ente.

5.3. La password deve essere di almeno 12 caratteri, formata da lettere maiuscole e minuscole e/o numeri. Non deve contenere riferimenti agevolmente riconducibili al dipendente/collaboratore (username, nomi o date relative alla persona o ad un familiare).

5.4. È necessario procedere alla modifica della password a cura del dipendente/collaboratore al primo accesso e, successivamente, almeno ogni sei mesi.

5.5. Per esclusive finalità di sicurezza informatica, è possibile che venga chiesto al dipendente/collaboratore l'inserimento di un proprio dato di contatto per accedere a servizi o sistemi dell'Ente. Tale operazione, conosciuta anche come autenticazione multifattore, si rende opportuna specialmente in caso di tentativi di accesso anomali o nuovi servizi attivati dall'Ente.

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

6. Utilizzo infrastruttura di rete e FileSystem

6.1. Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun dipendente/collaboratore deve essere in possesso di credenziali di autenticazione secondo il punto 5.

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

6.3. Il dipendente/collaboratore ha la disponibilità di accedere a risorse remote nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Ciascun dipendente/collaboratore, poi, dispone di un'area riservata e personale. Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso

secondo le regole previste nel successivo punto 12 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 dell'Amministratore di Sistema e non sono oggetto di backup periodici

6.4. Con regolare periodicità ciascun dipendente/collaboratore provvede alla pulizia degli archivi, Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.5. All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata dall'Amministratore di Sistema.

6.6. L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

6.7. L'Ente mette a disposizione dei soli dipendenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 5.

I log relativi all'uso del File System e della intranet, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 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".

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 dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla

sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.2. L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e il dipendente/collaboratore è tenuto a conservarli nella massima segretezza. Si consiglia l'uso di un software per la gestione delle password tra quelli messi a disposizione dell'Ente.

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 all'Amministratore di Sistema ogni malfunzionamento e/o danneggiamento

7.4. Il Personal Computer in dotazione dev'essere sistematicamente spento a fine giornata lavorativa.

7.5. Non è consentito al dipendente/collaboratore modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.

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

7.7. La gestione dei dati su PC è demandata al dipendente/collaboratore che dovrà provvedere a memorizzare sulle condivisioni i dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

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

7.9. L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza dei PC, per la rete locale e server, nonché potrà cambiare tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici.

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

7.13. Non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

7.14. Nel caso in cui il dipendente/collaboratore dovesse notare comportamenti anomali del PC, il dipendente/collaboratore è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

7.15. Non è consentita l'installazione di software privi di regolare licenza, l'utente dovrà ottenere espressa autorizzazione dell'Ente per installare e/o utilizzare qualsiasi programma o software dotato di licenza non proprietaria.

7.16. Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.

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 12 del presente Regolamento e, al verificarsi di fattispecie violative, l'Ente può procedere con l'applicazione delle sanzioni di cui all'art. 14.
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 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.

8.1. È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa.

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

8.3. 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.

8.4. 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, potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.

8.5. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema~~,~~ nella quale siano indicati chiaramente: motivo della richiesta, dipendente/collaboratore e postazione da cui effettuare la navigazione libera, intervallo

di tempo richiesto per completare l'attività. Il dipendente/collaboratore, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 12.1 e 12.2 del presente regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.

8.6. 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 strettamente collegati all'operatività~~,~~ con il rispetto delle normali procedure di acquisto.

8.7. È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli account che vengono utilizzati per le attività di comunicazione di progetto e/o istituzionali), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8.8. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi. 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.

8.9. 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.

8.10. Non è consentito l'utilizzo di sistemi di social networking a fini personali sul luogo di lavoro o durante l'orario lavorativo.

8.11. È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'Ente.

8.12. Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole l'Ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Si informa che l'Ente, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo dipendente/collaboratore, 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 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 12 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".

9. Utilizzo della posta elettronica

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

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

9.2. Ad ogni dipendente/collaboratore viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@informest.it. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. Il dipendente/collaboratore a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

9.3. Ciascun dipendente/collaboratore periodicamente provvede all'archiviazione di tutti i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa. Come indicato nel riquadro più sotto, tutti i messaggi inseriti nella cartella di archiviazione saranno conservati dall'Ente per almeno dieci anni.

9.4. L'Ente fornisce, altresì, delle caselle di posta elettronica associate a determinate funzioni, ufficio o gruppo di lavoro

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

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

9.7. Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.8. 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 all'Amministratore di Sistema.

9.9. 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 obbligatorio 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 di tipo collettivo, tipo ufficio….@informest.it. rivolgersi all'Amministratore di Sistema per tale eventualità.

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

9.11. È vietato inviare messaggi di posta elettronica in nome e per conto di un altro dipendente/collaboratore, salvo sua espressa autorizzazione;

9.12. 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.

9.13. 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.

9.14. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può' in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

9.15. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

Si informa che, ai sensi dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, l'Ente deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa.
Si informa altresì che l'Ente, per il tramite dell'Amministratore di Sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio ~~le~~ ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite dell'Amministratore di Sistema può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà sospesa per un periodo di 15 giorni e successivamente disattivata.

Nel periodo di sospensione l'account rimarrà attivo solo in ricezione e, in caso di ricezione di messaggi, genererà una risposta automatica al mittente invitandolo a reinviare il messaggio ad altro indirizzo mail dell'Ente. Trascorso il periodo di sospensione, ad eccezione dei messaggi archiviati dal dipendente nell'apposita cartella che saranno conservati per dieci anni, tutto il contenuto della mailbox verrà cancellato.
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

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

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, sono di proprietà dell'Ente e sono resi disponibili al dipendente/collaboratore per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine.

10.1. Il telefono affidato al dipendente/collaboratore è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

10.2. Qualora venisse assegnato un cellulare al dipendente/collaboratore, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), 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 (cfr. 8), se consentita.

10.3. Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.

10.4. Al fine di controllo del corretto utilizzo dei servizi di fonia, l'Ente può esercitare i diritti di cui all'art. 124 D.Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo. I controlli saranno eseguiti secondo criteri e modalità descritte all'art. 12 del presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà

richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.

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

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

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

10.7. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate il dipendente/collaboratore dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

11. Assistenza agli utenti e manutenzioni

11.1. L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

a) verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
b) verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
c) richieste di aggiornamento software e manutenzione preventiva hardware e software.

11.2. Gli interventi tecnici posso avvenire previo consenso del dipendente/collaboratore, quando l'intervento stesso richiede l'accesso ad aree personali del dipendente/collaboratore stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso del dipendente/collaboratore cui la risorsa è assegnata.

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

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

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

12.1. Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, 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, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere eseguiti conformemente ai 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.

12.2. L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili del dipendete/collaboratore, 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, 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 al punto 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

12.3 Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli 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 il Responsabile interno del trattamento per il tramite dell'Amministratore di Sistema, 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 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
c) Qualora il rischio di compromissione del sistema informativo 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 interno del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.4 Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un dipendente/collaboratore (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 il Responsabile interno del trattamento, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

d) Redazione di un atto da parte del Direttore e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
e) 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 del dipendente/collaboratore interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
f) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
g) 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 Regulation".

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 interno del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.
In caso di nuovo accesso da parte del dipendente/collaboratore 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 Regulation".

13. Partecipazioni a Social Media

13.1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

13.2. 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, 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.

13.3. Il presente articolo deve essere osservato dal dipendente/collaboratore 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.

13.4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. Il dipendente/collaboratore, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

13.5. Il dipendente/collaboratore deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio.

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

13.7. L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Ente, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'Ente.

13.8. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo riconducibili all'Ente mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

13.9. L'Ente si può dotare di una "social media policy" per ciascuna tipologia di piattaforma digitale, al fine di adeguare alle proprie specificità le disposizioni di cui al presente articolo. In particolare, la "social media policy" deve individuare, graduandole in base al livello gerarchico e di responsabilità del dipendente, le condotte che possono danneggiare la reputazione delle amministrazioni.

13.10. Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'Ente e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità attribuibili direttamente alla pubblica amministrazione di appartenenza.

13.11. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Ente di appartenenza o della pubblica amministrazione in generale.

13.12. Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche.

14. Sanzioni disciplinari

14.1. La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

14.2. Nel caso venga commesso un illecito (di qualsivoglia genere e/o natura, anche penale) o la cui commissione sia ritenuta probabile o solo sospettata l'Ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità

competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

14.3. In caso di violazione delle regole e/o degli obblighi del presente Regolamento da parte del dipendente e di cui l'Ente sia venuto in qualsivoglia modo a conoscenza – anche a seguito dei controlli previsti e disciplinati dall'art. 12 che precede – l'Ente stesso avrà la facoltà i) di effettuare qualsiasi verifica tecnica, anche per il tramite di un esperto informatico all'uopo incaricato, ii) di sospendere e/o bloccare e/o limitare e/o impedire gli accessi dell'account riferibile al responsabile della violazione e/o, comunque, di adottare qualsiasi diversa iniziativa ogniqualvolta ciò apparirà ragionevolmente necessario per la tutela dei propri diritti e/o delle proprie prerogative e/o per la protezione dell'integrità, della sicurezza o della funzionalità dei propri beni e strumenti informatici, nonché per impedire la reiterazione della condotta illecita.

15. Disposizioni finali

15.1. Il presente Regolamento è stato redatto dal Dirigente responsabile con il supporto dell'Amministratore di Sistema che è chiamato a garantire il coordinamento degli adempimenti.

15.2. La sua pubblicizzazione avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i dipendenti/collaboratori, e a tutti gli impiegati provvisti di e-mail; attraverso la rete informatica interna, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, nella sezione Amministrazione Trasparente dedicata del sito istituzionale.