



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

REGOLAMENTO AZIENDALE INERENTE LE MODALITA' DI UTILIZZO DELLA POSTA ELETTRONICA E DI INTERNET DA PARTE DEI DIPENDENTI DELLA AZIENDA U.S.L. DI PESCARA

Art. 1 Oggetto e finalità

1. Il presente Regolamento è redatto: alla luce della Legge 20.5.1970, n. 300, recante “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale nei luoghi di lavoro e norme sul collocamento”; del Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, adottata dal Gruppo di lavoro sulla protezione dei dati (Articolo 29), in data 29 maggio 2002; in attuazione del Decreto Legislativo n. 196 del 23 giugno 2003, recante “Codice in materia di protezione dei dati personali” (d’ora in avanti Codice); della Direttiva del 24.2.04 del Ministero per l’innovazione e le tecnologie ove si introduceva l’obbligo per la Pubblica Amministrazione di utilizzare l’e-mail non solo per le comunicazioni interne e tra amministrazioni ma soprattutto nei rapporti con i cittadini; della Circolare interna dell’Ufficio Privacy n. 5 del 23.2.2006 recante: “corretta trasmissione dei dati sensibili ai sensi dell’art. 22 del D.Lgs.n. 196/2003 e del comma 24 dell’All. B (Disciplinare Tecnico in materia di Misure Minime di Sicurezza)”; del Provvedimento del Garante per la protezione dei dati personali, del 01 marzo 2007, recante “Lavoro: le linee guida del Garante per posta elettronica e internet”; del mansionario ad uso del soggetto nominato incaricato n. 1856 del 29 Gennaio 2007 e del Documento per la Sicurezza adottato con delibera AUSL Pescara n. 140 del 28 marzo 2007.

2. La finalità è quella di verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet, muovendo dalla considerazione che prevenire gli abusi debba considerarsi più importante che individuarli.

Art. 2 Principi generali

1. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel D.Lgs.vo 196/03, e, precisamente:

a) **il principio di necessità** per il quale: l’utilizzo dei dati personali, attraverso l’impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite;

b) **il principio di correttezza**, per il quale: le caratteristiche essenziali dei trattamenti, siano essi svolti in modalità cartacea od informatica oppure mista: cartacea ed informatica, devono essere partecipate ai lavoratori;

c) **le finalità** alla base del trattamento dei dati personali devono essere: determinate, esplicite e legittime, oltre che pertinenti e non eccedenti.

2. E’ riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall’Amministratore di Sistema o dal personale delegato dall’Amministratore di Sistema, sempre nel rispetto della citata normativa.



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

Art. 3 Tutela del lavoratore

1. Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
2. E' garantito al singolo lavoratore il diritto di accesso ai dati personali che lo riguardano, nei modi stabiliti con Regolamento sull'esercizio del diritto di accesso ai dati personali trattati dalla Azienda, giusta Delibera n. 1182 del 24 agosto 2005 che ha modificato la Delibera n. 271/2004.

Art. 4 Corretto utilizzo di Internet

1. L'accesso alla rete aziendale è protetto da password; per l'accesso devono essere utilizzati User name e password assegnate dal C.E.D. (**Centro Elaborazione Dati**). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza
2. L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC 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. E' ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa, il cui accesso è consentito dal proxy aziendale con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti: del Ministero della Sanità, delle Università, degli Enti locali.
4. E' vietato compiere azioni che siano potenzialmente in grado di arrecare danno alla Azienda, ad es, il download o l'upload di file musicali, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.
5. E' fatto divieto all'utente il download di qualunque tipo di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema.
6. L'Azienda si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist internazionali in continuo aggiornamento e di predisporre filtri tali da prevenire determinate operazioni. Ciò per ridurre l'uso improprio della 'navigazione' in Internet.
7. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e dal C.E.D., con il rispetto delle normali procedure di acquisto.
8. E' assolutamente vietato l'utilizzo di abbonamenti privati (connessioni analogiche e non) per effettuare la connessione a internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema o del Management Aziendale previo parere tecnico dello stesso Amministratore.
9. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

Art. 5 Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le stesse regole di utilizzo previste per i Pc fissi connessi in rete, con particolare attenzione alla rimozione di eventuali file che non devono essere salvati o archiviati.
3. I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto
4. Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari
5. Nel caso di accesso a Internet tramite la rete aziendale:
 - utilizzare l'accesso in forma esclusivamente personale
 - utilizzare la password in modo rigoroso
6. Disconnettersi dalla rete aziendale al termine della sessione di lavoro
7. Collegarsi periodicamente alla rete interna per consentire l'aggiornamento dell'anti virus
8. Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

Art. 6 Corretto utilizzo della posta elettronica

1. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn).
2. Non è consentito diffondere messaggi del tipo "catena di s. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo;
3. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non sia possibile attivare la funzione autoreply o l'inoltro automatico **su altre caselle aziendali** e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;
4. Evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif, in qualunque altra situazione di incertezza contattare l'Amministratore di Sistema o il C.E.D.

Art. 7 Controlli disposti dalla Azienda

1. Nel rispetto dei principi di **pertinenza e di non eccedenza** ed evitando una interferenza ingiustificata **sui diritti e sulle libertà fondamentali dei lavoratori**, così come la possibilità di



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

controlli prolungati, costanti o indiscriminati, la Azienda si riserva di effettuare controlli sull'uso degli strumenti elettronici.

2. Detti controlli saranno svolti dal personale in servizio presso il centro Elaborazione Dati della azienda, con la supervisione dell'Amministratore di Sistema.

3. Il controllo scaturirà dalla necessità di dovere effettuare verifiche sulla funzionalità e sicurezza del sistema oltre che dal rilevamento di anomalie nell'utilizzo delle Rete.

4. Il controllo sarà svolto, in via preliminare, su dati aggregati relativi, a seconda dei casi, all'Azienda, al Presidio Ospedaliero, al Servizio, al Distretto Socio Sanitario di Base, all'Unità Operativa, all'Ufficio.

5. Nell'ipotesi in cui da tale forma di controllo anonimo dovesse scaturire un utilizzo anomalo degli strumenti aziendali, l'Azienda emetterà un invito – rivolto **ai Dirigenti, e per il loro tramite, ai dipendenti** afferenti alla realtà lavorativa interessata - di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

6. Qualora la anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo l'Azienda procederà ad effettuare controlli su base individuale.

Art. 8 Conservazione dei dati

1. In riferimento al documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro con nota WP55 del 29/05/2002 redatta dal Gruppo di Lavoro sulla Protezione dei Dati – Articolo 29, in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro tre mesi dalla loro produzione.

2. In casi eccezionali – ad es.: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

3. La Azienda si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

Art. 9 Sanzioni disciplinari

1. Si rimanda all'atto deliberativo n. 412 del 23 aprile 2008, recante “ Ulteriore provvedimento in ordine all'atto deliberativo n. 1028/2004 avente per oggetto: recepimento normativa modificatoria di settore in materia disciplinare” e all'art. 7 della Legge n. 300 del 20 maggio 1970, che si allega al presente Regolamento, oltre che alle disposizioni contenute nel Codice Civile.



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

Art. 10 Disposizioni finali

1. Il presente Regolamento è stato redatto dall'Ufficio Aziendale per la Privacy, (previa acquisizione, per quanto di competenza, dei pareri del Dirigente Ufficio Gestione Risorse Umane e del Dirigente del Servizio Informativo Aziendale), che è chiamato a garantire il coordinamento degli adempimenti.
2. Il suddetto regolamento è stato sottoposto al vaglio della RSU aziendale che ha espresso parere favorevole in merito al suo contenuto ed è stato sottoposto alla approvazione del Direttore Generale che lo ha approvato con atto deliberativo. Il suo contenuto è soggetto ad aggiornamento periodico.
3. La sua pubblicizzazione, a cura dell'Ufficio Privacy, avverrà nelle seguenti forme: trasmissione per posta interna a tutti i Dirigenti Responsabili di P.O., D.S.S.B., R.S.A, Dipartimenti e Uffici di Staff; attraverso la rete informatica interna, il sito aziendale, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.
4. E' fatto obbligo a chiunque spetti di osservarlo.

Legenda

Amministratore di Sistema - E' il gestore di una rete (LAN), solitamente connessa ad Internet. Alcune operazioni effettuate dall'amministratore sono: * verifica del corretto funzionamento della rete locale; * ricambio delle schede di rete; * installazione programmi; * gestione delle pagine web; * gestione dell'email degli user, delle newsgroup, ecc.; * limitazione dei diritti di accesso ai file (directory comprese); * definisce quali operazioni possono essere eseguite dagli utenti, la quota (massimo spazio disponibile per memorizzare nell'unità di massa i file dell'utente); * effettuare ogni tipo di operazione su qualsiasi risorsa degli utenti grazie all'accesso root; * suggerire la risoluzione dei problemi più comuni, relativi alla connessione e al regolare funzionamento del sistema.

Bcc o Ccn - Gli indirizzi dei destinatari diretti (To:) e di quelli in copia conoscenza (Cc:) sono ugualmente visibili a tutti i destinatari. La scelta di mettere un destinatario in uno dei due campi è legata al ruolo che le persone hanno riguardo all'argomento del messaggio. Ad esempio, se un messaggio richiede di eseguire un compito, si intende che si chiede a chi è destinatario diretto di eseguirlo, mentre i destinatari in copia conoscenza sanno che questa richiesta è stata fatta, ma non ci si aspetta che siano loro ad eseguire il compito.

Gli indirizzi dei destinatari in copia conoscenza nascosta non appaiono nel messaggio consegnato ai destinatari. Questo consente di fatto di far sapere a terzi che cosa si sta dicendo e a chi senza che i destinatari ufficiali ne siano a conoscenza. 'Mettere in CC' o 'in CCN' è locuzione diffusa negli ambienti lavorativi e nei gruppi sociali organizzati. Quando l'e-mail viene utilizzata per diffondere messaggi a molte persone che non si conoscono tra loro (ad esempio comunicati pubblici, annunci, messaggi spiritosi più o meno utili), il fatto che ciascun destinatario possa sapere chi sono gli altri destinatari e i loro indirizzi non è in generale opportuno, per ragioni di privacy e di sicurezza.

In particolare, se si invia un messaggio ad un gran numero di persone che non necessariamente si conoscono tra di loro, costoro non necessariamente saranno d'accordo che il loro indirizzo, ed il fatto che hanno ricevuto quel messaggio, sia reso noto ad estranei. Inoltre, molti worm si propagano per e-mail, e utilizzano gli indirizzi presenti nei messaggi per diffondersi. Inviare un messaggio con



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

gli indirizzi dei destinatari in chiaro significa quindi esporre tutti i destinatari ad un ulteriore rischio di contagio se uno di loro viene contagiato.

Per ovviare a questo problema, è consigliabile utilizzare in questi casi il Bcc:, oppure una mailing list.

Chat line - Il termine chat (in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che in paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima. Il "luogo" (lo spazio virtuale) in cui la chat si svolge è chiamato solitamente chatroom (letteralmente "stanza delle chiacchierate"), detto anche channel (in italiano canale), spesso abbreviato chan.

Download o upload - In generale con questo termine si intende il trasferimento di dati da un computer locale a uno remoto utilizzando un apparato di comunicazione, ad es. il modem, o tra computer della stessa rete. Per download si intende anche la visualizzazione sul proprio computer di una pagina internet.

Guest book - Fornisce ai visitatori l'opportunità di lasciare commenti (sul sito) per i nuovi utenti che entreranno nel sito

Proxy - Un proxy è un programma che si interpone tra un client ed un server, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client. In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software.

Remote banking - Per remote banking si intende l'insieme di servizi automatizzati che permettono ai clienti, grazie all'uso di terminali o di un semplice telefono, di collegarsi alla banca presso la quale intrattengono il conto corrente ed effettuare una serie di operazioni bancarie oppure di ricevere informazioni in tempo reale. A seconda del mezzo di comunicazione utilizzato si può parlare di phone banking ed internet banking

***.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif** - Si tratta di estensioni di file che mandano in esecuzione file eseguibili che, a loro volta, possono infettare il computer con un virus.



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

LEGGE 20 maggio 1970, n. 300 (Statuto dei lavoratori) Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento.

ART. 4 - Impianti audiovisivi.

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

ART. 7. - Sanzioni disciplinari.

Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato. Fermo restando quanto disposto dalla legge 15 luglio 1966, n. 604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni. In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa. Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna



www.ausl.pe.it

AZIENDA UNITA' SANITARIA LOCALE DI PESCARA UFFICIO PRIVACY

Tel. 085/8276374

E-mail: ufficioprivacy@ausl.pe.it

delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.

Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivolto dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto. Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio.

Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione.