



**ALL. B**

Del. PromoImpresa-Borsa Merci n° 41 del 13 dicembre 2019

**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 di Mantova (di seguito “CCIAA di Mantova”, 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 di Mantova 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.
3. La CCIAA di Mantova, al fine di incrementare il livello di sicurezza e semplificare la gestione degli strumenti informatici, ha adottato la tecnologia Virtual Desktop Infrastructure (VDI) che consente di avere postazioni di lavoro sempre performanti e configurate in modo idoneo alle sole attività lavorative. Al desktop virtuale si accede, con user-id e password, attraverso il pc fisico. (NON APPLICABILE A PROMOIMPRESA-BORSA MERCI)

**Sezione I**

**DISPOSIZIONI GENERALI**

**Art. 1**

**FINALITA'**

1. Il presente Disciplinare è diretto a:
  - a) porre in essere, unitamente al Disciplinare Tecnico in materia di Misure di Sicurezza, 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;
  - b) informare coloro che utilizzano per lavoro gli strumenti informatici, la Rete Informatica e Telematica e il Sistema di telefonia messi a disposizione dalla CCIAA di Mantova 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 di Mantova 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 di Mantova. Tali strumenti sono messi a disposizione del personale, degli addetti che operano in outsourcing e di 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. La CCIAA di Mantova 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.
5. Nello svolgimento dell'attività di monitoraggio e controllo la CCIAA di Mantova 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") per lo svolgimento della propria attività lavorativa.
2. Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli autorizzati in materia di trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003.
3. Al presente Disciplinare verrà data la massima pubblicità, mediante invio tramite PEC a tutti i dipendenti e collaboratori esterni, nonché nell'ambito della formazione obbligatoria in materia di tutela dei dati personali.
4. Per tutto quanto non espressamente contenuto nel presente Disciplinare si rinvia al Disciplinare Tecnico in materia di Misure di Sicurezza.

## **Sezione II**

### **USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA**

#### **Art. 4**

##### **CRITERI GENERALI DI UTILIZZO**

1. Gli strumenti informatici (personal computer, stampanti, ecc.), telematici (accesso ad internet, tramite collegamento fisso o mobile, posta elettronica, ecc.) e telefonici (telefono fisso, mobile, cellulare, ecc.), messi a disposizione dei dipendenti, 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 di Mantova 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 l'Ufficio Provveditorato e il dirigente d'area (o il responsabile da questi delegato), nell'ipotesi di furto, smarrimento, 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). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia al successivo art. 8.
2. Ogni utente abilitato all'accesso è tenuto ad utilizzare il sistema VDI per lo svolgimento delle proprie attività lavorative in quanto: **NON APPLICABILE A PROMOIMPRESA-BORSA MERCI**
  - il sistema VDI permette all'utente di avere un ambiente sempre configurato in modo idoneo alle esigenze lavorative;
  - tutti i dati contenuti all'interno del VDI sono sempre disponibili anche accedendo da postazioni diverse, utilizzando le proprie credenziali, e sono salvati su server dedicati che ne permettono il loro eventuale recupero;
  - il sistema VDI permette inoltre il ripristino quasi immediato della postazione di lavoro qualora ci fossero problemi sulla macchina fisica.

3. E' vietato:
  - a) installare sulla stazione di lavoro software, anche se gratuiti e/o in versione demo (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla CCIAA di Mantova e collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente;
  - b) 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 al tecnico informatico e al dirigente di area ogni anomalia o disfunzione al fine di ripristinare il corretto funzionamento degli stessi;
  - c) accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate nel Disciplinare in materia di Misure di Sicurezza che limitino l'accesso alle stazioni di lavoro stesse;
  - d) caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, in particolare quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;
  - e) in ogni caso, caricare, detenere e/o stampare materiale informatico (a mero titolo esemplificativo: testo, audio, video):
    - il cui contenuto 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.
4. Le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati dalla CCIAA di Mantova. Il personale non è autorizzato a modificare il sistema neppure se si tratta della postazione di lavoro assegnata.
5. 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, chiavette usb, 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 di Mantova;
  - c) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
  - d) installare, senza l'assistenza di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.
6. Le cartelle presenti nel server della CCIAA di Mantova sono aree di condivisione di informazioni strettamente professionali 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 questa unità. Su tale unità vengono svolte

regolari attività di verifica, amministrazione e back up da parte del tecnico informatico camerale e da Infocamere.

7. Il personale incaricato può in qualsiasi momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza, ovvero acquisiti o installati in violazione del presente Disciplinare, sia sulle stazioni di lavoro sia sui server di rete.
8. Al fine di garantire la corretta effettuazione delle attività di backup e conseguentemente la possibilità di ripristinare i files in caso di distruzione accidentale per guasti hardware o cancellazioni involontarie, i dipendenti devono salvare i files nelle cartelle (individuali o condivise) presenti sul server e non sulla macchina fisica.
9. Il backup dei dati e documenti eventualmente presenti esclusivamente sul PC è effettuato a cura dell'interessato che è responsabile sia della regolare periodicità dei salvataggi (almeno una volta alla settimana) sia della verifica che i supporti informatici utilizzati per il backup siano funzionali e non corrotti.
10. Con regolare periodicità, secondo le indicazioni fornite dal tecnico informatico, ciascun utente deve provvedere alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.

#### **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. E' vietato entrare nella rete e nei programmi con un codice di identificazione diverso da quello assegnato. Le credenziali di accesso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni impartite nel successivo articolo 8.
3. E', altresì, vietato:
  - a) scaricare e/o installare software non espressamente autorizzati dalla CCIAA di Mantova;
  - b) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa;
  - c) scaricare e/o usare materiale informatico (a mero titolo esemplificativo: software, testo, audio e video) il cui contenuto 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, anche utilizzando pseudonimi o nickname;
  - 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, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati;
  - h) accedere tramite gli strumenti camerale alle caselle di posta elettronica personali esterne.

4. In un'ottica preventiva la CCIAA di Mantova 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 di Mantova si riserva di disporre ed effettuare controlli relativi al traffico web, finalizzati al rispetto del presente Disciplinare, con le modalità di cui al successivo art. 10.

#### **Art. 7**

#### **UTILIZZO DELLA POSTA ELETTRONICA**

1. La CCIAA di Mantova mette a disposizione di ogni lavoratore il servizio di posta elettronica, assegnando a ciascuno una casella di posta individuale per fini esclusivamente lavorativi.
2. Al fine di agevolare lo svolgimento dell'attività lavorativa, la CCIAA di Mantova rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.
3. L'indirizzo di posta elettronica messa a disposizione dalla CCIAA di Mantova, contraddistinto dalla presenza del nome di dominio "mn.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 CCIAA di Mantova mette inoltre a disposizione di ogni dipendente una casella PEC individuale che deve essere utilizzata esclusivamente per le comunicazioni ufficiali da e verso l'Amministrazione. E' vietato utilizzare la casella PEC individuale per inviare mail all'esterno dell'Ente. L'indirizzo della casella PEC individuale può essere comunicato all'esterno esclusivamente per ragioni di servizio, previa presentazione di richiesta scritta debitamente motivata al Dirigente d'area e solo dopo aver ottenuto espressa autorizzazione.
6. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'incaricato nel rispetto dei criteri e delle regole indicati all'art. 8.
7. Al fine di un corretto utilizzo 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 di Mantova o a terzi nonché messaggi a catena e/o spam;
  - 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 o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio.
8. I dipendenti sono inoltre tenuti ad attenersi scrupolosamente alle istruzioni in materia di sicurezza inviate periodicamente da Infocamere e/o dal tecnico informatico.
9. In caso di assenze programmate dal lavoro, per ferie o per qualsiasi altro motivo di assenza prolungata, deve essere attivato 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.

10. In caso di assenze dal lavoro non programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica.

### Art. 8

#### GESTIONE DELLE CREDENZIALI DI ACCESSO

1. L'accesso al PC, agli applicativi Infocamere e alla posta elettronica è protetto da un sistema di autenticazione che richiede l'inserimento di un codice utente (username o user-id) e di una parola chiave (password). La corretta gestione delle credenziali di accesso è fondamentale in quanto:
  - tutela l'utilizzatore, ed in generale l'Ente, da accessi illeciti, violazioni e danneggiamenti del proprio patrimonio informativo;
  - tutela il dipendente da false imputazioni, garantendo che nessuno possa operare a suo nome.
2. Per la scelta delle password devono essere rispettate le seguenti regole:
  - a) Utilizzare almeno **8 caratteri** (la lunghezza ideale è di almeno 10-12 caratteri);
  - b) Utilizzare una combinazione di numeri, lettere minuscole e maiuscole, caratteri speciali quali **\$ % & ( @ # \$ = ) , ; - \_ + ^**
  - c) Non utilizzare parole che consentono di identificare facilmente l'utente, quali ad esempio: il nome o cognome proprio, del coniuge o dei figli, le date di compleanno o altre informazioni similari;
  - d) Non utilizzare parole ovvie, quali ad esempio: password, pippo, pluto, 123456, ecc.;
  - e) Cercare di non utilizzare parole reali o, eventualmente, sostituire le lettere con il loro corrispondente numerico o carattere speciale;
  - f) Evitare di utilizzare la medesima password per l'accesso al pc, ai vari applicativi e alla posta elettronica;
  - g) In sede di cambio della password, non scegliere una password già utilizzata in precedenza.
3. Per la corretta gestione delle credenziali di accesso è inoltre necessario rispettare le seguenti regole:
  - h) Cambiare regolarmente le password: la password per l'accesso ai programmi Infocamere e alla casella di posta elettronica deve essere obbligatoriamente cambiata almeno ogni **6 mesi** e deve rispettare i criteri che vengono visualizzati durante la procedura guidata; le password per l'accesso a programmi o banche dati contenenti dati personali particolari e/o giudiziari devono essere cambiate almeno ogni **3 mesi**;
  - i) Cambiare sempre al primo utilizzo la password di primo accesso quando fornita;
  - j) Non rivelare o condividere le password con colleghi di lavoro, famigliari o amici; in caso di interventi tecnici che richiedano l'accesso attraverso gli strumenti elettronici in dotazione ai dipendenti, la password deve essere digitata dal dipendente stesso;
  - k) Se si tiene traccia scritta delle proprie password, queste devono essere conservate in luogo sicuro e lontano da occhi indiscreti;



- l) Non utilizzare la funzione, offerta da alcuni software, che consente di salvare automaticamente la password per i successivi utilizzi dell'applicazione.
4. In caso di smarrimento o blocco della password per l'accesso ai programmi Infocamere è necessario rivolgersi al referente informatico o al suo sostituto in quanto abilitati ad effettuare le operazioni di reset.

#### **Art. 9**

#### **UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE**

1. Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dalla CCIAA di Mantova 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.
3. I dipendenti sono responsabili del corretto utilizzo del telefono fisso loro assegnato. Al fine di evitarne l'uso improprio da parte di terzi non autorizzati, è possibile inserire un codice di "blocco tastiera" facendone espressa richiesta all'Ufficio Provveditorato.
4. I dipendenti assegnatari di un telefono cellulare sono responsabili della custodia dello stesso dal momento dell'assegnazione e fino alla restituzione. In caso di furto o di smarrimento dell'apparecchio, l'assegnatario dovrà darne immediata comunicazione all'Ufficio Provveditorato ai fini dell'immediato blocco dell'utenza e presentare formale denuncia di furto o smarrimento da far pervenire in copia all'Ufficio Provveditorato per gli adempimenti di competenza. NON APPLICABILE A PROMOIMPRESA-BORSA MERCI

#### **Sezione III**

#### **CONTROLLI E SANZIONI**

#### **Art. 10**

#### **MODALITA' DI EFFETTUAZIONE DEI CONTROLLI**

1. La CCIAA di Mantova 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 da Infocamere su richiesta del Segretario Generale o del Dirigente 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, verrà 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, sono effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni di cui al successivo articolo 11.
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.
8. 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. 11 SANZIONI**

1. E' fatto obbligo a tutti i dipendenti e collaboratori della Camera di commercio di Mantova di osservare le disposizioni del presente Disciplinare.
2. 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 di Mantova 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.

#### **Art. 12 DISPOSIZIONI FINALI**

1. Il presente Disciplinare entra in vigore dal 1° dicembre 2019 e sostituisce ed abroga eventuali procedure o disposizioni con esso incompatibili.