ALLEGATO A

Camera di commercio, industria, artigianato e agricoltura del Gran Sasso d'Italia

DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE INFORMATICA E TELEMATICA (INTERNET E POSTA ELETTRONICA) E DEL SISTEMA DI TELEFONIA FISSA E MOBILE

PREMESSA

1. La Camera di commercio, industria, artigianato e agricoltura del Gran Sasso d'Italia (di seguito "CCIAA del Gran Sasso", o "Ente") promuove ed incentiva l'utilizzo sempre più diffuso delle moderne tecnologie nell'ambito dello svolgimento dell'attività lavorativa, in quanto consente di perseguire con maggior efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa.
2. A tal fine la CCIAA del Gran Sasso mette a disposizione dei lavoratori un'idonea strumentazione informatica, favorisce l'utilizzo della Rete Informatica e Telematica, con particolare riferimento all'uso di internet, della posta elettronica e del Sistema di telefonia fissa e mobile e ne promuove un utilizzo corretto attraverso l'adozione del presente Disciplinare.

Sezione I

DISPOSIZIONI GENERALI

Art. 1

FINALITA'

1. Il presente Disciplinare è diretto a:

2. porre in essere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici, della Rete Informatica e Telematica e del Sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;

a) informare coloro che utilizzano per lavoro gli strumenti informatici, la Rete Informatica e Telematica e il Sistema di telefonia messi a disposizione dalla CCIAA del Gran Sasso delle misure adottate e che si intendono adottare al fine di:

- garantire il diritto alla riservatezza degli utenti interni ed esterni della Rete Informatica, Telematica e di Telefonia;
- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

Art. 2

PRINCIPI GENERALI

1. La CCIAA del Gran Sasso promuove il corretto utilizzo degli strumenti informatici, della Rete Informatica e Telematica, con particolare riferimento all'uso di internet, alla posta elettronica, e del sistema di telefonia quali strumenti utili a perseguire con efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa, nel rispetto dei principi e delle linee guida delineati dalla normativa vigente.

2. La titolarità dei beni e degli strumenti informatici, telematici e di telefonia è in capo alla CCIAA del Gran Sasso. Tali strumenti sono messi a disposizione del personale, degli addetti che operano in outsourcing e per coloro che per lo svolgimento dell'attività lavorativa in ambito camerale ne facciano espressa richiesta. La dotazione degli strumenti e delle risorse informatiche, telematiche e di telefonia non costituisce titolo per l'acquisizione di alcun diritto in capo ai predetti soggetti e può essere: ridotta, sospesa o eliminata qualora ne sussistano le motivazioni.

3. Ogni soggetto identificato al precedente punto 2, dopo aver ricevuto le relative istruzioni, è responsabile, sotto i profili amministrativi civili e penali, del corretto uso degli strumenti informatici, telematici e di telefonia e del contenuto delle comunicazioni effettuate. Risponde dei danni, anche all'immagine dell'Ente, che possono derivare da comportamenti illeciti.

4. Le precauzioni di tipo tecnico predisposte dall'azienda possono proteggere le informazioni durante il loro transito fra i sistemi della rete locale, anche quando queste rimangono inutilizzate su un disco di un computer, ma unicamente se presenti o duplicate su sistemi server; nel momento in cui esse raggiungono fisicamente la postazione dell'utente finale o sono memorizzate solo in essa, la loro protezione dipende esclusivamente da quest'ultimo.

5. La CCIAA del Gran Sasso privilegia l'attività di prevenzione rispetto a quella di controllo, indicando ed attuando, in un'ottica di reciproco affidamento, appropriate misure di tutela e promuovendo misure di autotutela da parte dei fruitori, nonché assicurando la massima diffusione al contenuto del presente Disciplinare.

6. Nello svolgimento dell'attività di monitoraggio e controllo la CCIAA del Gran Sasso agisce nel rispetto della normativa vigente, con particolare riguardo alla tutela dei diritti dei lavoratori e alle garanzie in materia di protezione dei dati personali, nell'osservanza dei principi di ragionevolezza, correttezza, trasparenza e proporzionalità.

Art. 3

DESTINATARI

1. Il presente Disciplinare si applica ai dirigenti, ai dipendenti, o a questi assimilati, ed in genere a tutti gli autorizzati ad accedere alla rete camerale e agli strumenti informatici, telematici e di telefonia (d'ora innanzi più brevemente denominati "personale", "dipendenti" e/o "utenti") per lo svolgimento della propria attività lavorativa.

2. Sono escluse, al fine di preservare il libero esercizio delle funzioni politiche e sindacali, le strumentazioni individuali messe a disposizione degli Organi Camerali, nonché l'apposita strumentazione messa a disposizione della RSU.

3. Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli incaricati in materia di trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003.

4. Il mancato rispetto delle regole e dei divieti di cui al presente Disciplinare costituisce, per i dipendenti, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo di Lavoro vigente, fatto salvo comunque il diritto della CCIAA del Gran Sasso al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore. Il

mancato rispetto delle regole e dei divieti del presente Disciplinare costituisce, per i collaboratori esterni, violazione degli obblighi contrattuali.

5. Al presente Disciplinare verrà data la massima pubblicità, sia telematica sia anche mediante affissione in ogni posto di lavoro, in luogo accessibile a tutti i dipendenti e collaboratori esterni, nonché con l'adeguata formazione anche in relazione alla tutela dei dati personali.

Sezione II

USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4

CRITERI GENERALI DI UTILIZZO

1. Gli strumenti informatici (a titolo esemplificativo personal computer, stampanti, ecc.), telematici (a titolo esemplificativo accesso ad internet, tramite collegamento fisso o mobile, la posta elettronica), telefonici (a titolo esemplificativo telefono fisso, mobile, cellulare), messi a disposizione, costituiscono strumento di lavoro.

2. Pertanto, l'utilizzo di essi è consentito, di regola, per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative ed interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.

3. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro. E' escluso qualsivoglia uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.

4. L'utilizzo di tali strumenti messi a disposizione non configura alcuna titolarità, da parte del lavoratore, dei dati e delle informazioni trattate, che appartengono alla CCIAA del Gran Sasso ed ai quali l'Ente si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali.

5. Il personale deve custodire e utilizzare gli strumenti affidatigli in modo appropriato, con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza del sistema. Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente disciplinare e tale configurazione non deve essere modificata senza la preventiva necessaria autorizzazione dell'Amministratore di sistema o di chi ne abbia la competenza. Il personale è altresì tenuto ad informare direttamente il proprio dirigente/funzionario o il responsabile da questi delegato, nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli strumenti e/o del sistema.

Art. 5

UTILIZZO DEGLI STRUMENTI INFORMATICI

1. L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password).

   a) Le credenziali di autenticazione per l'accesso alle risorse informatiche (Rete Lan e PC) vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Dirigente o dal Responsabile dell'Ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei 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.

   b) Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password iniziale. La password è personale e riservata e dovrà essere conservata e custodita dall'utente con la massima diligenza senza divulgarla.

   c) La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole, minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).

   d) È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni quattro mesi.

   e) 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 della cessazione, a partire dalla quale le credenziali saranno disabilitate.

2. E' vietato:

   a) installare sulla stazione di lavoro software, anche se gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla CCIAA del Gran Sasso;

   b) collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente o autorizzati espressamente dall'Amministratore di sistema (ad esempio, ma non limitatamente a: chiavette USB, hard disk portatili, smartphone, fotocamere, webcam, stampanti);

   c) svolgere l'attività lavorativa con strumentazione personale (PC fissi, portatili, tablet, smartphone) connessi alla rete aziendale, senza espressa autorizzazione dell'Amministratore di sistema e previa verifica della sussistenza di misure minime ed idonee di sicurezza (es. Antivirus e/o software aggiornato e compatibile);

   d) lasciare incustodita la postazione di lavoro, anche per brevi periodi, senza bloccarla (mediante Ctrl+Alt+Canc);

   e) alterare, disattivare o modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro software installato sulle attrezzature e sugli strumenti, fissi e mobili (postazione di lavoro, notebook, tablet, cellulari, altri supporti, ecc.), forniti in dotazione al personale. Inoltre, l'incaricato/l'utente ha il dovere di usare e gestire le attrezzature e gli strumenti ricevuti in

dotazione con attenzione e diligenza, nonché quello di segnalare tempestivamente all'Amministratore di sistema ogni anomalia o disfunzione al fine di ripristinare il corretto funzionamento degli stessi;

f) accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate nel Disciplinare che limitino l'accesso alle stazioni di lavoro stesse;

g) caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;

h) in ogni caso, caricare, detenere e/o stampare materiale informatico:

- il cui contenuto (a mero titolo esemplificativo: testo, audio, video) sia chiaramente tutelato da diritto d'autore. Nel caso in cui ciò sia necessario per la propria attività lavorativa, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
- il cui contenuto sia contrario a norme di legge.

3. Le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati dalla CCIAA del Gran Sasso. Il personale non è autorizzato a modificare il sistema neppure se si tratta della postazione di lavoro assegnata.

4. A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:

a) modificare i collegamenti di rete esistenti;

b) usare dispositivi removibili (CD, dvd, hard disk, floppy etc.) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dalla CCIAA del Gran Sasso;

c) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;

d) installare, senza l'assistenza dell'Amministratore di sistema o di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.

5. Le cartelle [uffici] presenti nei server della CCIAA del Gran Sasso sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi, quali a titolo esemplificativo il salvataggio di **file privati** (documenti, fotografie, video, musica, pratiche, sms, mail , film e quant'altro). Allo stesso modo, le cartelle [utenti] presenti nei server della CCIAA del Gran Sasso sono aree di memorizzazione e conservazione esclusiva dei documenti di lavoro del singolo utente e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su tali unità vengono svolte regolari attività di verifica, amministrazione e back-up da parte dell'Amministratore di sistema o da personale incaricato.

6. 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. A titolo di esempio e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o chiavette USB ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di lavoro o di interesse, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

7. È vietata l'estrazione di originali e/o copie cartacee ed informatiche, per uso personale, di materiale di lavoro come documenti, manuali, fascicoli, lettere, data base, mail e quant'altro.

8. L’Amministratore di sistema e il personale incaricato può in qualsiasi momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza sia sulle stazioni di lavoro sia sui server di rete.

9. 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.

10. Con regolare periodicità, ciascun utente deve provvedere alla pulizia degli archivi di rete, con cancellazione dei file obsoleti o inutili o duplicati.

11. Ciascun dipendente può delegare per iscritto un altro lavoratore a accedere a dati e procedure del proprio personal computer nel caso in cui, durante la propria assenza, ciò si renda indispensabile ed indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa. A tale scopo, prima dell’assenza, il dipendente dovrà consegnare al lavoratore da lui delegato una busta chiusa contenente le proprie credenziali di accesso.

12. Il lavoratore delegato accede ai dati e alle procedure su richiesta del dirigente o del responsabile dell’area. Dell'attività compiuta è redatto apposito verbale, firmato dal dipendente delegato e dal dirigente/responsabile, che verrà consegnato al dipendente assente alla prima occasione utile. Nel caso in cui non sia autorizzato o presente il lavoratore delegato, il dirigente di settore/ responsabile dell’area accederà ai dati mediante assistenza dell’Amministratore di sistema. Di tale attività è redatto apposito verbale a cura del dirigente/responsabile, consegnato all'utente alla prima occasione utile.

Art. 6

UTILIZZO DELLA RETE INTERNET

1. L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito, di regola, per finalità direttamente attinenti o comunque connesse all'esercizio dell’attività lavorativa. E’ escluso qualsivoglia uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. E’ in ogni caso vietato l’uso reiterato e prolungato per fini personali.

2. Le credenziali di autenticazione per l’accesso alla rete internet (e di posta elettronica) vengono assegnate dal fornitore dei servizi Infocamere, per il tramite dell’Amministratore di sistema e previa formale richiesta del Responsabile dell’ufficio/area nell’ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Dirigente o dal Responsabile dell’Ufficio/area con il quale il collaboratore si coordina nell’espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell’utente ed elenco dei 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.

3. Al primo accesso, la password dell'account internet/posta elettronica deve essere cambiata ed è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole indicati dal fornitore del servizio Infocamere.

4. E' vietato entrare nella rete e nei programmi Infocamere con un codice di identificazione diverso da quello assegnato, utilizzando credenziali di altre persone. Le credenziali di accesso alla rete ed ai programmi sono segrete e dovranno essere conservate e custodite dall’utente con la massima diligenza senza divulgarle.

5. E’, altresì, vietato:

   a) scaricare e/o installare software non espressamente autorizzati dalla CCIAA del Gran Sasso;

   b) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio della attività

lavorativa;

c) scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia chiaramente tutelato dal diritto di autore;

d) partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;

e) navigare in internet su siti contrari a norme di legge;

f) effettuare ogni genere di transazione finanziaria per fini personali;

g) installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia *Peer to Peer* (es. eMule, bittorrent etc.) indipendentemente dal contenuto dei file scambiati.

6. In un'ottica preventiva, la CCIAA del Gran Sasso, per il tramite di Infocamere, ha già provveduto a predisporre un sistema informatico di filtraggio teso ad impedire la navigazione su siti web contrari a norme di legge, o considerati non sicuri. Tuttavia, la CCIAA del Gran Sasso si riserva di disporre ed effettuare controlli, anche tramite l'esame delle registrazioni degli accessi (file di log) relativi al traffico web a livello di Ente, finalizzati al rispetto del presente Disciplinare.

Art. 7

UTILIZZO DELLA POSTA ELETTRONICA

1. La CCIAA del Gran Sasso mette a disposizione di ogni lavoratore il servizio di posta elettronica Google Mail, assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi, nel formato standard *nome.cognome@gransasso.camcom.it* .
2. Al fine di agevolare lo svolgimento dell'attività lavorativa, specie nei rapporti con l'utenza, la CCIAA del Gran Sasso rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative o gruppi di lavoro) affiancandoli a quelli individuali.
3. L'indirizzo di posta elettronica messa a disposizione dalla CCIAA del Gran Sasso, contraddistinto dalla presenza del nome di dominio "gransasso.camcom.it", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.
4. E' escluso, di regola, l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.
5. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa.
6. Al fine della sicurezza e di un corretto utilizzo e della posta elettronica è vietato:

   a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno alla CCIAA del Gran Sasso o a terzi nonché messaggi a catena S.Antonio e/o spam. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo;

   b) scambiare messaggi impersonando un mittente diverso da quello reale;

   c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;

   d) aprire messaggi di posta in arrivo da mittenti di cui non sia certa l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js, *.pif, *.rar e *.zip. 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.

7. In caso di assenze programmate dal lavoro, per ferie o per qualsiasi altro motivo di assenza prolungata, è buona norma attivare preventivamente il sistema di risposta automatica. Il messaggio di risposta predefinito deve essere personalizzato dal personale e potrà indicare l'indirizzo di posta elettronica di un altro lavoratore al quale il mittente può fare riferimento in caso di comunicazioni urgenti.

8. In caso di assenze dal lavoro non programmate, il dipendente può attivare da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica;

9. E' consentito accedere alla posta elettronica mediante app installata sullo smartphone personale o da PC remoti;

10. Il lavoratore può delegare per iscritto un altro lavoratore a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al dirigente/funzionario di settore o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa nel caso in cui, durante la propria assenza, ciò si renda indispensabile e indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa. Il lavoratore delegato provvede su richiesta del dirigente/responsabile di area. Di tale attività è redatto apposito verbale consegnato al lavoratore alla prima occasione utile.

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 né sistematicamente né saltuariamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica e/o saltuaria dei messaggi di posta elettronica.
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 ovvero per motivi di sicurezza del sistema informatico, l'Ente, per il tramite dell'Amministratore di Sistema, può chiedere al fornitore del servizio Infocamere l'accesso 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 disattivata.

Art. 8

UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE

1. Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dalla CCIAA del Gran Sasso costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.

2. E' escluso, di regola, l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. E' in ogni caso vietato l'uso reiterato e prolungato per fini personali.

Art. 9

PARTECIPAZIONE A SOCIAL MEDIA

1. L'utilizzo a fini divulgativi, promozionali e di assistenza di Facebook, Twitter, Linkedin, Instagram, dei blog e dei forum, anche professionali, e di altri siti o social media in nome e per conto della CCIAA del Gran Sasso **è riservato esclusivamente all'Ente**; tale servizio sarà gestito ed organizzato attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente assegnato. Sono escluse ogni tipo di iniziative individuali da parte dei singoli dipendenti o collaboratori.

2. Fermo restando il diritto della persona alla libertà di espressione, è vietata la partecipazione assidua e/o continuativa agli stessi social media durante l'orario di lavoro.

3. I dipendenti, in merito alla condivisione di contenuti nei social media, dovranno 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. I dipendenti, nelle proprie comunicazioni personali, non potranno 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 del Segretario Generale.

4. Il dipendente 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 ed utenti, 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 degli interessati e con espressa autorizzazione del Segretario Generale.

5. Qualora l'utente 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, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

Art. 10

ASSISTENZA AGLI UTENTI E MANUTENZIONE

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

   – verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.

   – verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.

   – richieste di aggiornamento software e manutenzione preventiva hardware e software.

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

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. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente 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.

Sezione III

CONTROLLI

Art. 11

MODALITA' DI EFFETTUAZIONE DEI CONTROLLI

1. la CCIAA del Gran Sasso si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli saltuari e a campione che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici e di telefonia alle presenti prescrizioni.
2. I controlli sono effettuati periodicamente dall'Amministratore di sistema o su richiesta del Segretario Generale o dei Dirigenti responsabili d'Area.
3. I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici.
4. A seguito di detto controllo anonimo, laddove fosse rilevata una effettiva e grave anomalia dell'attività, potrà essere emesso un avviso generalizzato, con l'invito ad attenersi esclusivamente e scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Se a detta comunicazione non dovessero seguire, nei quindici giorni successivi, ulteriori anomalie, l'Ente non procederà a ulteriori controlli. In caso contrario, verranno inoltrati preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.
5. Qualora continuino i comportamenti non conformi, saranno effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni indicate in precedenza.
6. In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.
7. L'Ente inoltre non effettuerà, in nessun caso, né farà effettuare da eventuali Responsabili esterni, trattamenti di dati personali mediante sistemi *hardware* e/o *software* che mirino al controllo a distanza dei lavoratori, ovvero a ricostruire l'attività del lavoratore, quali a titolo esemplificativo e non esaustivo:

    a) lettura e/o registrazione sistematica dei messaggi di posta elettronica, ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio di posta elettronica stesso;
    b) riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore, dei contenuti delle medesime, nonché del tempo di permanenza sulle stesse;
    c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
    d) analisi occulta di computer o altri dispositivi portatili affidati in uso, ovvero delle rispettive connessioni ad Internet;
    e) le attività descritte, ed altre per i medesimi scopi, effettuate sulle utenze telefoniche fisse o relative a telefonia cellulare.

    Resta sempre salvo l'obbligo dell'Ente di comunicare i *log file* o altre evidenze contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta secondo la normativa vigente.

Art. 12

EVENTUALI CONTROLLI SUI VEICOLI

1. Per i veicoli forniti ai dipendenti quando funzionali allo svolgimento delle attività, la CCIAA del Gran Sasso esclude l'utilizzo di sistemi di rilevazione della posizione dei veicoli stessi attraverso dispositivi basati su tecnologie GPS o altre con le medesime finalità.
2. L'eventuale collocazione ed utilizzazione dei dispositivi di cui al comma precedente è ammessa, previa specificazione delle esigenze che le giustificano, con la procedura di cui all'art. 4, comma 1, della legge n. 300/1970. Il trattamento dei dati personali è effettuato nel pieno rispetto di quanto previsto dal GDPR, con particolare riferimento ai principi di necessità, pertinenza, non eccedenza e minimizzazione.

Sezione IV

DISPOSIZIONI FINALI

Art. 13

INFORMATIVA

1. Il contenuto del presente disciplinare integra l'informativa già fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 [e 14] del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003.

Art. 14

DISPOSIZIONI FINALI

1. Il presente Disciplinare entra in vigore dal 1/03/2021 e sostituisce ed abroga eventuali procedure o disposizioni con esso incompatibili.
2. Copia del Disciplinare è affisso nelle bacheche istituzionali e messo a disposizione con invio mail attraverso la posta elettronica interna.