Policy per l'utilizzo degli Strumenti Informatici

EURO.PA SERVICE SRL
Approvato: CDA del 21 10 2020

SOMMARIO

PREMESSA

L'uso degli strumenti informatici da parte di dipendenti e collaboratori

A seguito del provvedimento generale del Garante per la tutela dei dati personali del 1° marzo 2007 relativo all'utilizzo di Internet e della posta elettronica da parte dei dipendenti e collaboratori, Euro.pa Service srl ha ritenuto opportuno aggiornare e sintetizzare in un unico documento le previsioni adottate nella gestione dell'utilizzo degli strumenti aziendali di comunicazione (telefono, fax, posta elettronica, personal computer e internet).

I principi fondamentali adottati per il corretto utilizzo degli strumenti informatici sopra citati sono i seguenti:

- ✓ la navigazione internet è consentita solo all'interno di siti attinenti alla normale attività lavorativa;
- ✓ sono assolutamente vietati i 'download' di software / programmi (fatto salvo casi eccezionali e/o preventivamente autorizzati) in particolare di: file musicali, file video e tutti i file che non rientrano nella normale attività lavorativa;
- ✓ l'utilizzo della posta elettronica deve essere esclusivamente e tassativamente per fini lavorativi: non è consentito l'utilizzo della stessa per scopi personali.

Euro.pa Service srl precisa che, al fine di prevenire eventuali abusi degli strumenti sopra citati (internet e posta elettronica) ha ritenuto necessario dotarsi di strumenti in grado di impedire l'accesso indiscriminato ad alcune categorie di siti non attinenti la sfera professionale ed in particolar modo di bloccare il funzionamento dei servizi di alcuni tra i più diffusi programmi di 'messaggeria istantanea'.

Euro.pa Service srl inoltre ha adottato particolari sistemi in grado di filtrare i messaggi di posta elettronica di provenienza dubbia e/o con domini inclusi in particolari elenchi denominati 'black list' e soprattutto di bloccare i messaggi considerati 'spazzatura' (spam).

Euro.pa Service srl si rende disponibile a rilasciare indirizzi di posta elettronica condivisi tra più dipendenti, affiancandoli a quelli individuali. In questo caso, gli indirizzi privati potranno essere utilizzati solo internamente a Euro.pa Service srl, garantendo così il corretto livello di privacy (esempio: comunicazioni private tra un dipendente e l'ufficio del personale, e viceversa), mentre quelli condivisi potranno essere utilizzati per lo scambio di posta con l'esterno. Euro.pa Service srl invita gli interessati a rivolgersi all'ufficio/responsabile IT.

Euro.pa Service srl informa che attualmente non viene adottato nessun controllo della navigazione in Internet dei dipendenti; tuttavia si riserva in qualsiasi momento e, soprattutto a fronte di particolari circostanze (verifiche di funzionalità, sicurezza dei sistemi, anomalie riscontrate) di effettuare controlli in conformità alla legge in vigore onde evitare il reiterarsi degli abusi degli strumenti informatici aziendali.

Con il presente disciplinare interno Euro.pa Service srl adotta le prescrizioni previste dal provvedimento generale del Garante del 1° marzo 2007 rispetto all'uso di posta elettronica e internet da parte di dipendenti e collaboratori. Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro sull'uso degli strumenti informatici da parte dei dipendenti saranno effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

Tutti i dipendenti e collaboratori sono portati a conoscenza dell'avvenuto adeguamento delle regole inerenti all'utilizzo degli strumenti informatici aziendali mediante la diffusione del presente disciplinare interno. Analogamente viene aggiornata ed integrata l'informativa resa ai dipendenti per renderli edotti delle modalità e finalità di utilizzo dei dati personali.

INTRODUZIONE

Il presente documento si rivolge a tutti i dipendenti di Euro.pa Service srl.

I computer, account di sistema, e-mail, telefoni (inclusi i telefoni portatili), caselle di posta vocale ed altre simili risorse sono di proprietà di Euro.pa Service srl e vengono assegnate per assistere i propri dipendenti nell'esecuzione del loro lavoro giornaliero.

L'obiettivo del presente documento è riepilogare concetti e responsabilità connessi con le principali regole di comportamento alle quali si è chiamati ad attenersi per evitare rischi di tipo informatico nel rispetto della normativa italiana vigente sulla protezione dei dati personali, con particolare riguardo all'utilizzo di Internet e della posta elettronica.

Il documento contiene inoltre l'elenco dei controlli che Euro.pa Service srl si riserva di effettuare in conformità alla legge e le possibili sanzioni disciplinari in cui il dipendente può incorrere.

SCOPO

Il documento si articola nelle seguenti sezioni: '**Accesso al sistema informatico**', '**Utilizzo della postazione di lavoro**, '**Utilizzo dei dispositivi rimovibili**', '**Utilizzo del software**', '**Utilizzo di internet**', '**Utilizzo della Posta elettronica**', **'Utilizzo di telefonia, fax e caselle vocali', 'Sanzioni Disciplinari'**, **'Sistemi di controllo informatici'**, '**Comunicazione Incidenti Informatici**', '**Tutela della Privacy' e 'Classificazione delle informazioni.**

Le ultime due sezioni, "Tutela della Privacy" e "Classificazione delle informazioni", evidenziano la terminologia, i concetti principali e le responsabilità legate al trattamento delle informazioni secondo la normativa vigente in materia di protezione dei dati.

Le altre sezioni riassumono le principali norme comportamentali per il corretto utilizzo delle risorse informatiche da parte dell'utente.

1. ACCESSO AL SISTEMA INFORMATICO

Ogni utente che utilizza una Postazione di Lavoro deve disporre di un codice di accesso personale, non cedibile e costituito da una "*userid*", ovvero codice identificazione utente. Convenzionalmente è utilizzato come "*userid*" l'iniziale del nome seguita dal cognome (MROSSI per Mario Rossi) ed in caso di omonimie, si aggiunge un progressivo numerico (un eventuale Maurizio Rossi verrebbe identificato come MROSSI02, e così via).
La "*userid*" deve essere protetta da password (parola chiave) anch'essa personale, segreta, non comunicabile ad altri.

1.1 Norme di sicurezza e responsabilità

L'uso della coppia di credenziali "*userid*" e "*password*" è strettamente personale e comporta l'assunzione di responsabilità riguardo le azioni dolose e colpose che tale accesso consente. Di seguito sono riepilogate le norme principali relative alla corretta gestione degli userid e delle password.

1.1.1 Userid

- ✓ Il collegamento alla Postazione di Lavoro può avvenire esclusivamente impiegando il proprio "userid". Non è permesso l'utilizzo di utenti generici tipo "ospite" o "guest".
- ✓ E' previsto un numero massimo di tentativi di accesso falliti pari a 5, dopo i quali viene attivato il blocco della userid da parte del sistema di accesso. Il blocco ha una durata di 15 minuti, dopo i quali l'utenza ritorna ad essere disponibile.

1.1.2 password

- ✓ composizione della password:

- deve essere almeno di 8 caratteri
- può contenere qualsiasi carattere (lettere maiuscole, lettere minuscoli, numeri e caratteri di punteggiatura). Attenzione: per il sistema, lettere maiuscole o minuscole sono differenti!
- È bene che non sia una parola di senso compiuto (quindi niente nomi propri, nomi comuni, sigle troppo famose, ecc.).
- La password deve essere cambiata almeno ogni 90 giorni; ogni volta che viene cambiata deve essere completamente differente dalla precedente per evitare sequenze prevedibili; deve essere differente dalle ultime 10 utilizzate precedentemente.
- La password appena cambiata, non può essere ricambiata prima di sette giorni.
- La password non deve assolutamente essere comunicata ad altri e tanto meno scritta su post-it attaccati sul PC, sotto il tavolo o in altri luoghi facilmente accessibili; nel caso si sospetti che la propria password sia conosciuta da altri, è indispensabile sostituirla immediatamente.
- La password iniziale deve essere sostituita al primo collegamento con una password personale.
- In caso di dimenticanza della password o di blocco dell'userid, l'utente deve inoltrare richiesta per la reinizializzazione alla funzione preposta.
- Le password sono immediatamente revocate da ICT quando vengono a cessare le condizioni che ne giustificano l'utilizzo (dimissioni, cambio di attività, ecc.).
- Le considerazioni sopra riportate sulle password di accesso alla Rete sono valide anche per tutte le altre password che permettono di accedere ad altre applicazioni.

2. UTILIZZO DELLA POSTAZIONE DI LAVORO

Gli utenti sono responsabili della buona conservazione delle attrezzature e, nella loro attività, sono tenuti a porre la massima cura per evitare di deteriorare o danneggiare le apparecchiature e causare direttamente o indirettamente spreco di materiali.

L'utente è tenuto a verificare all'inizio della sua sessione di lavoro la regolarità di funzionamento delle apparecchiature e la presenza della dotazione di eventuali periferiche connesse alla postazione di lavoro. L'utente deve segnalare eventuali anomalie al proprio responsabile, che dovrà a sua volta comunicarlo alla funzione preposta.

L'ubicazione delle postazioni di lavoro utente (solitamente all'interno di uffici) viene scelta in modo da ridurre il rischio di un loro impiego abusivo. Euro.pa Service srl adotta ogni cautela per prevenire possibili situazioni potenzialmente pericolose. Ogni dipendente è a sua volta tenuto a segnalare al proprio Responsabile se l'ubicazione della sua postazione lavoro presenti profili di rischio in relazione a mutate situazioni, anche di natura occasionale.

2.1 Norme di sicurezza e responsabilità

Per garantire un livello adeguato di sicurezza per l'utilizzo delle postazioni di lavoro, si elencano le seguenti regole cui è necessario attenersi scrupolosamente:

- utilizzare appropriatamente il servizio informatico o telefonico del quale si necessita e per il quale si è autorizzati rispettando gli scopi ai quali lo stesso è destinato, esclusivamente e tassativamente per fini lavorativi e non a scopo personale;
- segnalare alla funzione preposta e al proprio responsabile ogni accertata violazione delle norme che regolano l'utilizzo delle Postazioni di Lavoro;
- attivare, in caso di necessità di allontanamento dal posto di lavoro, la procedura di blocco della workstation ovvero premere il pulsante "Lock Workstation" dopo aver premuto la

combinazione di tasti CTRL+ALT+CANC o altre combinazioni di caratteri consone col tipo di dispositivo usato (ad esempio, per i thin client la combinazione è CRTL-ALT-INS).

- accedere alla macchina con il proprio userid e la propria password; se la postazione di lavoro è condivisa tra più utenti, ogni utente prima di lasciarla in uso ad un'altra persona deve obbligatoriamente scollegarsi;
- segnalare alla funzione preposta le postazioni di lavoro che non hanno configurata la partenza automatica dello "screen saver" con password dopo 15' di inattività;
- spegnere i personal computer al termine della giornata lavorativa per evitarne usi impropri, utilizzando la procedura di chiusura del sistema operativo (Shutdown), che provvede in automatico alla disconnessione dell'utente dalla rete informatica e alla corretta chiusura della postazione; possono rimanere accesi fuori dall'orario lavorativo solo i PC dedicati a particolari attività autorizzate;
- non utilizzare modem o schede wireless senza autorizzazione specifica; in generale, è fatto divieto di modificare la postazione di lavoro con l'aggiunta di HW e SW non preventivamente autorizzato e concordato con la funzione preposta. Il divieto vale soprattutto per ogni dispositivo USB, facilmente collegabile al PC.
- presidiare le stampanti quando trattano informazioni sensibili o riservate; stampe di informazioni sensibili o riservate possono essere effettuate senza presidio solo se le stampanti sono collocate in area protetta ed inaccessibile a chi non sia autorizzato;
- riporre, quando non utilizzati, i supporti contenenti informazioni sensibili o riservate in contenitori, cassetti o casseforti chiusi a chiave; ciò vale per tutti i supporti informatici (floppy disk, nastri, CD-ROM, DVD, dispositivi rimovibili, ecc.) e non solo per i documenti cartacei;
- non condividere le directory dell'hard disk del proprio PC con altre postazioni utente; per la condivisione di documenti/file è obbligatorio utilizzare i dischi di rete;
- non modificare la configurazione del PC aziendale; per ogni modifica l'utente deve rivolgersi alla funzione preposta",

3. Utilizzo dei Dispositivi Rimovibili

L'utilizzo dei dispositivi di memorizzazione rimovibili (es. chiavi USB, palmari) in ambito aziendale deve essere controllato e ricondotto alle effettive necessità, per evitare i rischi di:

- furto del dispositivo/supporto con la presenza di dati aziendali all'interno;
- potenziale trasmissione di virus, spyware o software malevolo da un PC privato al PC aziendale. Si ricorda comunque che i Personal Computer aziendali sono protetti da software Antivirus e Antispyware costantemente aggiornati.

3.1 Norme di sicurezza e responsabilità

Per garantire un livello adeguato di riservatezza, integrità e disponibilità dei dati memorizzati su dispositivi o supporti rimovibili, si elencano le seguenti regole cui è necessario attenersi scrupolosamente:

- i dispositivi o supporti removibili autorizzati devono essere utilizzati esclusivamente per motivi di lavoro;
- l'eliminazione delle informazioni inutili o obsolete dai dispositivi e dai supporti removibili deve essere effettuata in modo da evitare il permanere di tracce residue che potrebbero essere usate a danno del Gruppo. Nel caso di dispositivi removibili deve essere effettuata una cancellazione del file totale e permanente, mentre nel caso di supporti non riscrivibili (es. CD o DVD non RW) il supporto stesso deve essere fisicamente distrutto prima dell'eliminazione;
- in caso di furto o smarrimento del dispositivo o supporto removibile, si ha l'obbligo di avvisare il proprio Responsabile;
- in caso di dimissioni, quiescenza, il dipendente è tenuto a restituire tutti i dispositivi o mezzi ricevuti in dotazione da Euro.pa Service srl.

4. Utilizzo del Software

4.1 Norme di sicurezza e responsabilità

Per ragioni di sicurezza e di tutela del copyright, gli utenti sono tenuti a osservare le seguenti norme riguardo all'utilizzo del software:

- non è consentito installare software non licenziati da Euro.pa Service srl (giochi, programmi acquistati con le riviste nelle edicole e/o scaricati da Internet, screen saver, ecc.) e che violino le leggi a tutela del copyright.
- non è consentito duplicare o copiare software o altre scritture protette da diritti d'autore;
- non è consentito copiare file di provenienza incerta o esterna su supporti magnetici/ottici per finalità non attinenti alla propria prestazione lavorativa;
- non è consentito cancellare parzialmente o totalmente i programmi consegnati in dotazione con il PC aziendale;
- non è consentito modificare la configurazione del PC aziendale, con particolare riguardo ai programmi di protezione Antivirus e Antispyware;
- non è consentito installare software di rilevazione di vulnerabilità nonché software che permetta di realizzare attacchi informatici;
- non è consentito utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere per finalità illecite il contenuto di comunicazioni e/o documenti informatici;
- non è consentito collocare, anche temporaneamente, nelle aree destinate alla condivisione di informazioni strettamente professionali, file che non siano attinenti allo svolgimento dell'attività lavorativa;
- per utilizzare programmi diversi da quelli in dotazione, l'utente deve rivolgersi alla funzione preposta; ogni nuovo software, o aggiornamento deve essere installato esclusivamente dal personale addetto.

5. Utilizzo del Internet

Il servizio viene erogato tramite dei server centralizzati in Euro.pa Service srl, chiamati "proxy". Per esigenze tecnologiche e di sicurezza le richieste di accesso a internet da parte degli utenti vengono memorizzate in un file di log, che periodicamente con cadenza settimanale ed automaticamente viene cancellato attraverso procedure di sovra registrazione.

Internet costituisce il principale mezzo attraverso cui i personal computer possono essere infettati da software malevolo (es. virus, worm, cavalli di Troia, spyware, adware, keylogger, ecc.), contenuto in file scaricati da pagine internet o allegati trasmessi via posta elettronica.

Il software malevolo, noto anche come "malicious software", "malware", "codice dannoso" o "codice nocivo", è un software realizzato e veicolato espressamente per raggiungere almeno uno dei seguenti obiettivi:

- danneggiare seriamente il computer e i dati in esso contenuti;
- rallentare il funzionamento del computer o la connessione a Internet;
- utilizzare il computer per diffondersi su altri computer;
- carpire, all'insaputa dell'utente, le sue credenziali di accesso a sistemi/applicazioni o altre informazioni, quali ad esempio i siti internet visitati, o altri dati personali sensibili o riservati.

5.1 Norme di sicurezza e responsabilità

- Ai fini della sicurezza, su tutti i Personal Computer deve essere attivo il software di protezione fornito, che comprende il modulo Antivirus, Antispyware e il Personal Firewall. Per garantire il massimo livello di sicurezza, il software antivirus distribuito sui client è costantemente aggiornato in tempo reale da un motore centrale, che è collegato

permanentemente con il fornitore del prodotto per recepire, sempre in tempo reale, ogni implementazione necessaria a debellare eventuali vulnerabilità.

Questi software non devono quindi essere disabilitati sui client.

- Il Servizio di connessione a Internet è fornito gratuitamente da Euro.pa Service srl la cui responsabilità, in qualità di provider, è regolata dal D. Lgs. 70/2003.
- L'utente ha l'obbligo di utilizzare Internet esclusivamente per scopi consentiti dalle leggi vigenti rispettando le regole di sicurezza e le norme di comportamento indicate nel presente documento.

  In particolare:

  - La navigazione internet è consentita solo all'interno dei siti attinenti alla normale attività lavorativa
  - sono assolutamente vietati i download di file musicali, file video, software/programmi (fatto salvo casi eccezionali e/o preventivamente autorizzati) e di tutti i file che non rientrano nella normale attività lavorativa
  - non è consentito effettuare transazioni finanziarie tramite Internet, ivi comprese le operazioni di trading on-line, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione aziendale e con il rispetto delle normali procedure di acquisto
  - va evitata ogni forma di registrazione, anche a titolo personale, in siti i cui contenuti non siano legati all'attività lavorativa
  - non è consentito partecipare per motivi non professionali a forum, utilizzare chat-line, bacheche elettroniche e registrazioni in guest book anche utilizzando pseudonimi; l'accesso a simili fonti di informazione, se effettuato esclusivamente per motivi professionali, potrà avvenire solo previa autorizzazione scritta da parte della Direzione
- Si precisa che Euro.pa Service srl non mette a disposizione alcuna modalità di accesso personale ad internet nemmeno dietro pagamento o fatturazione a carico dell'interessato
- Ad ogni singolo utente viene richiesto un comportamento rispettoso dell'etica e delle norme non scritte che regolano la rete (Netiquette).
- L'utente è direttamente responsabile, civilmente e penalmente, a norma delle leggi vigenti, dell'uso fatto durante la navigazione. Tale responsabilità si estende anche alla violazione delle norme sul diritto d'autore, alla diffamazione, avvenuta mediante l'invio di materiale offensivo su un sito della rete; alla violazione delle norme sul buon costume e contro lo sfruttamento sessuale dei minori, con la pubblicazione di materiale pornografico con minori; alla violazione delle norme sull'ordine pubblico, con la pubblicazione, ad esempio, di materiale di stampo terroristico; alla violazione del diritto alla riservatezza, alla concorrenza sleale, nel caso di informazioni false o diffamatorie messe in rete tra imprese concorrenti; alla violazione delle norme sulla protezione dei marchi degli accessi protetti, delle licenze d'uso, delle regole di copyright.
- Euro.pa Service srl all'utente, qualora la Pubblica Autorità denunci un uso improprio dei Servizi da parte dell'utente stesso oppure nel caso in cui venga accertato un traffico anomalo o un uso del Servizio contrario alle leggi, ai regolamenti o alla policy di utilizzo.
- L'utente, nel caso in cui riscontri un malfunzionamento o un problema di aggiornamento nel software di protezione antivirus del proprio Pc, è tenuto ad attivare tempestivamente la funzione preposta per il ripristino della corretta funzionalità.
- L'utente, nel caso in cui riscontri un'anomalia dovuta a probabile infezione da virus del proprio Pc, è tenuto ad attivare tempestivamente alla funzione preposta.

5.2 Controlli

Nel pieno rispetto delle norme che disciplinano il rapporto di lavoro e delle vigenti disposizioni in materia di privacy, Euro.pa Service srl si riserva la possibilità di effettuare dei controlli mirati sul log del proxy per il riscontro di anomalie nella funzionalità del servizio, la verifica di eventuali abusi o su richiesta delle pubbliche autorità. Le informazioni memorizzate nel file di log vengono registrate secondo un tracciato che impedisce l'identificazione immediata del singolo utente. Il file di log è accessibile solo a un ristretto numero di amministratori dei sistemi proxy.

Gli eventuali controlli da parte di Euro.pa Service srl verranno effettuati con gradualità. In prima battuta verranno effettuate verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrà passare a controlli su base individuale.

6. Utilizzo della Posta Elettronica

In ragione dell'attività svolta da Euro.pa Service srl, tutti i dipendenti sono dotati di una casella di e-mail aziendale.
Si ricorda che l'e-mail aziendale è da considerarsi uno strumento di lavoro ed è quindi importante osservare alcuni comportamenti al fine di preservarne l'integrità e il funzionamento. La casella di posta elettronica aziendale deve quindi contenere soltanto messaggi attinenti all'attività lavorativa svolta e non corrispondenza privata.
Per particolari esigenze di business, Euro.pa Service srl mette a disposizione indirizzi di posta elettronica condivisi intestati all'unità organizzativa, rendendo così chiara la natura non privata della corrispondenza.
Euro.pa Service srl mette inoltre a disposizione di ciascun utente apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenza programmate (es. per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" di altri colleghi a cui rivolgersi, oppure dell'indirizzo di posta condiviso dall'unità organizzativa.
In caso di prolungata assenza non programmata o impedimento del dipendente, quando sia indispensabile e indifferibile intervenire per esclusive necessità di operatività aziendale e di sicurezza del sistema, il Responsabile dell'Ufficio, agendo in qualità di fiduciario, può richiedere l'accesso alla casella di e-mail della persona assente, al fine di recuperare informazioni strettamente necessarie all'attività lavorativa, avvisando comunque l'interessato e l'Ufficio Sicurezza.
Si ricordano i principali comportamenti da evitare nell'impiego dello strumento, ovvero:

- evitare di utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza e necessità; tale divieto include l'uso di allegati compressi contenenti materiale extra lavorativo.
- evitare di installare programmi di natura incerta magari pervenuti via posta elettronica;
- evitare di rispondere a messaggi a rischio di "Phishing", una pratica che ha come finalità il furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli opportunamente creati per apparire autentici. L'utente è solitamente invitato a visitare il sito evidenziato nel messaggio con la scusa di dover confermare dei dati. L'utente è perciò ingannato e portato a rivelare dati, come ad esempio il numero del proprio conto corrente, nome utente e password, numero di carta di credito, ecc. Queste informazioni vengono memorizzate dal sito Web e quindi inviate a potenziali malintenzionati. Per difendersi dal "Phishing" è sufficiente cancellare il messaggio di posta elettronica ed evitare di collegarsi ai siti segnalati nello stesso. In caso di dubbio è sempre bene contattare l'Ente che apparentemente ha inviato il messaggio per accertarsi della reale provenienza dello stesso;
- evitare di aprire messaggi di posta elettronica ed eseguire file allegati ai messaggi di provenienza dubbia;
- evitare di inoltrare messaggi di posta alimentando "catene di Sant'Antonio";
- evitare di rispondere a messaggi di posta "non sollecitati" ovvero provenienti da mittenti sconosciuti chiedendo magari di essere cancellati da quella lista di invio; così facendo si conferma, a chi ha spedito il messaggio, l'esistenza effettiva del proprio indirizzo di e-mail esponendosi di fatto ad ulteriori e continui invii.

6.1 Controlli

Il servizio viene erogato tramite dei server di posta centralizzati. Solo in caso di accesso via Web alla casella di posta elettronica è prevista la memorizzazione delle informazioni in un file di log, che viene periodicamente ed automaticamente cancellato, con cadenza settimanale, attraverso procedure di sovra registrazione.

Tali informazioni sono accessibili solo agli amministratori dei sistemi di posta elettronica e possono venire accedute solo in casi particolari (es. per la rilevazione di anomalie) o su richiesta delle pubbliche autorità.
Gli eventuali controlli da parte di Euro.pa Service srl devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrà passare a controlli su base individuale.

7. Utilizzo di telefonia, fax e caselle vocali

L'utilizzo di telefoni, fax e caselle vocali forniti da Euro.pa Service srl deve essere limitato alle comunicazioni necessarie per lo svolgimento del lavoro, salvo casi eccezionali; il dipendente è tenuto a limitare la ricezione di telefonate personali sulle linee telefoniche, avendo cura di contenere la durata delle conversazioni al minimo indispensabile.

7.1 Telefonia fissa

In ragione dell'attività svolta da Euro.pa Service srl o, tutti i dipendenti sono dotati di un telefono fisso aziendale.
Il servizio di telefonia fissa viene erogato con un unico profilo di abilitazione che permette ogni tipologia di chiamata (urbana, interurbana, internazionale e verso cellulari). Solo i numeri "speciali" quali 199, 166, ecc. sono inibiti.

7.2 Telefonia mobile

Il cellulare aziendale viene dato su richiesta de preposti e previa approvazione del datore di Lavoro. Con il cellulare aziendale non sono consentite telefonate personali, a meno che il cellulare non disponga dei una SIM "DUAL RAM".

7.3 Fax

Ogni fax inviato o ricevuto che riguardi o contenga impegni per Euro.pa Service srl deve essere visionato e autorizzato dal responsabile direzione/area/ufficio che effettua la comunicazione.
Gli impiegati che usano il facsimile devono verificare il numero di fax del destinatario a cui desiderano inviare le informazioni e verificarne l'avvenuta ricezione da parte del destinatario.

Non devono essere inviati dati riservati a mezzo fax senza la dovuta autorizzazione. Qualora avvenisse un invio o ricezione di fax contenenti dati riservati, l'apparecchio deve essere tenuto sotto osservazione dal dipendente nel momento in cui il fax viene inviato o ricevuto.

I fax inviati o ricevuti non devono essere lasciati incustoditi nei pressi dell'apparecchio.

8. Sanzioni Disciplinari

Ogni singolo dipendente è tenuto al rispetto di queste norme comportamentali.
Dalla violazione di tali norme, a seconda della gravità delle infrazioni commesse, delle relative conseguenze specifiche e delle circostanze obiettive in cui si verificano, potrà derivare:

- L'applicazione delle sanzioni disciplinari previste dal CCNL applicato;
- il licenziamento per notevole inadempimento degli obblighi contrattuali a norma dell'art. 3 della legge 15 luglio 1966, n. 604;
- il licenziamento per giusta causa a norma dell'art. 2119 C.C.

<u>Sanzioni disciplinari</u>

Ai sensi del CCNL di categoria, le infrazioni dei dipendenti possono dar luogo all'applicazione dei seguenti provvedimenti disciplinari:

a. il rimprovero verbale;
b. il biasimo inflitto per iscritto;
c. la multa

la sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni.

Applicazione delle sanzioni disciplinari

A) Il rimprovero verbale ed il biasimo inflitto per iscritto saranno applicati in caso di mancanze di lieve entità, a seconda della rilevanza delle conseguenze e a seconda delle circostanze obiettive in cui le infrazioni sono commesse.
B) La multa e la sospensione dal servizio e dal trattamento economico, da uno a dieci giorni, sarà applicata in caso di mancanze più gravi, a seconda della rilevanza delle conseguenze e a seconda delle circostanze obiettive in cui le infrazioni sono commesse.
C) Tenuto conto della gravità dei fatti medesimi, delle modalità e circostanze di effettuazione delle mancanze, e tenuto anche conto di eventuali recidive, può essere ritenuto applicabile il licenziamento per giusta causa o giustificato motivo.

Procedure per l'applicazione delle sanzioni disciplinari

Prima di deliberare i provvedimenti disciplinari del "biasimo inflitto per iscritto" e della "sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni", l'impresa contesta per iscritto la mancanza all'interessato il quale può presentare, entro 15 giorni, le proprie difese scritte, anche tramite l'organizzazione sindacale cui aderisce o conferisce mandato.
Qualora decida di adottare un provvedimento, l'Impresa lo comunicherà all'interessato entro i successivi 15 giorni oppure entro 15 giorni dal ricevimento delle eventuali difese scritte presentate dal lavoratore.
Per esigenze derivanti da difficoltà nella fase di valutazione delle difese scritte del lavoratore, il termine di cui al comma precedente sarà prorogato di 15 giorni purché l'impresa ne dia comunicazione scritta al lavoratore stesso.
Il provvedimento della "sospensione dal servizio e dal trattamento economico" deve essere comunicato dall'Impresa all'organizzazione sindacale cui aderisce l'interessato.

Licenziamento per giustificato motivo

Sarà applicato per grave violazione delle norme e dei doveri inerenti alle direttive di Euro.pa Service srl in merito, tenuto conto della particolare natura della mancanza e/o della sua recidività.

Alla risoluzione del rapporto di lavoro di cui al capoverso precedente sono estese le procedure previste per i provvedimenti disciplinari dall'art. 7 della legge 20 maggio 1970, n. 300.
Licenziamento senza preavviso
Il licenziamento senza preavviso sarà applicato nei casi di mancanze così gravi da non consentire la prosecuzione, anche provvisoria, del rapporto di lavoro, per il venir meno del peculiare elemento fiduciario che sta a fondamento del rapporto stesso.

Sospensione cautelare

Quando sia richiesto dalla natura della mancanza o dalla necessità di accertamenti in conseguenza della medesima, l'Impresa, in attesa di deliberare l'eventuale provvedimento può disporre, dalla data di comunicazione della contestazione e comunque non oltre cinque giorni dalla ricezione della eventuale risposta del lavoratore/lavoratrice, la sospensione temporanea dal servizio per il tempo strettamente necessario, fermo restando la corresponsione degli emolumenti.

9. Sistemi di controllo informatici

Per quanto riguarda i sistemi di controllo informatici, sui personal computer degli utenti è installato uno strumento di controllo remoto della postazione, accessibile solo dagli operatori di Help Desk per interventi di manutenzione e ripristino guasti a distanza. L'accesso al pc dell'utente viene effettuato soltanto su richiesta dell'utente stesso e richiede ogni volta un esplicito consenso da parte di quest'ultimo attraverso accettazione di una finestra di "pop-up".

Euro.pa Service srl tiene a precisare che:

- non viene effettuata alcuna riproduzione sistematica delle schermate internet visualizzate dal lavoratore
- non viene effettuata alcuna lettura/ registrazione di caratteri inseriti tramite tastiera o analogo dispositivo
- non viene effettuato nessun tipo di analisi occulta di computer portatili affidati in uso
- non viene effettuata alcuna lettura/registrazione sistematica dei messaggi di posta elettronica né dei relativi dati esteriori relativi ai messaggi stessi.

10. Comunicazione Incidenti Informatici

Qualora il dipendente dovesse avere evidenza di comportamenti ritenuti anomali e/o comunque al di fuori della normale operatività (segnalazioni di virus, accesso non autorizzato a postazioni di lavoro o sistemi, ricezione di mail "strane", ecc.) deve avvisare la funzione preposta al fine di valutare il reale impatto del fenomeno osservato.

11. Tutela della privacy

Sono di seguito riepilogati i termini e i concetti fondamentali relativi al trattamento delle informazioni a tutela della Privacy.

- Il termine Privacy si riferisce al rispetto dei diritti, delle libertà fondamentali e della dignità di ogni persona fisica, con particolare riferimento ai diritti alla riservatezza e all'identità personale. La tutela della Privacy è regolamentata dal **Codice in materia di protezione dei dati personali (D.Lgs 196/03)**, che ha riunito in un unico testo le disposizioni legislative.
- Si definisce "**dato personale**" qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione. Alcuni dati personali sono "**dati comuni**" e soggetti agli obblighi generali della legge. Si tratta per esempio di: nome, cognome e indirizzo, codice fiscale, ragione sociale o partita Iva. Ci sono però altri dati personali, i "**dati sensibili**" e i "**dati giudiziari**", per i quali la legge prevede una disciplina particolare. Si tratta per esempio delle informazioni riguardanti lo stato di salute, l'origine razziale ed etnica, le convinzioni filosofiche o religiose, l'appartenenza a un sindacato, a un partito politico, oppure dei dati idonei a rivelare provvedimenti di carattere giudiziario.
- La normativa italiana sulla Privacy disciplina la sicurezza dei dati disponendo che i dati personali devono essere **custoditi e controllati**. Questo comportamento deve essere osservato per ridurre al minimo i rischi di:
  - distruzione o perdita dei dati, anche accidentale;
  - accesso non autorizzato ai dati;
  - trattamento dei dati non consentito o non conforme alle finalità della raccolta.
- Il contenimento di questi rischi deve essere raggiunto mediante l'adozione di **idonee e preventive misure di sicurezza**, riassunte nel presente documento.
- In relazione al D.Lgs. 196/2003, ogni anno la società riassume in un documento specifico, detto "**Documento Programmatico di Sicurezza"**, per se stessa e per le compagnie alle quali fornisce servizi informatici, tutte le misure di sicurezza logica e fisica adottate per la tutela della privacy e le relative responsabilità.

12. Classificazione delle informazioni

Le informazioni disponibili all'interno di Euro.pa Service srl sono classificabili secondo tre livelli:

- **pubblico**: informazione di carattere pubblico che non possiede particolari requisiti di riservatezza;
- **interno:** informazione interna i cui requisiti di riservatezza rispetto al personale esterno sono importanti ma non fondamentali;

- **riservato:** informazione che possiede elevati requisiti di segretezza; se trasmessa elettronicamente, da personale autorizzato, deve essere protetta da crittografia.