

**REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI AZIENDALI DA PARTE DEI DIPENDENTI  
DI METRO BRESCIA SOCIETÀ A RESPONSABILITÀ LIMITATA**

Approvato dal Consiglio di Amministrazione di Metro Brescia Società a Responsabilità Limitata nella seduta del 02.09.2016.

## ARTICOLO 1 - PREMESSE

- 1.1. Il presente “*Regolamento sull’utilizzo degli strumenti aziendali da parte dei dipendenti di Metro Brescia Società a Responsabilità Limitata*” (d’ora in poi “**Regolamento**”) è adottato da Metro Brescia Società a Responsabilità Limitata (d’ora in poi, “**Metro Brescia**” e/o “**Società**”), avente sede legale in Brescia, Via Leonida Magnolini, 3, (C.A.P. 25135), Tel. +39 030.2358966, Fax +39 030.2358536, E-mail: segreteria@metrobrescia.eu, posta elettronica certificata (PEC): metrobrescia@legalmail.it. La Società fa parte del Gruppo Brescia Mobilità (d’ora in poi, “**Gruppo**”), di cui Brescia Mobilità S.p.A. è la capogruppo (“**Capogruppo**”), con la quale la Società medesima ha stipulato un contratto di servizio.
- 1.2. Il Regolamento si applica a tutti i dipendenti con rapporto di lavoro a tempo indeterminato o determinato della Società (d’ora in poi, “**Dipendente/i**” e/o “**Utente/i**” e/o “**Personale**”).
- 1.3. Il Regolamento ha l’obiettivo di definire l’ambito di applicazione, le modalità e le norme sull’utilizzo degli strumenti aziendali da parte dei Dipendenti [postazione di lavoro e *Personal Computer* (d’ora in poi, “**PC**”), rete e navigazione Internet, posta elettronica, *badge* aziendale, stampanti, *plotter*, *fax* e fotocopiatrici, telefoni fissi, telefoni cellulari aziendali, autoveicoli aziendali], al fine di evitare condotte inconsapevoli e/o scorrette e/o illecite che possano esporre la Società a problematiche di sicurezza, di immagine e/o patrimoniali per eventuali danni cagionati a soggetti terzi, nonché a responsabilità della medesima e del Dipendente, sotto ogni profilo giuridicamente rilevante; l’insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare il comportamento dei Dipendenti ai principi di diligenza, di informazione e di correttezza nell’utilizzo degli strumenti aziendali; ciò, anche secondo quanto prescritto dal Piano Triennale di Prevenzione della Corruzione Gruppo Brescia Mobilità e dai successivi aggiornamenti, dal Codice Etico e Comportamentale (“**Codice Etico**”) e dal Modello di Organizzazione e di Gestione adottato dalla Società, ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 e ss.mm.ii. (“*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’articolo 11 della legge 29 settembre 2000, n. 300*”) (d’ora in poi, “**D.Lgs. 231/2001**”).
- 1.4. Il Regolamento è redatto nel rispetto dei Contratti Collettivi Nazionali di Lavoro applicabili ai Dipendenti (d’ora in poi, sia al singolare sia al plurale, “**C.C.N.L.**”), della normativa e della disciplina, pubblica e privata, vigente ed applicabile in materia, ed, in particolare, tra questa, della Legge 20 maggio 1970, n. 300 e ss.mm.ii. (“*Norme sulla*

tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento”) (d’ora in poi, “**Statuto dei Lavoratori**”), del Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. (“*Codice in materia di protezione dei dati personali*”) (d’ora in poi, “**D.Lgs. 196/2003**”), degli atti appositamente emanati dal Garante per la Protezione dei Dati Personali (d’ora in poi, “**Garante**”) e, nell’ambito di questi, in particolare, della Delibera 1.03.2007, n. 13 (Gazzetta Ufficiale del 10.03.2007, n. 58) (d’ora in poi, “**Delibera 13/2007**”), denominata “*Lavoro: le linee guida del Garante per posta elettronica e internet*”.

- 1.5.** Il Regolamento fa salva, per ciascun Dipendente, l’osservanza, tra l’altro, del Codice Etico e del Modello di Organizzazione e di Gestione della Società adottato ai sensi del D.Lgs. 231/2001, nonché del Piano Triennale di Prevenzione della Corruzione delle società del Gruppo Brescia Mobilità e dei successivi aggiornamenti, di tutte le Disposizioni di Servizio (d’ora in poi, “**DDS**”) e Comunicazioni di Servizio (d’ora in poi “**CDS**”) vigenti e/o che verranno adottati dalla Società nonché di ogni ulteriore prescrizione aziendale anche futura all’adozione del Regolamento.

## **ARTICOLO 2 – OBBLIGHI GENERALI DEL DIPENDENTE**

- 2.1.** Il Dipendente conforma la sua condotta, anche nell’utilizzo degli strumenti aziendali, al dovere di diligenza e di correttezza nonché all’obbligo di fedeltà di cui agli articoli 2104 (“*Diligenza del prestatore di lavoro*”) e 2105 (“*Obbligo di fedeltà*”) del Codice Civile<sup>1</sup>, atteggiamenti, questi, destinati a sorreggere ogni atto o comportamento posto in essere nell’ambito del rapporto di lavoro.
- 2.2.** Il Dipendente è personalmente responsabile, sotto ogni profilo giuridicamente rilevante, dell’utilizzo degli strumenti aziendali affidatigli dalla Società per lo svolgimento della propria mansione nonché dei relativi dati trattati per finalità aziendali. A tal fine, ogni Dipendente, nel rispetto degli obblighi di diligenza richiamati al precedente comma 2.1., è tenuto a tutelare, per quanto di propria competenza, gli strumenti aziendali in suo possesso da utilizzi impropri o non autorizzati, danni e/o abusi anche derivanti da negligenza, imprudenza o imperizia, con l’obiettivo di preservare l’integrità degli strumenti stessi e delle risorse aziendali nonché la riservatezza delle informazioni.
- 2.3.** In tale contesto, il Dipendente, a titolo esemplificativo e non esaustivo, deve:

---

<sup>1</sup> **Ai sensi dell’art. 2104 (“Diligenza del prestatore di lavoro”) del Codice Civile** “*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall’interesse dell’impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l’esecuzione e per la disciplina del lavoro impartite dall’imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*”; **ai sensi dell’art. 2105 (“Obbligo di fedeltà”) del Codice Civile** “*Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l’imprenditore, né divulgare notizie attinenti all’organizzazione e ai metodi di produzione dell’impresa, o farne uso in modo da poter recare ad essa pregiudizio*”.

- a) collaborare con diligenza, osservare le normative vigenti in materia, le norme del C.C.N.L. ad esso applicabile, il Regolamento, le disposizioni impartite dalla Società, le istruzioni ricevute dai propri superiori gerarchici;
- b) mantenere riservate le informazioni di cui dispone in relazione alle proprie mansioni e non utilizzarle a fini privati e al di fuori dello svolgimento delle proprie attività;
- c) adempiere alle formalità previste per la rilevazione delle presenze sul luogo di lavoro nel rispetto dei principi di correttezza;
- d) non svolgere durante l'orario di lavoro occupazioni non attinenti al servizio;
- e) avere cura dei beni strumentali aziendali a lui affidati;
- f) non utilizzare strumenti o dotazioni aziendali per ragioni diverse da quelle di servizio.

### **ARTICOLO 3 – OBBLIGHI SPECIFICI DEL DIPENDENTE IN MATERIA DI UTILIZZO DEGLI STRUMENTI AZIENDALI**

**3.1.** Fermi restando gli obblighi generali descritti all'art. 2, si riportano, di seguito, le prescrizioni specifiche relative al corretto utilizzo dei principali strumenti aziendali in dotazione al Dipendente.

#### **3.1.1. POSTAZIONE DI LAVORO**

Il Dipendente deve utilizzare la postazione di lavoro fornita dalla Società esclusivamente per le specifiche finalità inerenti alla propria attività lavorativa, in modo pertinente allo svolgimento della stessa, nel rispetto degli obblighi di diligenza e di correttezza sullo stesso gravanti. Per postazione di lavoro si intende il complesso unitario di PC, *notebook*, *software*, accessori, periferiche ed ogni altro *device* concesso; in particolare, le norme comportamentali da osservarsi nell'utilizzo della postazione di lavoro sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) il Dipendente deve proteggere il PC e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro;
- b) il Dipendente che si allontana dalla propria postazione di lavoro, ma sia certo di ritornarvi entro la fine della giornata lavorativa, è tenuto:
  - 1) ad accertarsi di aver chiuso tutti i documenti e/o applicazioni aperti, per permettere ad altri Utenti di utilizzare le stesse risorse se condivise tramite *server* di rete;
  - 2) a bloccare il sistema (per es. sui sistemi Windows XP e superiori con la combinazione di tasti CTRL+ALT+CANC e quindi "*Blocca computer*") o ad attivare la

funzione di *logout* (per es. sui sistemi Windows XP e superiori la combinazione di tasti CTRL+ALT+CANC e quindi “*Disconnett*”);

- 3) ad impostare l’attivazione automatica dello *screen saver* entro pochi minuti di inattività, per impedire la lettura dei dati presenti a video; è necessario che l’accesso al sistema dopo l’attivazione dello *screen saver* sia vincolato all’autenticazione dell’Utente, abilitando l’opzione “*Al ripristino proteggi con password*”;
- c) il Dipendente che si allontana dalla propria postazione di lavoro per non ritornarvi entro la fine della giornata lavorativa è tenuto a terminare la sessione di lavoro arrestando il sistema;
- d) il Dipendente deve utilizzare sulle postazioni di lavoro esclusivamente i *software* autorizzati e forniti dalla Società;
- e) il Dipendente deve segnalare in ogni caso e preventivamente al proprio Responsabile (ove presente) o all’Ufficio IT *Department* - Servizio Informatico Aziendale del Gruppo (d’ora in poi, “**S.I.A.**”), attraverso il *Service Desk Ticketing* o altre modalità indicate dal S.I.A. medesimo, la necessità di installare un eventuale *software* aggiuntivo e necessario, rispetto all’installazione *standard*, per lo svolgimento dell’attività lavorativa, anche nell’eventualità in cui sia gratuito; la richiesta relativa a nuove installazioni o a modifiche dei sistemi preesistenti dovrà essere inoltrata al Responsabile del S.I.A., con autorizzazione del proprio Responsabile; a tal proposito, si specifica che:
  - 1) è vietata l’installazione di programmi, *modem*, supporti magnetici o altri apparecchi senza la prevista preventiva autorizzazione;
  - 2) è vietata la connessione alla rete aziendale di *computer* personali o di altri apparecchi informatici senza la indicata preventiva autorizzazione;
  - 3) è vietato modificare le configurazioni stabilite dall’Amministrazione del Sistema Informatico della Società, quale persona fisica alla quale, nell’ambito della Società, è stato conferito il compito di sovrintendere alle risorse dei sistemi operativi (d’ora in poi, “**Amministratore di Sistema**”);
  - 4) è vietata l’installazione di applicazione per la gestione del Voice over IP (VoIP – utilizzo della rete Internet per l’effettuazione di telefonate) senza preventiva autorizzazione, in quanto potrebbero essere utilizzati canali di comunicazione non protetti;
  - 5) è vietata la connessione della rete aziendale ad altre reti mediante mezzi di comunicazione informatica quali, a titolo esemplificativo, *modem* su linea telefonica analogica e/o digitale, *modem* radio, *router x DSL* terrestre, *router x DSL wireless*;
  - 6) è vietata la memorizzazione di documenti informatici di natura offensiva, oltraggiosa e/o discriminatoria, per sesso, lingua, religione, razza, origine etnica, opinione e

appartenenza sindacale e/o politica, o, comunque, per finalità perseguibili ai sensi della normativa vigente (es.: antiterrorismo, anticorruzione, etc.);

- 7)** è vietato l'utilizzo dello strumento *software* e/o *hardware* atto ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- 8)** è vietato l'utilizzo degli strumenti informatici aziendali al fine di comunicare informazioni/notizie coperte da segreto professionale (quali, a titolo esemplificativo ma non esaustivo, documenti di gara, documenti che per disposizioni aziendali sono coperti da segreto professionale, etc.);
- 9)** qualora la funzione ricoperta e gli strumenti in dotazione consentano anche l'utilizzo in mobilità (es. PC portatili, Tablet, etc.), il Dipendente può utilizzare, fuori dall'orario lavorativo, lo strumento fornito per consultare siti Internet o analizzare documenti anche diversi da quelli aziendali a condizione di utilizzare autonoma connessione di rete e di rispettare i divieti previsti ai precedenti punti 1), 3), 4), 6), 7) e 8);
- f)** in ipotesi di malfunzionamento del PC, il Dipendente deve avvalersi esclusivamente del S.I.A. attraverso il *Service Desk Ticketing* o altre modalità indicate dal S.I.A. medesimo; ricevuta la segnalazione, è lo stesso S.I.A. a fornire l'assistenza necessaria;
- g)** ogni credenziale di identificazione informatica si riferisce ad un singolo Dipendente; non è consentito l'utilizzo della stessa credenziale da parte di più Utenti, fatti salvi i casi di "userid" amministrativi utilizzati dall'Amministratore di Sistema, nel caso in cui vi sia la necessità di consentire l'accesso ai servizi stessi senza conoscere, a priori, i soggetti che vi devono accedere;
- h)** la procedura di assegnazione delle credenziali ai Dipendenti prevede la creazione di una credenziale di identificazione informatica per l'accesso ai servizi del dominio del Gruppo e della relativa casella di posta elettronica; gli *account* così creati per ogni Dipendente non hanno scadenza prestabilita, se non quella relativa alla cessazione del rapporto di lavoro;
- i)** l'assegnazione di nuove ed ulteriori credenziali deve essere effettuata tramite richiesta al S.I.A. attraverso il *Service Desk Ticketing* o altre modalità indicate dal S.I.A. medesimo;
- j)** le credenziali del Dipendente sono costituite da un "userid" (di norma composto dalla matricola preceduta dalla sigla della Società) e da una *password*; al momento del primo accesso, deve essere effettuata la procedura di cambio della *password*, che ha una validità pari a 90 (novanta) giorni;

- k)** le credenziali di identificazione informatica alle risorse di dominio ed alle applicazioni sono immediatamente disattivate nel caso in cui un Dipendente interrompa la sua collaborazione lavorativa con la Società;
- l)** le credenziali di identificazione informatica rimaste inutilizzate da almeno 6 (sei) mesi sono disattivate, salvo si tratti di quelle utilizzate dall'Amministratore di Sistema per mere finalità di gestione tecnica e quelle utilizzate per l'accesso ai sistemi ed alle basi di dati dalle applicazioni;
- m)** ogni Dipendente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed ad uso esclusivo;
- n)** in caso di assenze programmate (come, ad esempio, in caso di ferie) e qualora vi siano esigenze di assicurare la continuità dell'attività lavorativa attraverso l'accesso ai documenti/*file* di lavoro, il Dipendente condivide, per mezzo delle cartelle di rete, le informazioni trattate nell'espletamento delle proprie mansioni con gli Utenti con cui sinergicamente espleta la propria attività lavorativa (ad esempio componenti gruppo di lavoro, referenti progetti, etc.); in alternativa, il Dipendente può autorizzare il Responsabile gerarchico di primo o secondo livello ad accedere al documento/*file* necessario ad assicurare la continuità dell'attività lavorativa; tale operazione è eseguibile anche su più *files* o cartelle;
- o)** in caso di assenze non programmate (come, ad esempio, in caso di malattia), qualora l'Utente non abbia condiviso nelle cartelle di rete i documenti/*files* di cui alla precedente lett. n) e non abbia neppure autorizzato il Responsabile gerarchico di primo o secondo livello all'accesso, il Responsabile della Struttura di appartenenza del Dipendente assente, esclusivamente per un'effettiva ed improrogabile esigenza di assicurare la continuità dell'attività lavorativa, previa autorizzazione del Dirigente responsabile della struttura organizzativa di appartenenza, può richiedere al S.I.A. di essere autorizzato ad accedere ai dati del PC; tale istanza deve pervenire in copia al Dipendente assente e l'eventuale autorizzazione rimane valida solo per il tempo strettamente necessario al recupero del/dei *file/s* e/o della cartella/e che si reputano indispensabili per dare continuità all'attività lavorativa oppure per un periodo di tempo limitato (quale, ad esempio, quello della malattia del Dipendente assente), al termine del quale la funzione di autorizzazione è automaticamente disattivata; di tale operazione di accesso ai dati ed alle informazioni richiesti e/o dopo averli trasmessi, deve essere redatto apposito verbale che viene consegnato al S.I.A. ed al responsabile del trattamento dei dati; copia di tale verbale deve essere conservata agli atti della struttura S.I.A. affinché anche il Dipendente stesso possa prenderne visione al rientro;

- p) al momento della comunicazione di risoluzione del rapporto di lavoro, il Dipendente, onde consentire il recupero di ogni informazione necessaria allo svolgimento delle attività lavorative, deve rilasciare all'Ufficio Personale della Capogruppo apposita liberatoria all'accesso del profilo personale presente sul PC in dotazione e, se assegnata, all'area di rete governata dallo stesso profilo; il Dipendente deve aver cura di rimuovere, ove presente, ogni dato personale e/o non attinente all'attività lavorativa; qualora il Dipendente non adempia a quanto indicato, la Società potrà accedere al PC ed alla casella di posta elettronica ed, una volta acquisiti i documenti strettamente attinenti alle attività lavorative, si procederà all'eliminazione di ogni altro dato estraneo alle attività aziendali;
- q) è fatto divieto al Dipendente:
- 1) scrivere la *password* su fogli o biglietti (come per esempio su "*post-it*" lasciato sul *monitor* o sotto la tastiera);
  - 2) scrivere le *password* in un documento elettronico che non sia criptato (quale, ad esempio, un file denominato "*password.txt*" presente sul *desktop*);
  - 3) rivelare la propria *password* e dare indicazioni in merito al formato ed alla lunghezza;
  - 4) trasmettere la *password* in chiaro, attraverso Internet, reti pubbliche o dispositivi *wireless* (es. messaggi di posta elettronica, etc.);
  - 5) utilizzare le funzioni di memorizzazione delle *password* sui *browser*;
  - 6) richiedere per via esplicita od implicita la consegna di altrui credenziali.

### 3.1.2. RETE E NAVIGAZIONE INTERNET

L'accesso e l'utilizzo di Internet ("**Navigazione Internet**"), in azienda e nei luoghi lavorativi, è uno strumento messo a disposizione del Dipendente per lo svolgimento esclusivo delle mansioni lavorative; è, pertanto, vietato al Dipendente l'uso improprio della Navigazione Internet; in particolare, le norme comportamentali da osservarsi nell'utilizzo di Internet sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) la Navigazione Internet è consentita durante l'orario di lavoro per lo svolgimento delle mansioni lavorative e, pertanto, è fatto divieto al Dipendente navigare in siti Internet non attinenti allo svolgimento delle stesse;
- b) è fatto divieto al Dipendente l'effettuazione di ogni genere di transazione finanziaria a titolo privato durante l'orario di lavoro, ivi comprese le operazioni di *remote banking*, acquisti *online* e simili, salvo casi espressamente autorizzati dal proprio Responsabile per motivi di urgenza;

- c) è fatto divieto al Dipendente connettere ad Internet *modem* o altri apparati di accesso remoto non espressamente autorizzati dal S.I.A. e/o strumentazioni informatiche che la Società concede in utilizzo allo stesso e che sono connesse alla rete informatica interna del Gruppo;
- d) è fatto divieto al Dipendente connettere alla rete informatica interna della Società strumenti elettronici personali o, comunque, non espressamente autorizzati;
- e) è fatto divieto al Dipendente installare e/o comunque utilizzare *software peer-to-peer* (per es. Skype, Emule, Limewire, Kazaa, Ares, BitTorrent, BitTornado, eDonkey, WinMX, Napster, Morpheus, Filetopia, SoulSeek, Shareaza, Azureus, etc.);
- f) è fatto divieto al Dipendente utilizzare strumenti per lo scambio di dati mediante sistemi esterni (es.: Dropbox, Wettransfer, etc.) poiché essi non garantiscono i necessari livelli di sicurezza e tutela della *privacy*;
- g) è fatto divieto al Dipendente utilizzare strumenti di *sniffing*, *cracking* o *scanning* e introdurre o diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, etc.) nella rete aziendale o nei sistemi;
- h) per ragioni inerenti alla sicurezza del sistema informatico, non è concesso l'accesso a siti Internet che, mediante l'attività di *web proxy* pubblici, possano aggirare l'obbligo di utilizzo del *web proxy* per la Navigazione Internet; da tali esigenze di sicurezza deriva il divieto di:
  - 1) modificare le configurazioni *standard* del *browser web* fornito dalla Società;
  - 2) accedere a caselle *web mail* di posta elettronica personale;
  - 3) scaricare o eseguire da siti Internet *software* o altro contenuto attivo;
  - 4) utilizzare siti Internet pubblici di condivisione dei *files* e di archiviazione *online*;
  - 5) caricare documenti aziendali e/o inerenti all'attività lavorativa su siti Internet pubblici di condivisione, archiviazione o *backup online*;
- i) è fatto divieto di navigare su siti Internet o registrarsi a siti Internet non attinenti allo svolgimento delle proprie mansioni lavorative;
- j) è fatto divieto di effettuare il *download* di programmi o *files* multimediali (musicali e/o filmati), anche se gratuiti, salvo autorizzazione preventiva ed espressa da parte del proprio Responsabile e del S.I.A.;
- k) è fatto divieto di partecipare a *forum* ed utilizzare *chat line* e servizi di *messenger*;
- l) è vietato lo scambio e la conservazione di *files* a contenuto offensivo, oltraggioso e/o discriminatorio, per sesso, lingua, religione, razza, origine etnica, opinione e

appartenenza sindacale e/o politica, o, comunque, per finalità perseguibili ai sensi della normativa vigente (es.: antiterrorismo, anticorruzione, etc.).

### **3.1.3. POSTA ELETTRONICA**

Il Dipendente deve utilizzare la posta elettronica esclusivamente per le specifiche finalità inerenti alla propria attività lavorativa, nel rispetto delle esigenze di funzionalità e di sicurezza dei sistemi informatici; in particolare, le norme comportamentali da osservarsi nell'utilizzo della posta elettronica sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a)** è vietato l'uso della posta elettronica per attività non attinenti allo svolgimento delle proprie mansioni lavorative;
- b)** è vietato utilizzare la posta elettronica per trasmettere documenti riservati e/o confidenziali o, comunque, coperti da segreto professionale o di Legge;
- c)** è vietato al Dipendente l'utilizzo della posta elettronica personale registrata a domini esterni al Gruppo (es.: hotmail, gmail, etc.) attraverso gli strumenti aziendali in dotazione;
- d)** la casella di posta elettronica certificata (P.E.C.) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali; tale operazione deve essere, quindi, effettuata nel rispetto della normativa vigente in materia e, in particolare, del D.Lgs. 196/2003;
- e)** è vietato lo scambio di messaggi di posta elettronica a contenuto offensivo, oltraggioso e/o discriminatorio, per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o, comunque, per finalità perseguibili ai sensi della normativa vigente (es.: antiterrorismo, anticorruzione, etc.);
- f)** è vietata la partecipazione a dibattiti, a *forum*, a *mail list*, etc. a titolo privato;
- g)** in caso di assenza prolungata dall'attività lavorativa è necessario impostare il sistema di risposta automatica ai messaggi di posta elettronica in arrivo;
- h)** secondo le indicazioni rese dalla Delibera 13/2007 del Garante, in previsione della possibilità che, in caso di assenza improvvisa e/o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, ciascun Dipendente deve scegliere e delegare un altro Dipendente a verificare il contenuto dei messaggi e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; il titolare del trattamento ha l'obbligo di redigere un apposito verbale ed informare il Dipendente interessato alla prima occasione utile;

- i) nei casi in cui il Dipendente cessi il proprio rapporto di lavoro con la Società, è concessa allo stesso la facoltà di reindirizzare per un periodo di tempo massimo di 30 (trenta) giorni, i messaggi di posta elettronica ricevuti sulla casella di posta elettronica aziendale verso un altro indirizzo di posta elettronica aziendale, previa autorizzazione del Responsabile della Struttura di appartenenza; qualora il dimissionario non provvedesse a ciò, il Responsabile S.I.A. procede a tale operazione attivando, al contempo, una risposta automatica al mittente per informarlo che il messaggio è stato reindirizzato;
- j) è obbligo del Dipendente segnalare tempestivamente al S.I.A. qualsiasi guasto e/o malfunzionamento della posta elettronica; ricevuta la segnalazione, è lo stesso S.I.A. a fornire la necessaria assistenza.

#### **3.1.4. BADGE AZIENDALE**

Il Dipendente deve utilizzare il *badge* aziendale esclusivamente per le specifiche finalità inerenti alla propria attività lavorativa, nel rispetto degli obblighi di diligenza e di correttezza su di esso gravanti; in particolare, le norme comportamentali da osservarsi nell'utilizzo del *badge* aziendale sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) il *badge* aziendale è personale e non può essere ceduto ad altri;
- b) il *badge* aziendale deve essere utilizzato per rilevare l'ingresso e l'uscita del Dipendente dalla Società all'inizio ed al termine dell'orario di lavoro, nonché all'inizio ed al termine della pausa pranzo; eventuali mancate timbrature dovranno essere autorizzate dal proprio superiore gerarchico; la timbratura deve essere effettuata al terminale più vicino alla propria postazione di lavoro e non deve esservi posticipo tra la timbratura e l'inizio effettivo della propria attività lavorativa;
- c) è obbligo del Dipendente segnalare tempestivamente al S.I.A. e all'Ufficio Personale della Capogruppo qualsiasi guasto e/o malfunzionamento del *badge*; ricevuta la segnalazione, è lo stesso S.I.A. a fornire le necessarie indicazioni operative sulle modalità con le quali procedere all'eventuale sostituzione.

#### **3.1.5. STAMPANTI, PLOTTER, FAX E FOTOCOPIATRICI**

Il Dipendente deve utilizzare stampanti, *plotter*, *fax* e fotocopiatrici esclusivamente per le specifiche finalità inerenti alla propria attività lavorativa, nel rispetto degli obblighi di diligenza e di correttezza su di esso gravanti; in particolare, le norme comportamentali da osservarsi nell'utilizzo di tali strumenti aziendali sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) stampanti, *plotter*, *fax* e fotocopiatrici e tutti gli accessori (ivi comprese le risme di carta, toner, etc.), possono essere utilizzati solo per finalità attinenti alle proprie mansioni

lavorative; è, quindi, assolutamente vietato l'utilizzo di tali strumenti per usi diversi da quelli aziendali o per fini privati;

- b) non è permesso asportare accessori di stampanti, *plotter*, *fax*, fotocopiatrici;
- c) per quanto riguarda la manutenzione e/o la riparazione di stampanti, *plotter*, *fax* e fotocopiatrici in ipotesi di guasto e/o malfunzionamento, il Dipendente deve avvalersi esclusivamente del S.I.A.;
- d) è richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; si richiede, quindi, di evitare di lasciare le stampe incustodite e di ritirarle immediatamente non appena uscite dalla stampante;
- e) l'utilizzo dei *fax* per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare; nei casi in cui questo sia necessario, occorre preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza e, successivamente, richiedere la conferma telefonica di avvenuta ricezione.

### **3.1.6. TELEFONI FISSI - TELEFONI CELLULARI AZIENDALI**

Il Dipendente deve utilizzare gli impianti di telefonia fissa e mobile messi a disposizione dalla Società, per le specifiche finalità inerenti alla propria attività lavorativa, nel rispetto degli obblighi di diligenza e correttezza su di esso gravanti; in particolare, le norme comportamentali da osservarsi nell'utilizzo di tali strumenti aziendali sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) la Società mette a disposizione, a seconda del ruolo o della funzione del singolo Dipendente, impianti di telefonia fissa e mobile, che devono essere utilizzati nel rispetto delle seguenti regole:
  - 1) il telefono fisso aziendale deve essere utilizzato esclusivamente per finalità attinenti alle mansioni lavorative e, quindi, non può essere utilizzato per finalità private (né chiamate in uscita né chiamate in entrata), salvi casi eccezionali per provate necessità;
  - 2) il telefono cellulare - se assegnato ai soli fini dello svolgimento dell'attività professionale (ad esempio, in riferimento alla mansione, per reperibilità, per chiamate di emergenza, etc.) - non può essere utilizzato per finalità private, salvi casi eccezionali per provate necessità; in ogni caso, al fine di rilevare eventuali anomalie nell'utilizzo, quale parametro di riferimento del traffico, sia voce sia dati, viene preso a riferimento il valore del traffico medio annuo dell'intera dotazione di telefonia mobile aziendale dell'ultimo anno intero disponibile;

- 3) il telefono cellulare se assegnato a titolo promiscuo, tenuto conto della mansione/funzione svolta e della motivazione per la quale è stato fornito in dotazione, può essere utilizzato anche per motivi personali alle condizioni assegnate, sia pur nel rispetto dei generali obblighi di diligenza, di correttezza e di sicurezza di cui al Regolamento nonché nel rispetto del principio di proporzionalità; in ogni caso, al fine di rilevare eventuali anomalie nell'utilizzo, quale parametro di riferimento del traffico, sia voce sia dati, viene preso a riferimento il valore del traffico medio annuo dell'intera dotazione di telefonia mobile aziendale dell'ultimo anno intero disponibile;
- b) il telefono aziendale è personale e non può essere ceduto ad altri; ogni Dipendente assegnatario di telefono aziendale è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione;
  - c) è vietato aggiungere *account* di posta elettronica personali sul telefono aziendale senza autorizzazione del proprio Responsabile sentito anche il parere del S.I.A.;
  - d) è vietato aggiungere l'*account* di posta elettronica aziendale assegnata al Dipendente sui propri telefoni personali senza autorizzazione del proprio Responsabile sentito anche il parere del S.I.A.;
  - e) è vietato caricare sul telefono aziendale applicazioni diverse da quelle in uso all'interno della Società senza autorizzazione del proprio Responsabile sentito anche il parere del S.I.A.;
  - f) è obbligo del Dipendente segnalare tempestivamente al S.I.A. qualsiasi guasto e/o malfunzionamento del telefono aziendale (fisso o cellulare); ricevuta la segnalazione, è lo stesso S.I.A. a fornire le necessarie indicazioni operative sulle modalità con le quali procedere alla riparazione e/o all'eventuale sostituzione;
  - g) nel caso di furto e/o di smarrimento del telefono cellulare aziendale, il Dipendente deve darne tempestiva comunicazione al S.I.A., e, nel caso in cui sia necessario (ad es. perdita SIM) anche alle Autorità competenti, quali, ad esempio, gli Uffici di Polizia.

### 3.1.7. **AUTOVEICOLI AZIENDALI**

Per autoveicoli aziendali, per le finalità di cui al Regolamento, si intendono esclusivamente gli autoveicoli aziendali (parco macchine) di proprietà della Società, messi a disposizione del Personale per i casi in cui, per finalità lavorative, se ne renda necessario l'uso; sono esclusi, invece, dall'ambito di applicazione del Regolamento gli autoveicoli dati in dotazione al personale Dirigente e/o direttivo della Società per uso promiscuo, per i quali è prevista la relativa disciplina e imposizione fiscale all'atto della concessione in dotazione.

Il Dipendente deve utilizzare gli autoveicoli aziendali messi a disposizione dalla Società, per le specifiche finalità inerenti alla propria attività lavorativa, nel rispetto degli obblighi di diligenza e correttezza su di esso gravanti; in particolare, le norme comportamentali da osservarsi nell'utilizzo di tali autoveicoli sono, a titolo esemplificativo e non esaustivo, le seguenti:

- a) fermo quanto previsto dalla CDS 10/2016 e dalla CDS 54/2014 e fatte salve ulteriori prescrizioni aziendali che potranno essere emanate in vigore del Regolamento, gli autoveicoli aziendali devono essere utilizzati esclusivamente per ragioni di servizio e nei casi, debitamente dimostrabili, in cui l'uso dei normali mezzi di trasporto pubblico sia inconciliabile con gli impegni da assolvere, con la celerità dell'espletamento dell'attività lavorativa e l'urgenza della stessa; è, pertanto, vietato l'utilizzo per qualsiasi altro scopo, personale o privato;
- b) per l'utilizzo degli autoveicoli aziendali il Dipendente ha l'obbligo di compilare e far autorizzare il modulo appositamente predisposto dall'Ufficio competente della Società;
- c) è vietato consentire la guida e l'utilizzo degli autoveicoli aziendali a persone estranee al servizio e, comunque, non Dipendenti della Società; l'omissione di tale prescrizione comporta la diretta responsabilità per eventuali danni arrecati dall'utilizzo dell'autoveicolo a cose e/o persone da parte del Dipendente che impropriamente abbia dato l'autorizzazione;
- d) è vietato il trasporto di personale non dipendente se non in casi strettamente connessi all'espletamento dell'attività lavorativa, previa autorizzazione rilasciata dal Responsabile dell'Area Personale della Capogruppo e, in sua assenza, dal Direttore Generale della Società;
- e) l'uso degli autoveicoli aziendali può essere consentito per trasferte comprensive di più giornate lavorative, previa autorizzazione rilasciata dal Responsabile dell'Area Personale della Capogruppo ed in sua assenza dal Direttore Generale della Società; quanto precede tenuto conto del tipo di missione da svolgere o per oggettive difficoltà che abbiano ricadute negative in termini di svolgimento dell'attività lavorativa;
- f) salvo diversa autorizzazione rilasciata dal Responsabile dell'Area Personale della Capogruppo, previa autorizzazione del Dirigente dell'Area Organizzativa dove opera il Dipendente che ne ha fatto richiesta, fuori orario di servizio tutti gli autoveicoli aziendali dovranno essere parcheggiati presso la sede della Società; il parcheggio dovrà avvenire all'interno degli spazi disponibili presso la stessa sede; l'autoveicolo dovrà inoltre essere chiuso a chiave e non dovranno essere lasciati all'interno del mezzo chiavi di apertura della sede e/o telecomandi di apertura-controllo cancelli/portoni, etc. e/o oggetti personali;
- g) il Dipendente alla guida dell'autoveicolo aziendale è tenuto a rispettare rigorosamente il Decreto Legislativo 30 aprile 1992, n. 285 e ss.mm.ii. (*"Nuovo codice della strada"*)

(d'ora in poi, "**Codice della Strada**") e/o ogni ulteriore normativa in materia di circolazione stradale nonchè ad usare lo stesso con responsabilità; tutte le contravvenzioni derivanti da violazione del Codice della Strada saranno a suo carico;

- h) negli autoveicoli aziendali è vietato fumare;
- i) in caso d'incidente, provocato o subito, il Dipendente coinvolto alla guida dell'autoveicolo aziendale dovrà ottemperare a tutte le prescrizioni previste dal Codice della Strada e/o da ogni ulteriore normativa in materia di circolazione stradale ed informare tempestivamente il competente ufficio aziendale;
- j) il Dipendente deve segnalare tempestivamente le anomalie di funzionamento della vettura al competente ufficio aziendale;
- k) in via generale, l'uso di autoveicolo proprio, con successiva richiesta di rimborso delle spese, non può essere autorizzato, ad esclusione dei seguenti casi:
  - 1) quando sia necessario un intervento urgente ed improrogabile in carenza o indisponibilità di autoveicoli aziendali;
  - 2) quando l'uso dell'autoveicolo proprio risulti per la Società più conveniente in termini economici e di efficienza del servizio e consenta un notevole miglioramento delle tempistiche operative di svolgimento dell'attività lavorativa, sempre previa autorizzazione del Responsabile dell'Area Personale della Capogruppo.

#### **ARTICOLO 4 – DISCIPLINARE CONTROLLI – CODICE DISCIPLINARE**

- 4.1. In ordine alle verifiche sul rispetto del Regolamento, la Società applica il "*Disciplinare sui Controlli di Metro Brescia Società a Responsabilità Limitata*" adottato dalla stessa, ove sono previsti controlli che escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Decreto Legislativo 14 settembre 2015, n. 151 e ss.mm.ii. ("*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183*"), al D.Lgs. 196/2003, allo Statuto dei Lavoratori ed ai provvedimenti appositamente emanati dal Garante, e, in particolare, alla Delibera 13/2007.
- 4.2. Eventuali violazioni accertate del Regolamento e degli atti in esso richiamati sono perseguibili secondo quanto previsto nel "*Codice Disciplinare di Metro Brescia Società a Responsabilità Limitata*" adottato dalla Società, nonché con le azioni legali consentite e previste dalla normativa vigente in materia.

## **ARTICOLO 5 – APPROVAZIONE, AGGIORNAMENTO E PUBBLICIZZAZIONE DEL REGOLAMENTO**

- 5.1.** Il Regolamento è stato adottato e approvato da Metro Brescia Società a Responsabilità Limitata con Delibera del Consiglio di Amministrazione del 02.09.2016.
- 5.2.** Il Regolamento sarà sottoposto ad aggiornamento periodico, in ragione di mutate esigenze aziendali, di modifiche normative intervenute nel corso della sua vigenza, di indirizzi e/o di indicazioni e/o di interpretazioni provenienti dalle varie Autorità in materia ed in ogni altra circostanza in cui la Società riterrà necessario e/o opportuno modificarne e/o aggiornarne i contenuti.
- 5.3.** Il Regolamento deve essere adeguatamente pubblicizzato e portato a conoscenza di tutti i Dipendenti della Società, a cura dell'Area Personale, Organizzazione e Relazioni Industriali della Capogruppo, mediante efficaci forme di comunicazione e pubblicazione, con la previsione dell'obbligo di rispettarne i contenuti. Ai Dipendenti assunti in epoca successiva alla data di adozione e di approvazione del Regolamento, lo stesso dovrà essere consegnato all'atto dell'assunzione.