DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Amr
Agenzia mobilità romagnola

Regole di condotta ed obblighi dei dipendenti in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto in applicazione delle disposizioni di cui al Regolamento UE 679/16 e del Codice Privacy

Versione n.	**Motivo della revisione**	**Data Approvazione**
1.0	Prima emissione	03/03/2021 (PG n.972/21 del 4/3/21)
2.0	Modifiche al Cap. 8	14/06/2022 (PG n.2570/22 del 14/6/22)
3.0	Inserimento par. 8.3	Determinazione AU n. 1 del 10.01.2025

1. Capitolo I – AMBITO GENERALE

1.1 Definizioni

Ente/Organizzazione/Azienda: AGENZIA MOBILITA' ROMAGNOLA (di seguito Agenzia o AMR)

Regolamento UE 679/16: Regolamento in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati approvato dal Parlamento Europeo e dal Consiglio dell'Unione Europea il 27/04/2016

Codice privacy: Decreto Legislativo 196 del 30 Giugno 2003 come modificato dal D.Lgs. 101 del 10 Agosto 2018.

Data-breach: una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Dipendente: personale dell'Agenzia assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Agenzia.

Responsabile Informatico: il Responsabile Sistemi Informativi e Tecnologie.

1.2 Premessa

L'ambito lavorativo porta l'Agenzia a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare le attività che le vengono contrattualmente richieste.

Tali informazioni possono essere considerate, ai sensi del Regolamento Europeo 679/16 e del Codice privacy italiano vigenti, "**dati personali**" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Agenzia adotti una serie di misure minime ed idonee alla loro tutela.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per NDA (Accordo di riservatezza) o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" strettamente intesi a norma di legge.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Agenzia.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza

nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, la scrivente Agenzia ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica agli **Incaricati** che si trovino ad operare con dati dell'Agenzia.

Un uso dei COMPUTER e di altri dispositivi elettronici (di seguito DISPOSITIVI) nonché dei servizi di Internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate, nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dello stesso.

1.3 Autorizzazione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'Agenzia valuta la presenza dei presupposti per autorizzare all'uso dei vari dispositivi aziendali, di Internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l'Agenzia valuta la permanenza di tali presupposti, potendo revocare, in tutto o in parte l'iniziale autorizzazione, con comunicazione individuale.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare uno o anche tutte le seguenti strumentazioni:

1. L'utilizzo del COMPUTER o di altri DISPOSITIVI e/o funzioni di esso;
2. L'utilizzo della posta elettronica;
3. L'accesso a Internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Regolamento Europeo 679/16 e del Codice Privacy. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

1.4 Titolarità dei dispositivi e dei dati

AMR è esclusiva titolare e proprietaria dei Dispositivi messi a disposizione degli Incaricati ai soli fini dell'attività lavorativa.

AMR è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

1.5 Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nella disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di AMR, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6 Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'Agenzia, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dispositivi in uso;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

2. Capitolo II – PASSWORD

2.1 Le Password

Le password sono un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'Agenzia nel suo complesso.
Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

L'Agenzia ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password. In particolare, per quanto riguarda le password di accesso al Dominio, è in funzione un sistema automatico di richiesta di aggiornamento delle stesse, impostato dall'Agenzia secondo il livello di sicurezza stabilito dalla stessa.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

In qualsiasi momento l'organizzazione si riserva il diritto di revocare all'Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2 Regole per la corretta gestione delle password

L'Incaricato, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e possono contenere anche lettere maiuscole, caratteri speciali (per esempio, i seguenti: { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _). e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno ogni 3 mesi a seconda che l'incaricato tratti dati cd. particolari (es. dati inerenti salute, appartenenza politica o sindacale, etc.) o meno.
   A tal fine è stato adottato un sistema automatico di richiesta di aggiornamento password.
6. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Agenzia.

Al fine di una corretta gestione delle password, l'organizzazione esorta a non utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, (ad es. pippo, security, etc);

7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza o utilizzata in servizi ed attività extralavorative

2.3 La password nei sistemi

Ogni Incaricato può variare in modo autonomo la propria password di accesso a quei sistemi aziendali che sono dotati di tale funzionalità. La password può essere sostituita dal Titolare o da suo incaricato, anche qualora l'Utente l'abbia dimenticata.

3. Capitolo III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1 Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In alcuni casi potrebbe essere necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richieda uno username e una password.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2 Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata e spegnere il PC;
4. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

4. Capitolo IV - USO DEL PERSONAL COMPUTER DELL'AGENZIA

4.1 Modalità d'uso del COMPUTER aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

I files creati, elaborati o modificati sul computer assegnato devono essere sempre salvati sul sistema di repository documentale centralizzato.

4.2 Corretto utilizzo del COMPUTER aziendale

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema, utilizzando account con privilegi di amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali e di rete (repository e backup) che ai server aziendali nonché al singolo computer, anche in remoto.

In particolare, l'Incaricato deve adottare le seguenti misure:

1. Utilizzare le aree di memoria della rete dell'Agenzia ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3 Divieti Espressi sull'utilizzo del COMPUTER

All'incaricato **sono vietate** le seguenti operazioni:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer, senza l'autorizzazione del Responsabile Informatico.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Agenzia.
4. Installare alcun software di cui l'Agenzia non possieda la licenza, né installare alcuna versione diversa,

anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. È vietato fare copia del software installato.

5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione del Responsabile Informatico.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive, ad esclusione dell'installazione di patch o aggiornamenti proposte dal sistema.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dall'organizzazione.

4.4 ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via Internet, via mail, scambio di supporti removibili, file-sharing, chat e altro.

L'incaricato si impegna a rispettare le regole seguenti:

1. Installare gli antivirus sui dispositivi se non ancora presenti, segnalandolo al Responsabile Informatico;
2. Adottare le procedure di aggiornamento antivirus, segnalando eventuali problemi al Responsabile Informatico;
3. Comunicare al Responsabile Informatico ogni anomalia o malfunzionamento del sistema antivirus di cui possa rendersi conto;
4. Comunicare immediatamente al Responsabile Informatico eventuali segnalazioni di presenza di virus o file sospetti;
5. Comunicare immediatamente al Responsabile Informatico eventuali data-breach.

Inoltre, all'incaricato:

a) È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
b) È vietato ostacolare l'azione dell'antivirus aziendale;
c) È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Agenzia anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
d) È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

5. Capitolo V – INTERNET

5.1 Internet è uno strumento di lavoro

La connessione alla rete Internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è consentito sporadicamente, per questioni urgenti ed indifferibili e con gli accorgimenti di cui al presente documento.

In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati, in ragione delle particolari mansioni svolte.

5.2 Misure preventive per ridurre navigazioni illecite

L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

5.3 Divieti Espressi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati sensibili ai sensi della normativa vigente in materia di riservatezza dei dati personali.
2. È fatto divieto di accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet, qualora non siano autorizzati o legati all'attività lavorativa.
4. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
5. È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list utilizzando il marchio o la denominazione dell'Azienda, salvo specifica autorizzazione dell'Azienda stessa.
6. E' vietata ogni tipo di attività sui social network che non sia legata alle proprie funzioni.
7. È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. È vietato accedere dall'esterno alla rete interna dell'Azienda, salvo con le specifiche procedure previste dall'Azienda stessa.
10. È vietato creare siti web personali sui sistemi dell'Azienda.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è effettuata sotto la personale responsabilità dell'Incaricato e potrebbe essere considerata violazione degli obblighi contrattuali.

5.4 Divieti di Sabotaggio

È vietato accedere ad Internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Agenzia per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5 Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, etc.) se non espressamente autorizzato dall'organizzazione.

6. Capitolo VI – POSTA ELETTRONICA

6.1 La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. Non è pertanto consentito l'uso della posta elettronica aziendale per motivi personali.

Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica aziendale.
Le caselle e-mail possono anche essere assegnate con natura impersonale (tipo info, Amministrazione, Assistenza, etc.) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", in linea con i suggerimenti dati dal Garante a tal proposito, in passato.

Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fortemente raccomandato di non utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

6.2 Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'organizzazione è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

6.3 Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione (amr-romagna.it) per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
2. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
3. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
4. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
5. È vietato l'utilizzo della email personale per mezzo dei dispositivi aziendali;
6. È vietato utilizzare la email personale per inviare messaggi di natura aziendale, salvo situazioni eccezionali e previa specifica autorizzazione aziendale.

6.4 Posta Elettronica in caso di assenze improvvise e programmate

Nel caso di assenza prolungata è previsto che sia attivato il servizio di risposta automatica (Auto- reply) con

indicazioni del sostituto e della data di rientro salvo accordi diversi con la Dirigenza.
In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato – dietro autorizzazione del Dirigente di riferimento e comunicandolo al Responsabile Informatico - deve nominare un collega fiduciario che, in caso di assenza, abbia accesso alla sua casella di posta elettronica.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o quest'ultimo sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica, informandone l'incaricato stesso non appena possibile.

6.5 Utilizzo illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori della razza dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

7. Capitolo VII – USO DI ALTRI DISPOSITIVI

7.1 Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd,ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quali ad esempio una chiave USB, un hard disk esterno, una memory card) su cui copiare temporaneamente i dati per un facile trasporto o per altri usi (es. macchine fotografiche o videocamere con memory card).

Questi dispositivi devono essere gestiti con le stesse accortezze previste nel presente disciplinare per gli strumenti informatici in dotazione e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.2 Dispositivi personali.

Ai dipendenti non è permesso svolgere la loro attività lavorativa utilizzando strumentazione personale tranne i casi in cui ciò sia consentito dal presente Disciplinare o autorizzato da accordi e regolamenti aziendali, sia collettivi che individuali.

Nei casi predeterminati dallo stato di necessità, e fino a diverse disposizioni, ai dipendenti che svolgono la loro attività lavorativa da casa è consentito l'uso di strumentazione personale previa comunicazione al Responsabile Informatico.

Al dipendente è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …) salvo casi di necessità autorizzati dal Responsabile Informatico che impartirà le necessarie istruzioni.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'Agenzia solo se espressamente autorizzati dall'Agenzia stessa e assumendone formalmente la responsabilità del trattamento.
Tali dispositivi potranno essere preventivamente valutati dall'Agenzia, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

Tutti i dipendenti hanno ricevuto uno smartphone aziendale ed una SIM CARD aziendale, tuttavia alcuni preferiscono utilizzare lo smartphone personale eventualmente installandovi la SIM CARD aziendale.
Inoltre, nella convenzione Intercent-ER per la fonia mobile a cui AMR ha aderito, è prevista la possibilità (attivabile su ciascuna SIM) che le SIM CARD aziendali possano essere utilizzate per effettuare telefonate personali anteponendo il prefisso 4146 al numero chiamato; i numeri di telefono chiamati in questa modalità risultano "oscurati" nei tabulati telefonici a cui AMR ha accesso.

7.3 Distruzione dei Dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo, dovranno essere restituiti all'Agenzia che provvederà a ricondizionarli seguendo le norme di legge in vigore al momento.

8. Capitolo VIII -APPLICAZIONE E CONTROLLO – STRUMENTI DI PROTEZIONE

8.1 Il controllo

L'Agenzia, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment (valutazione di vulnerabilità) del sistema informatico.
Per tali controlli l'organizzazione si riserva la possibilità di avvalersi di soggetti esterni.

8.1.1 GPS sui veicoli aziendali

Sui veicoli aziendali a noleggio in uso promiscuo al personale (cioè non assegnati nominalmente), sono installati dispositivi GPS per la geolocalizzazione dei veicoli medesimi, per finalità di tutela del patrimonio aziendale. L'installazione è stata concordata con la RSU aziendale, come da accordo sottoscritto ai sensi dell' art. 4, primo comma, l. n. 300/1970.

8.1.2 APP MARCATEMPO:

Sugli smartphone aziendali è installata una app marcatempo, utilizzabile in casi codificati per la registrazione della presenza al lavoro.

Tale app è installata anche su alcuni smartphone personali.

La app marcatempo localizza la posizione del dipendente. Per interrompere la localizzazione è necessario disattivare la connessione dati e la localizzazione nello smartphone.

Al termine della timbratura, la registrazione della posizione viene interrotta. È tuttavia opportuno, a tutela della libertà del dipendente, che la APP venga chiusa correttamente al termine dell'utilizzo.

A tutti i dipendenti è stata distribuita una Privacy policy specifica.

8.1.3 SIM CARDS AZIENDALI

AMR ha accesso ai tabulati delle chiamate effettuate dalle SIM CARDS aziendali assegnate ai dipendenti.
Qualora la SIM CARD aziendale sia utilizzata per effettuare telefonate personali, si obbligano i dipendenti ad anteporre al numero chiamato il prefisso 4146, anche per oscurare, nei tabulati delle chiamate effettuate, una parte del numero telefonico del destinatario.

8.2 Modalità di verifica

In applicazione del principio di necessità di cui all'art. 5 del Regolamento Europeo 679/16, nonché della privacy by design e by default di cui all'art. 25 della medesima normativa, l'organizzazione promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri delle apparecchiature informatiche aziendali, in ogni caso minimizzando la raccolta e l'uso di dati riferibili agli Incaricati, fatte salve le indicazioni di legge. Allo scopo potrà adottare strumenti tecnici, organizzativi e fisici, volti a prevenire trattamenti

illeciti dei dati trattati con strumenti informatici.

AMR informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, i controlli atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) l'azienda effettuerà in prima istanza un avvertimento in modo generalizzato, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Nei casi più gravi, potrà farsi ricorso anche a provvedimenti di carattere disciplinare.

8.3 Strumenti di protezione generali

Fermo quanto già osservato, la Società ha adottato le seguenti ed ulteriori misure di protezione riguardanti gli strumenti informatici e il loro utilizzo.

- Antivirus preinstallato in ciascun dispositivo informatico utilizzato dal personale della Società;
- Mappatura delle licenze riguardanti i programmi per elaboratore utilizzati dal personale della Società;
- Accesso da remoto alle reti aziendali tramite VPN;
- Sistema di server aziendali gestito internamente accessibili esclusivamente da personale autorizzato;
- Sistema di back-up centralizzato dei server aziendali, con procedure di ripristino dei sistemi in caso di malfunzionamenti che ne impediscano l'utilizzo;
- Sistema di difesa perimetrale della rete aziendale basato su firewall.

9. Capitolo IX – PROVVEDIMENTI DISCIPLINARI

9.1 Conseguenze delle infrazioni al Disciplinare

Le infrazioni alle prescrizioni del presente Disciplinare potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale e/o di Comparto applicato, nonché ai sensi del vigente sistema sanzionatorio adottato dalla Società.

10. Capitolo X – VALIDITA’, AGGIORNAMENTO ED AFFISSIONE

10.1 Validità

Il presente Disciplinare ha validità a partire da: 10.01.2025

10.2 Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell’organizzazione o in caso di mutamenti legislativi.

Ogni variazione del presente Disciplinare sarà comunicata ai dipendenti incaricati.

10.3 Affissione e pubblicità

Il presente Disciplinare, ed ogni successivo aggiornamento, verrà pubblicato sulla intranet aziendale ai sensi dell’art. 7 della legge 300/70 e verrà data comunicazione dell’avvenuta pubblicazione tramite email ai dipendenti. Il presente Disciplinare potrà altresì essere affisso nelle bacheche accessibili ai dipendenti nei locali aziendali.

Data, 10.01.2025

Visto del Direttore Generale

Firmato digitalmente da: Guido Guerrieri
Organizzazione: AGENZIA MOBILITA' ROMAGNOLA/02143780399
Data: 16/01/2025 08:01:54

Firma del Titolare del trattamento