AFOL METROPOLITANA

REGOLAMENTO PER LE ATTIVITÀ DEI SISTEMI INFORMATIVI E LA PROTEZIONE DEI DATI

Approvato dal Consiglio di Amministrazione in data 25/03/2019
con delibera n.7 del verbale n.54

SEDE LEGALE
via Soderini, 24, 20146 Milano
PI 08928300964

protocollo@afolmet.it
www.afolmet.it

Art. 1 - Campo d'applicazione

Il presente Regolamento si applica a tutte le attività supportate da sistemi informatici e telematici per l'elaborazione e la trasmissione di dati aziendali e/o riferiti a persone fisiche, siano essi contabili, fiscali, gestionali, tecnici e commerciali nonché tutte le attività per il trattamento dati sia in forma digitale che manuale.
A tal fine, viene individuato l'insieme di regole atte a definire il corretto comportamento da tenere nell'utilizzo dei dispositivi e dei servizi messi a disposizione degli utenti di AFOL Metropolitana, garantendo la conformità dei sistemi informativi ai requisiti di sicurezza e alle vigenti normative sulla protezione dei dati personali.

Destinatari del presente regolamento sono i dipendenti, collaboratori e tutti gli utilizzatori che a vario titolo, nello svolgimento della propria attività, ricorrono ai servizi informatici e telematici forniti da AFOL Metropolitana. Non disciplina invece strumenti e servizi che AFOL Metropolitana mette a disposizione dell'utenza esterna. In tali casi il settore richiedente è responsabile dell'osservazione delle norme di legge in materia.

Art. 2 - Accesso a banche dati esterne pubbliche e/o private

L'accesso alle banche dati sia di carattere pubblico che privato è consentito solo se inerente alle finalità lavorative ed è consentito solo per l'accesso a informazioni strettamente collegate alle proprie mansioni e per cui si possiedono le autorizzazioni all'aggiornamento e/o consultazione.
Il personale autorizzato alla consultazione delle banche dati esterne deve uniformarsi alle procedure in essere per tali consultazioni.
È vietato effettuare estrapolazioni, estrazioni, acquisizioni, e stampe di dati per i quali non si è autorizzati alla consultazione.
In caso di accesso involontario a banche dati per le quali non si possiedono le opportune autorizzazioni, è fatto obbligo di interromperne la consultazione e di darne immediata comunicazione al proprio responsabile.

Art. 3 - Utilizzo degli strumenti informatici

Un utilizzo consapevole degli strumenti informatici rappresenta una condizione imprescindibile e un obiettivo prioritario da perseguire.
A ogni dipendente e collaboratore di AFOL Metropolitana è fatto specifico divieto di utilizzare impropriamente la strumentazione informatica data in dotazione da AFOL Metropolitana.
Per strumentazione informatica si intende qualunque apparecchiatura atta a comunicazioni di tipo digitale, vocale, di consultazione dati, navigazione internet, consultazioni di immagini e/o video.
La strumentazione informatica (fissa o mobile) e i relativi programmi e/o applicazioni affidati al personale sono strumenti di lavoro e pertanto:

- devono essere custoditi in modo appropriato;
- possono essere utilizzati esclusivamente per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali;
- devono essere prontamente segnalati a AFOL Metropolitana il furto, danneggiamento o smarrimento di tali strumenti.

I dipendenti e collaboratori di AFOL Metropolitana che si trovino ad operare mediante l'utilizzo di sistemi informatici aziendali dovranno scrupolosamente rispettare le procedure all'uopo previste, ossia:
Ciascun dipendente, all'atto di presa in servizio, verrà dotato di proprie credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ai trattamenti che dovrà effettuare. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente, associato ad una parola chiave riservata, individuata e conosciuta solamente dal medesimo.
Le credenziali di autenticazione non utilizzate da almeno sei mesi verranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali verranno disattivate anche in caso di perdita della qualifica che consente all'incaricato l'accesso ai dati personali.
Le *password* di accesso ai dispositivi e/o sevizi dovranno essere modificate almeno ogni 6 mesi. Ogni singola password dovrà rispettare le seguenti regole di complessità:

- non deve contenere il nome account dell'utente;
- deve essere composta da almeno otto caratteri;
- deve contenere caratteri di almeno tre delle quattro categorie seguenti:
- lettere maiuscole dell'alfabeto latino (dalla A alla Z);
- lettere minuscole dell'alfabeto latino (dalla a alla z);
- numeri in base 10 (da 0 a 9);
- caratteri non alfanumerici, ad esempio punto esclamativo (!), dollaro ($), simbolo di cancelletto (#) o percentuale (%).

La *password* e il nome utente assegnati non dovranno essere rivelati a nessuno e per alcun motivo. Ciascun utente è tenuto ad adottare le necessarie cautele per assicurare la segretezza della password e per evitare che altri vengano, anche accidentalmente, a conoscenza di tale password. Quest'ultima non deve essere riportata su alcun appunto, non deve essere trascritta su supporti (es. fogli, post-it) facilmente accessibili a terzi, né memorizzata sul proprio PC, né deve essere comunicata per telefono salvo che per gravi necessità. Nel caso di sospetto che altri siano a conoscenza della propria *password* si dovrà informare il Responsabile dei Sistemi Informativi e modificare la password.
Le banche dati a cui si ha accesso devono essere utilizzate per il solo scopo per cui sono state create ed è vietato installare programmi non autorizzati.
È vietato installare modem o altri dispositivi non autorizzati.
Qualora il proprio computer non venga temporaneamente utilizzato, deve essere impostato lo screensaver.
È vietato l'utilizzo di floppy disc – cd rom – chiavette usb, di altri supporti o di programmi che non siano stati forniti dall'azienda e/o approvati dal Responsabile dei Sistemi Informativi.

AFOL Metropolitana dota di caselle di posta elettronica anche i consulenti esterni, i collaboratori e gli stagisti allo scopo di salvaguardare l'integrità e l'immagine dell'ente in ogni comunicazione di servizio interna ed esterna e per garantire la correttezza e la liceità delle informazioni scambiate dalle caselle dei consulenti che sono comunque sottoposte alle misure minime di sicurezza definite in questo disciplinare.
Le caselle sono attive per la durata del rapporto di collaborazione, alla scadenza del contratto vengono automaticamente disattivate. La richiesta di apertura delle caselle viene inoltrata dal Responsabile del Servizio ed approvata dal Direttore Generale.
Le caselle per personale esterno hanno la seguente struttura:
n.cognome.cons@afolmet.it
n.cognome.st@afolmet.it

Art. 4 - Utilizzo del personal computer

Onde evitare il grave pericolo di introdurre *malware* nonché di alterare la stabilità delle applicazioni installate sul proprio computer, è consentito installare programmi diversi da quelli pre-installati solo se formalmente autorizzati dal Responsabile dei Sistemi Informativi che ne determina anche le modalità di installazione.
Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente da AFOL Metropolitana.
Non è consentito utilizzare strumenti *software* e/o *hardware* atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
Non è consentito modificare le configurazioni impostate del proprio PC, sia software che hardware (ad esempio: installazione di masterizzatori, schede *wireless*, memoria RAM, schede audio/video, altoparlanti, etc.).
Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem).
Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, *files* multimediali, se non a fini prettamente lavorativi.
La *password* di accesso alla rete aziendale è strettamente personale ed è assolutamente necessario che la stessa non venga comunicata e/o resa accessibile ad altre persone.

Art. 5 - Utilizzo del personal computer portatile

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.
Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;
- avvertire tempestivamente il Responsabile dei Sistemi Informativi, che darà le opportune indicazioni, in caso di furto di un PC portatile;
- essere sempre ben consapevole delle informazioni archiviate sul portatile (essendo quest'ultimo maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa);
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico;
- per quanto possibile, non archiviare dati riservati, personali e/o contenenti categorie "particolari" (ai sensi dell'art. 9 Reg. UE 2016/679) nelle memorie del PC portatile. In ogni caso, l'eventuale salvataggio in locale dovrà durare il tempo strettamente necessario a riversare i dati sui *files* server dell'azienda e successivamente i *files* locali andranno eliminati.

Art. 6 - Utilizzo di supporti magnetici

Non è consentito scaricare, salvare e/o utilizzare *files* contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa. Tutti i *files* di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus e, se del caso, a relativa autorizzazione all'utilizzo da parte del Responsabile dei Sistemi Informativi.

Art. 7 - Navigazione in Internet

Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli contrari all'etica Aziendale, alla decenza, alla normativa vigente in materia di reati postali, di reati contro la persona, di reati di terrorismo, di reati a scopo sessuale e in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente.
Non è consentito scaricare di *software* a pagamento, gratuiti (*freeware*) e *shareware* prelevato da siti Internet, se non formalmente autorizzati dal Responsabile dei Sistemi Informativi.
Non è permessa la partecipazione, per motivi non professionali a Forum, l'utilizzo di *chat line*, di bacheche elettroniche, le registrazioni in *guest book* anche utilizzando pseudonimi (o *nicknames*) e l'iscrizione a *mailing list*.

Art. 8 - Utilizzo della posta elettronica

Non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate.
Qualunque comunicazione ricevuta o spedita utilizzando l'indirizzo di posta di AFOL Metropolitana non è corrispondenza personale del dipendente, per cui potrebbero essere effettuati controlli remoti al fine di verificare l'uso improprio o illecito degli strumenti forniti in dotazione.
In ipotesi di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica assegnato al dipendente rimarrà attivo per 3 mesi; nel suddetto periodo, a tutti coloro che scriveranno all'indirizzo in parola verrà inviata una "risposta automatica", contenente l'indicazione di altro indirizzo *email* al quale contattare l'azienda.
Non è consentito l'utilizzo del dominio di posta elettronica di AFOL Metropolitana per la partecipazione a dibattiti, Forum o *mail-list*, salvo diversa ed esplicita autorizzazione.
La *password* di accesso al sistema di posta elettronica è strettamente personale ed è assolutamente necessario che la stessa non venga comunicata e/o resa accessibile ad altre persone. La posta elettronica diretta all'esterno di AFOL Metropolitana può essere intercettata da estranei, e dunque, non deve assolutamente essere usata per inviare documenti di lavoro "Strettamente Riservati", se non formalmente autorizzati dalla Direzione.
Inoltre gli utilizzatori della posta elettronica devono attenersi alle seguenti regole di comportamento:

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative;

b)prestare attenzione ai messaggi di posta elettronica e ai *file*, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:

- evitare di aprire il messaggio, evitare di aprire gli allegati o cliccare sui "*link*" eventualmente presenti;
- segnalare l'accaduto al Responsabile dei Sistemi Informativi, cancellare il messaggio e svuotare il "cestino" della posta;

c) evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;

d) in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.

e) non è consentito inviare, tramite posta elettronica, certificati di sorta agli interessati che ne facciano richiesta con email; questi devono essere invitati a:

- scaricare il certificato di interesse - se disponibile - tramite accesso al Sistema Informativo Sintesi, previa autenticazione;
- inviare la richiesta tramite email PEC unitamente a copia del documento d'identità (è in questo caso consentito inviare il certificato all'indirizzo PEC del richiedente);
- recarsi personalmente presso gli Uffici di AFOL Metropolitana per richiedere il certificato.

L'ambiente di posta è in grado di identificare ed eliminare i principali virus nascosti negli allegati; tuttavia è possibile che qualche virus non venga intercettato ed è compito di ogni utente vigilare e cancellare ogni e-mail con allegati sospetti specialmente se non se ne conosce la provenienza.

Art. 9 - Incaricati al trattamento di dati personali

Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso, considerando a tal fine tutti i dati come "confidenziali" e, di norma, soggetti al segreto d'ufficio.
Le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

In caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.
Non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile.
Deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.
Tutti coloro che, nell'esercizio delle proprie mansioni, trattano dati personali in nome e per conto di AFOL Metropolitana devono osservare le seguenti disposizioni.
La raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali può avvenire esclusivamente se richiesto per lo svolgimento delle proprie mansioni.
La documentazione cartacea contenente eventuali dati sensibili (come trattenuta sindacale o stato di salute del lavoratore) deve essere conservata separatamente in fascicoli non accessibili a personale non autorizzato ad accedervi (preferibilmente, la documentazione in parola deve essere conservata in armadi chiusi a chiave).
Le banche dati devono essere conservate con la massima attenzione e scrupolosità al fine di evitare che soggetti non autorizzati vengano a conoscenza dei dati.
Quando ci si assenta dal proprio ufficio le banche dati cartacee devono essere riposte negli armadi o nei cassetti.
Chiunque trasporti all'esterno documenti contenenti dati personali ne è responsabile della conservazione, protezione, integrità e non diffusione, mettendo quindi in atto tutte le procedure a tal fine necessarie.
Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati che rientrano nell'ambito del trattamento definito, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati.
L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
Ogni Incaricato del trattamento dei dati personali deve richiedere agli interessati solamente i dati strettamente necessari allo svolgimento delle mansioni assegnate e correlati alle finalità per le quali vengono richiesti; in ipotesi di rilascio - da parte degli interessati - di dati "particolari" (ai sensi dell'art. 9 Reg. Eu. 2016/679) ulteriori e non necessari, gli stessi non devono essere acquisiti o, quantomeno, devono essere oscurati a cura degli incaricati.
Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

Per i **trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici**, tutti coloro che nell'esercizio delle loro mansioni trattano dati personali in nome e per conto di AFOL Metropolitana debbono osservare le seguenti disposizioni.
I documenti contenenti categorie "particolari" di dati personali (ai sensi dell'art. 9 Reg. UE 2016/679) affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, sono controllati e custoditi dagli incaricati fino alla restituzione in modo tale che ad essi non accedano persone prive di autorizzazione.
L'accesso agli archivi contenenti categorie "particolari" di dati personali (ai sensi dell'art. 9 Reg. UE 2016/679) è controllato.
Le persone che accedono ai suddetti archivi devono essere preventivamente autorizzate dal proprio Responsabile gerarchico.
I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
È inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
È proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti, anche accidentalmente, da terzi non autorizzati. Queste precauzioni diventano particolarmente importanti quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

Qualora si ricevano nel proprio ufficio utenti o colleghi e si tengano sulla propria scrivania fascicoli o documentazione contenente dati personali, si consiglia di fare attenzione a rivoltare le cartelle o i documenti; laddove compatibile con le necessità organizzative, i dipendenti devono inserire sul frontespizio delle cartelle e/o dei faldoni dati e informazioni che non permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento.
È necessario, prima di gettare documentazione contenente dati personali (soprattutto se si tratta di dati "particolari") nel cestino della carta, provvedere a renderne non comprensibile il contenuto. Al fine di realizzare il predetto scopo, potranno essere utilizzati apparati distruggi documenti o altri più banali accorgimenti come ad esempio lo strappo dei documenti, la separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Art. 10 - Verifiche

Il Servizio Sistemi Informativi può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto *virus*, *malware*, intrusioni telematiche, fenomeni quali *spamming*, *phishing*, *spyware*, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.
Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il *desktop* delle singole postazioni.
Il Servizio Sistemi Informativi può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di *file* o applicazioni pericolose).
Il Servizio Sistemi Informativi, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, è abilitato ad accedere alla posta elettronica dell'utente per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'utente.
Il Servizio Sistemi Informativi può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti o mediante "*file di log*" della navigazione svolta.
L'eventuale controllo sui *file di log* da parte del Servizio Sistemi Informativi non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto –Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, fatti salvi in ogni caso specifici obblighi di legge.
Il sistema di registrazione dei *log* è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
Il Servizio Sistemi Informativi è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.
Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
In ogni caso, AFOL Metropolitana garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (*log*) al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

AFOL Metropolitana si riserva di verificare, nei limiti delle norme di legge e di contratto collettivo, il rispetto di quanto previsto nel presente regolamento e l'integrità del proprio sistema informatico.
Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzate dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento. In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito delle strutture lavorative di aree nelle quali si è verificata l'anomalia.
Qualora il controllo anonimo rilevi un utilizzo anomalo degli strumenti informatici, il Responsabile Sistemi Informativi effettuerà un avviso generalizzato inerente l'utilizzo anomalo rilevato, con l'invito ad attenersi scrupolosamente alle istruzioni impartite.
Se le anomalie dovessero perdurare, si procederà a controlli su base individuale o per postazioni di lavoro segnalando il comportamento al Responsabile del Servizio di appartenenza del dipendente e all'Ufficio del Personale che, se necessario, attiverà un procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L. e dai Regolamenti aziendali.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento verrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Art. 11 - Strumenti di protezione da *Malware*

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615- quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici di protezione da *malware* che verranno aggiornati regolarmente.

Art. 12 - Compiti del Servizio Sistemi Informativi

AFOL Metropolitana si è dotata di strumenti informatici che impediscono accesso e/o ricezione di materiale improprio e contrario alle leggi vigenti ed alla concezione etica aziendale. E' compito del Responsabile dei Sistemi Informativi di mantenere in essere tali strumenti e di eventualmente prevedere nuove regole per un corretto utilizzo degli strumenti informatici in possesso dei dipendenti.
È inoltre compito del Responsabile dei Sistemi Informativi verificare, nei limiti consentiti dalle norme di legge e contrattuali, il rispetto delle regole e dell'integrità del sistema informativo Aziendale, degli strumenti che lo compongono e dei dati in esso contenuti.
Il Responsabile del Servizio Sistemi Informativi deve informare semestralmente l'Organismo di vigilanza sugli aspetti significativi afferenti le diverse attività informatiche di propria competenza, in particolare per quanto attiene a:
Accessi abusivi alla rete informatica ed eventuali violazioni dei Sistemi Informativi
Contestazioni in ordine alla regolarità delle licenze.

Art. 13 - Attività di informazione dei dipendenti

I dipendenti e collaboratori di AFOL Metropolitana devono dare sollecita comunicazione ai propri Responsabili gerarchici, che ne daranno comunicazione al Responsabile Sistemi Informativi, di ogni eventuale danno, da essi provocato anche involontariamente, nonché di ogni eventuale danno comunque riscontrato durante l'utilizzo dei sistemi informatici.
Inoltre devono comunicare ai propri responsabili gerarchici, che ne daranno comunicazione al Responsabile Sistemi Informativi, ogni e qualunque consultazione impropria che abbiano commesso anche per errore.
I dipendenti e collaboratori di AFOL Metropolitana, al fine di non esporre sé stessi e l'Azienda a rischi sanzionatori, sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente e alla regolamentazione aziendale.
I dipendenti e collaboratori di AFOL Metropolitana sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica.
Tutti i dipendenti e collaboratori di AFOL Metropolitana sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituiscono inadempimento contrattuale che potrà comportare:

- per il personale dipendente, oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;
- per i collaboratori esterni, oltre che la risoluzione del contratto, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.