ORIGINALE

AZIENDA U.S.L.
PESCARA

Il giorno 12 GEN. 2016 nella sede dell'Unità Sanitaria Locale di Pescara.

IL DIRETTORE GENERALE

dr. Claudio D'Amario, nominato dalla Giunta Regionale con deliberazione n. 46 del 30/01/2012 acquisiti i pareri allegati del Direttore Amministrativo e del Direttore Sanitario, ha adottato il seguente provvedimento su proposta del Direttore dell'U.O.C. AFFARI GENERALI E LEGALI e del Dirigente Responsabile U.O.S.D. SISTEMI INFORMATIVI E TELECOMUNICAZIONI:

N. 23

OGGETTO: **APPROVAZIONE DEL REGOLAMENTO AZIENDALE INERENTE LE MODALITA' DI UTILIZZO DELLA POSTA ELETTRONICA, DI INTERNET E DEGLI STRUMENTI INFORMATICI DA PARTE DEL PERSONALE DELLA AZIENDA U.S.L. DI PESCARA PER RENDERE LA PRESTAZIONE LAVORATIVA. REVOCA DELLA DELIBERA N. 891 DEL 25.7.2015**

IL DIRETTORE GENERALE

- Letta e condivisa l'allegata relazione del Titolare P.O. "Privacy e Trasparenza", dott. Giovanni Modesti, e del Collaboratore Tecnico Professionale Informatico, dott. Antonio Montese a fondamento del presente provvedimento del quale costituisce parte integrante e sostanziale;
- Visto il D. Lgs. n. 196/2003 e s.m.i.;
- Visti la Legge 10 dicembre 2014, n. 183;
- Visto il Decreto Legislativo n. 151 del 14 settembre 2015;
- Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario per quanto di rispettiva competenza;

DELIBERA

1. Di revocare la Delibera n. 891 del 25.7.2008, recante "Regolamento aziendale inerente le modalità di utilizzo della posta elettronica e di Internet";
2. Di approvare l'allegato "Regolamento aziendale inerente le modalita' di utilizzo della posta elettronica, di internet e degli strumenti informatici da parte del personale della Azienda U.S.L. di Pescara per rendere la prestazione lavorativa";
3. Di conferire al presente provvedimento, per ragioni di urgenza, la clausola di immediata esecutività;
4. Di pubblicare il presente provvedimento nell'Albo pretorio della Asl, ai sensi del D.Lgs. n. 33/2013.

Allegato A Originale

Il Titolare P.O. "Privacy e Trasparenza", dott. Giovanni Modesti, e il Collaboratore Tecnico Professionale Informatico, dott. Antonio Montese, formulano la seguente proposta:

Visti:
Il 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;
Il Decreto Legislativo n. 196 del 23 giugno 2003, recante "Codice in materia di protezione dei dati personali" (d'ora in avanti Codice);
Il 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";
Il Provvedimento del Garante per la protezione dei dati personali, del 1.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, recante il seguente oggetto "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori";
La Direttiva n. 2/09 del 26.5.2009 della Presidenza del Consiglio dei Ministri – Dip. Funz. Pubblica la quale rileva che l'utilizzo delle tecnologie informatiche costituisce ormai il principale strumento di lavoro a disposizione dei dipendenti delle pubbliche amministrazioni e, pertanto, riconosce da un lato alle PP.AA., in quanto datori di lavoro, l'obbligo di assicurare la funzionalità e il corretto utilizzo degli strumenti informatici da parte dei lavoratori, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici; dall'altra riconosce all'Amministrazione il potere di controllo sul corretto utilizzo di tali mezzi, nel rispetto di alcune regole e principi generali quali il principio di proporzionalità, cioè di pertinenza e non eccedenza delle attività di controllo; di rispetto delle procedure di informazione/consultazione delle rappresentanze dei lavoratori; della preventiva informazione ai lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere dati personali."
Il Documento di valutazione dei rischi (DUVRI) adottato con delibera AUSL Pescara n. 375 del 26 marzo 2015;
La Legge 10 dicembre 2014, n. 183 e il Decreto Legislativo n. 151 del 14 settembre 2015, recante "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità".
Considerato che:
l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi dettati dal D.Lgs. 7 marzo 2005, n. 82 e dal D.P.R. 16 aprile 2013, n. 62 recante il Codice di comportamento dei dipendenti pubblici a norma dell'art. 54 del D.Lgs. 30 marzo 2001, n. 165;
Vista:
la Delibera n. 891 del 25.7.2008, recante "Regolamento aziendale inerente le modalità di utilizzo della posta elettronica e di Internet";
Attesa:
alla luce della nuova normativa di settore sopra richiamata, la necessità di dovere procedere alla revoca della Delibera n. 891 del 25.7.2008 ed alla redazione del nuovo Regolamento aziendale inerente le modalita' di utilizzo della posta elettronica, di internet e degli strumenti informatici da parte del personale della Azienda U.S.L. di Pescara per rendere la prestazione lavorativa;

PROPONGONO

1. Di revocare la Delibera n. 891 del 25.7.2008, recante "Regolamento aziendale inerente le modalità di utilizzo della posta elettronica e di Internet";
2. Di approvare l'allegato Regolamento aziendale inerente le modalita' di utilizzo della posta elettronica, di internet e degli strumenti informatici da parte del personale della Azienda U.S.L. di Pescara per rendere la prestazione lavorativa;
3. DI conferire al presente provvedimento, per ragioni di urgenza, la clausola di immediata esecutività.

Il Titolare P.O. "Privacy e Trasparenza"
Dott. Giovanni Modesti

Il Collaboratore Tecnico Professionale Informatico
Dott. Antonio Montese

REGOLAMENTO AZIENDALE INERENTE LE MODALITA' DI UTILIZZO DELLA POSTA ELETTRONICA, DI INTERNET E DEGLI STRUMENTI INFORMATICI DA PARTE DEL PERSONALE DELLA AZIENDA U.S.L. DI PESCARA PER RENDERE LA PRESTAZIONE LAVORATIVA.

Art. 1

Oggetto e finalità

1) Il presente Regolamento disciplina l'utilizzo degli strumenti informatici (postazioni di lavoro fisse e mobili, posta elettronica, Internet ed Intranet) che l'azienda U.S.L. di Pescara mette a disposizione del personale e si pone la finalità di garantire la privacy dei dipendenti e prevenire usi indebiti degli stessi strumenti.

2) Il presente Regolamento è adottato alla luce del:
   a) 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;
   b) Decreto Legislativo n. 196 del 23 giugno 2003, recante "Codice in materia di protezione dei dati personali" (d'ora in avanti Codice);
   c) 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";
   d) Provvedimento del Garante per la protezione dei dati personali, del 1.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, recante il seguente oggetto "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori";
   e) Direttiva n. 2/09 del 26.5.2009 della Presidenza del Consiglio dei Ministri – Dip. Funz. Pubblica la quale rileva che l'utilizzo delle tecnologie informatiche costituisce ormai il principale strumento di lavoro a disposizione dei dipendenti delle pubbliche amministrazioni e, pertanto, riconosce da un lato alle PP.AA., in quanto datori di lavoro, l'obbligo di assicurare la funzionalità e il corretto utilizzo degli strumenti informatici da parte dei lavoratori, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici; dall'altra riconosce all'Amministrazione il potere di controllo sul corretto utilizzo di tali mezzi, nel rispetto di alcune regole e principi generali quali il principio di proporzionalità, cioè di pertinenza e non eccedenza delle attività di controllo; di rispetto delle procedure di informazione/consultazione delle rappresentanze dei lavoratori; della preventiva informazione ai lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere dati personali."
   f) Documento di valutazione dei rischi (DUVRI) adottato con delibera AUSL Pescara n. 375 del 26 marzo 2015;

g) Legge 10 dicembre 2014, n. 183 e Decreto Legislativo n. 151 del 14 settembre 2015, recante "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità".

3) Il presente regolamento disciplina:

   a) i criteri di assegnazione e le modalità di utilizzo degli strumenti informatici nell'ambito dello svolgimento dell'attività lavorativa del personale della AUSL Pescara;

   b) le modalità di utilizzo del personal computer, della posta elettronica, di internet, della rete aziendale, delle password assegnate, e le relative responsabilità;

   c) le modalità di accesso ai servizi di assistenza, di richieste nuove forniture sia hardware che software, di richiesta fuori uso bene informatico

   d) le modalità di effettuazione dei controlli sul corretto utilizzo degli strumenti informatici e le conseguenze della violazione delle disposizioni del presente regolamento.

4) l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi dettati dal D.Lgs. 7 marzo 2005, n. 82 e dal D.P.R. 16 aprile 2013, n. 62 recante il Codice di comportamento dei dipendenti pubblici a norma dell'art. 54 del D.Lgs. 30 marzo 2001, n. 165;

5) le disposizioni del presente regolamento si applicano a tutti coloro che intrattengono un rapporto di impiego con l'Ente (Amministratori, personale dirigente e delle categorie a tempo indeterminato o a tempo determinato) qualora siano autorizzati all'utilizzo di strumentazioni informatiche, dell'accesso ad internet, della posta elettronica e della posta elettronica certificata. Le stesse disposizioni si estendono, in quanto compatibili, a tutti coloro che, in qualità di utenti esterni, gestiscono ed utilizzano gli strumenti informatici forniti dalla AUSL Pescara, sulla base di un rapporto di lavoro, di stage o tirocinio ovvero di fornitura o appalto di servizi.

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' riconosciuta al datore di lavoro la facoltà di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte dall'Amministratore di Sistema e/o dal personale del Servizio Informativo e Telecomunicazioni aziendale, sempre nel rispetto della citata normativa.

3) Le apparecchiature informatiche, i programmi e in generale, la strumentazione che l'Azienda AUSL di Pescara mette a disposizione dei soggetti di cui all'art. 1 comma 5, al fine di usufruire dei servizi di rete, ed in particolar modo dei servizi Internet/Intranet/Posta Elettronica Certificata/Posta Elettronica, devono essere utilizzati esclusivamente per esigenze istituzionali o di lavoro, nel pieno rispetto delle norme contenute nel presente regolamento.

4) L'Azienda AUSL di Pescara è titolare di tutte le risorse informative aziendali il cui corretto utilizzo è regolamentato dal presente regolamento che a tal fine assolve anche a finalità informative.

5) L'Azienda AUSL di Pescara, nel rispetto dei requisiti e dei criteri di cui al D.Lgs. 7 marzo 2005, n. 82 e del D.Lgs 30/06/2003 n. 196 memorizza e conserva i dati relativi al traffico telematico per il tempo strettamente necessario agli adempimenti di natura tecnica o relativi alla sicurezza e comunque giustificati dall'adempimento a precise disposizioni normative. Tali dati sono detenuti e custoditi dalla UOSD Sistemi Informativi e Telecomunicazioni.

6) Nel rispetto del principio della prevenzione degli abusi, l'Azienda si riserva il diritto di interdire o sospendere in qualsiasi momento l'accesso a determinati siti, mediante sistemi di blocco automatico o simili, ovvero a limitare l'accesso ai soli siti riconducibili all'attività istituzionale dell'Ente, così come di bloccare la ricezione di files sospetti allegati a messaggi di posta elettronica aziendale ovvero di bloccare i messaggi di posta elettronica valutati offensivi o potenzialmente pericolosi.

7) Ogni infrazione alle regole dettate dal presente Regolamento esporrà l'utente alle conseguenze, previste dalla specifica normativa nazionale e aziendale e dal sistema sanzionatorio di cui all'art. 14 del presente atto.

8) Tutti i soggetti interessati dalle disposizioni del presente Regolamento sono tenuti a contattare la UOSD Sistemi Informativi e Telecomunicazioni, prima di intraprendere qualsiasi attività non disciplinata nelle disposizioni del presente atto, al fine di verificare che tali attività non siano in contrasto con la disciplina delle funzionalità informatiche così come stabilite dall'Azienda.

Art. 3

Tutela del lavoratore

1) Alla luce dell'art. 4, comma 1, L.n. 300/1970, così come sostituito dall'art. 23 del d.lgs. n. 151/2015, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, dal quale derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, prevede il loro impiego esclusivamente per i seguenti motivi: a) esigenze organizzative e produttive; b) sicurezza del lavoro; c) tutela del patrimonio aziendale.

2) L'art. 4, richiamato al precedente punto 1., introduce una distinzione a seconda che oggetto di regolamentazione siano: a) gli impianti audiovisivi; oppure, b) gli "strumenti di lavoro utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze" (come pc., tablet, smartphone, telefoni aziendali, badge, e altri device mobili anche attraverso servizi di geolocalizzazione).

3) I "controlli sugli impianti", sono vietati salvo il raggiungimento di un accordo sindacale o la richiesta di una espressa autorizzazione amministrativa alla Direzione Territoriale del Lavoro (DTL) o al Ministero del Lavoro e, comunque, sono ammissibili solo per una delle finalità indicate al punto 1. del presente articolo. La disciplina di tale materia è oggetto di apposito Regolamento aziendale che andrà a sostituire quello attualmente in vigore.

4) I "controlli sugli strumenti di lavoro" sono consentiti senza la necessità di effettuare alcuna specifica procedura e sono oggetto del presente Regolamento. Per detti controlli la Azienda deve adempiere all'obbligo di fornire una adeguata informazione (mediante specifiche informative e regolamenti interni), sull'uso degli strumenti e sullo svolgimento dei controlli, oltre che nel rispetto di quanto disposto dal Decreto Legislativo n. 196 del 23 giugno 2003.

5) I dati raccolti potranno essere utilizzati per le sole finalità connesse al rapporto di lavoro, quindi anche a fini disciplinari nei confronti del lavoratore.

6) 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

Soggetti, competenze e responsabilità

1) Il presente articolo, in relazione all'utilizzo delle attrezzature e dei servizi informatici, disciplina competenze e le responsabilità dei soggetti individuati al precedente art. 1 comma 5.

2) I Direttori/Dirigenti di Unità Operative sono tenuti a:

   a) tenere aggiornato il registro delle assegnazioni delle postazioni informatizzate per dipendenti/dirigenti assegnati alla propria struttura;

   b) interagire con il SIT per la definizione dei piani di dispiegamento/aggiornamento delle postazioni di lavoro informatizzate e per il loro razionale utilizzo;

   c) valutare le richieste di fornitura di nuove postazioni o di aggiornamento di quelle in esercizio e di acquisizione di nuove componenti software per la propria struttura.

3) I Dirigenti sono tenuti ad assicurare:

   a) che il personale assegnato si uniformi alle regole ed alle procedure previste dal presente Regolamento;

   b) il rispetto degli obblighi inerenti il trattamento dei dati personali gestiti dalla propria Unità Operativa, in applicazione di quanto previsto dal D.Lgs. n. 196/2003 e s.m.i.;

   c) tutte le attività gestionali necessarie ad assicurare il corretto utilizzo del patrimonio informatico della proprio Unità Operativa.

4) I soggetti preposti alla gestione del sistema informatico aziendale, così come individuati dal Dirigente Responsabile della UOSD Sistemi Informativi e Telecomunicazioni sono incaricati di:

   a) monitorare il dispiegamento delle postazioni informatizzate nell'ambito delle singole strutture;

   b) monitorare le richieste di fornitura di nuove postazioni o di aggiornamento di quelle in esercizio, nonché dei software in uso presso le stesse articolazioni;

   c) monitorare, nel rispetto della riservatezza degli utenti e secondo le previsioni del presente regolamento, il corretto utilizzo del patrimonio informatico;

   d) segnalare prontamente al Responsabile della sicurezza informatica ogni eventuale attività non autorizzata sui sistemi.

5) Il Responsabile della sicurezza informatica, individuato nel Dirigente Responsabile del UOSD Sistemi Informativi Aziendali e Telecomunicazioni, è tenuto a svolgere le seguenti attività:

   a) adozione di tutte le misure atte a garantire la sicurezza del Sistema Informativo Aziendale;

   b) implementazione delle policy di sicurezza sul Sistema Informativo Aziendale;

   c) fornire informazioni in materia di sicurezza informatica, provvedendo , altresì, a diramare le direttive necessarie per un utilizzo ragionevolmente sicuro del sistema informativo.

6) Ciascun assegnatario o fruitore di risorse informatiche come individuato all'art. 1 comma 5, è personalmente e direttamente responsabile per ciò che concerne:

a) il rispetto delle regole di cui al presente regolamento;

b) ogni uso che venga fatto delle attrezzature informatiche e delle credenziali (account, passwords, user Id) assegnategli, fatto salvo l'eventuale uso improprio degli stessi derivante da causa di forza maggiore o da fatto non imputabile allo stesso.

7) Al fine di favorire gli adempimenti di cui al presente Regolamento, la U.O.C. Gestione Risorse Umane provvede tempestivamente a comunicare al U.O.S.D. Sistemi Informativi e Telecomunicazioni l'elenco del personale assunto/cessato.

Art. 5

Canali di comunicazione

1) Ogni tipo di richiesta riguardante le apparecchiature informatiche, gli applicativi aziendali, il sistema operativo, i software in uso in Azienda, la rete aziendale e rete internet, la posta elettronica aziendale e la posta elettronica certificata PEC, la telefonia fissa e mobile, dispositivi fax, ed ogni altro dispositivo afferente all' UOSD Sistemi Informativi e Telecomunicazioni, dovrà necessariamente pervenire attraverso il seguente canale di comunicazione:

HELP DESK supporto informatico di **I livello**

- Chiamando il numero **085 425 3095**
- Inviando una e-mail all'indirizzo **helpdesk@ausl.pe.it**

Gli orari del servizio dell' Help-Desk sono:
08:00 – 18:00 dal lunedì al venerdì
08:00 – 14:00 sabato

2) È in ogni caso esclusa la trasmissione delle richieste di cui al comma precedente a mezzo fax; tale previsione si impone in osservanza dei temi trattati dal CAD (Codice dell'amministrazione digitale d.lgs. n. 82/2005) con esplicito riferimento alla dematerializzazione dei documenti prodotti nell'ambito dell'attività della Pubblica Amministrazione.

3) Il personale addetto all' HELPDESK potrà fornire anche assistenza remota sui PC degli utenti utilizzando modalità di collegamento che richiedono conferma di consenso da parte dell'utente stesso.

Art. 6

Assegnazione di hardware e software al personale

1) Ad ogni dipendente dell'Azienda (personale dirigente e delle categorie, a tempo indeterminato o a tempo determinato), su richiesta di Direttori e Dirigenti può essere

assegnata una postazione informatica fissa costituita da: unità centrale, schermo, tastiera, mouse. (*Modulo richiesta apparecchiature informatiche All. 2*)

2) Su richiesta motivata di Direttori e Dirigenti, per le esigenze legate a specifiche funzioni e in sostituzione della postazione standard, si potranno assegnare pc portatili. In questo caso potrà essere assegnato anche un schermo, una tastiera, un mouse.

3) Ogni postazione informatica sarà dotata dei software operativi ed applicativi, con regolari licenze, individuati dal SIT. Sarà cura del Direttore/Dirigente Responsabile della Struttura assegnataria segnalare eventuali esigenze integrative. Il SIT provvederà alla verifica tecnica di compatibilità della richiesta integrativa e potrà darne corso, ove possibile, nei limiti delle disponibilità finanziarie e dei procedimenti amministrativi.

4) Le richieste di acquisto, sia hardware che software di qualunque bene o servizio di natura informatica, dovranno essere sempre redatte a firma del Dirigente Responsabile dell'U.O. richiedente ed inoltrate all' UOSD Sistemi Informativi e Telecomunicazioni tramite la modulistica predisposta (dove previsto) per l'avallo tecnico propedeutico al successivo acquisto da parte dell'Ufficio ABS/Economato.

5) Ogni donazione o comodato d'uso di strumentazione informatica e/o software a favore della AUSL di Pescara deve essere comunicata all'ufficio Sistemi Informativi e Telecomunicazioni Aziendali che provvederà dopo le opportune verifiche ad autorizzare l'accettazione; la non comunicazione esclude le apparecchiature e i programmi dall'assistenza.

6) Non si fornirà nessun tipo di supporto tecnico per i dispositivi acquisiti senza il preventivo nulla osta del SIT.

7) Si declina ogni tipo di responsabilità e non si offre alcun supporto tecnico su apparecchiature e/o programmi (HW/SW) installati senza coinvolgere il personale tecnico autorizzato dal SIT.

8) Gli acquisti legati a necessità sistemistiche aziendali saranno imputati ad apposito centro di costo legato alla spesa informatica generale, mentre gli acquisti legati ad esigenze specifiche di singole Unità Operative verranno imputate al centro di costo della struttura richiedente.

9) Qualora si tratti di acquisti finalizzati alla sostituzione di attrezzature obsolete o in dismissione, la richiesta di acquisto dovrà essere preceduta dalla richiesta di dichiarazione di fuori uso.

10) La struttura SIT provvede, in via esclusiva, all'assegnazione diretta delle dotazioni informatiche agli aventi diritto su indicazione del Direttore/Dirigente Responsabile delle Strutture richiedenti.

11) Nessuna modifica alle predette assegnazioni, può essere disposta senza la preventiva autorizzazione del Direttore/Dirigente Responsabile della struttura assegnataria e del SIT.

12) Anche al fine di predisporre una efficace programmazione del fabbisogno informatico , le singole Strutture provvedono, con cadenza annuale, a fornire al SIT l'elenco aggiornato e completo dei computer a disposizione della Struttura e dei relativi utilizzatori.

13) L'utente non può disporre lo spostamento del PC di proprietà dell'Azienda in altro ufficio o fuori dai locali di pertinenza aziendale, salvo espressa autorizzazione del Dirigente, sentita la UOSD Sistemi Informativi e Telecomunicazioni.

14) Le attività di trasloco delle postazioni di lavoro e/o relative utenze telefoniche devono essere concordate preventivamente con l'HELPDESK informatico al numero 085 425 3095 o all'indirizzo di posta elettronica helpdesk@ausl.pe.it .

15) Le strutture aziendali sono invitate, fin dalla definizione dei bandi di gara, a segnalare all'UOSD Sistemi Informativi e Telecomunicazioni ogni tipo di intervento o opera riguardante il trasloco, la costruzione, la manutenzione o la ristrutturazione di locali in cui insistono personal computer e apparati attivi o passivi per reti di trasmissione dati e telefonia, o cablaggi dati/fonia su cavi in rame, su cavi in fibra ottica e su mezzi radioelettrici (wifi), anche al fine di impegnare le risorse e limitare i tempi per la riconfigurazione dei personal computer e riattivazione dei servizi di fonia e dati sulle sedi oggetto dell'intervento.

Art. 7

Dismissione Beni Informatici

1) La dismissione dei cespiti e quindi anche dei beni informatici è di competenza dell'Ufficio Tecnico ed è regolamentata con Del. 553 del 29/05/2013.

2) Il SIT, su incarico dell'Ufficio Tecnico, valuta e approva le singole richieste in base a criteri di efficienza e di obsolescenza.

3) La sostituzione di un bene informatico dismesso non è da considerarsi automatica ed avviene solo su valutazioni spettanti al SIT.

Art. 8

Utilizzo del personal computer assegnato

1) Il personal computer, fisso o portatile, assegnato al dipendente è uno strumento di lavoro e deve essere utilizzato secondo criteri di diligenza e correttezza e nel rispetto delle prescrizioni del presente Regolamento.

2) Nel caso di assegnazione di personal computer di tipo portatile l'utente deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro ed in caso di allontanamento deve custodirlo in un luogo non accessibile da parte di terzi non autorizzati.

3) Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo autorizzazione esplicita da parte del responsabile del SIT.

4) Non è possibile installare software senza la preventiva autorizzazione del SIT anche al fine di prevenire l'introduzione di virus, l'utilizzo di licenze illegali e per proteggere l'integrità del sistema informativo aziendale.

5) I soggetti di cui all'art. 1 sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) e non possono duplicare o utilizzare i software assegnati al di fuori di quanto consentito dagli accordi di licenza.

6) Non possono essere installati e/o utilizzati supporti hardware diversi da quelli assegnati (es. modem, masterizzatori, webcam, microfoni e in generale qualsiasi tipo di supporto informatico) né è consentito il collegamento alla rete aziendale di personal computer e altro hardware di proprietà dei soggetti di cui all'art. 1.

7) Le postazioni di lavoro PC sono collegate alla rete di trasmissione dati della Azienda AUSL di Pescara e l'utilizzo delle stesse è consentito esclusivamente agli utenti le cui credenziali di accesso alla rete dell'Azienda AUSL siano state registrate nel Dominio informatico aziendale.

8) A ciascun utente è assegnato un codice d'identificazione utente (username) e una password per l'accesso al proprio personal computer, alla posta elettronica e ad internet (Modulo richiesta account All. 1) . La password deve essere custodita con la massima cura e non divulgata. La password di accesso al personal computer, alla rete, alla posta elettronica ed a Internet è riservata e personale.

9) Nel caso si sospetti che la password abbia perso la segretezza, questa deve essere immediatamente sostituita, in autonomia o chiedendo supporto al SIT.

10) Gli utenti sono tenuti a variare la password con cadenza periodica, in conformità a quanto previsto dal Regolamento tecnico in materia di misure minime di sicurezza (Allegato B al Codice in materia di protezione dei dati personali).

11) È assolutamente proibito accedere al proprio computer, ad internet, alla posta elettronica e nei programmi con un codice di identificazione utente diverso da quello personale.

12) Gli utenti possono utilizzare il personal computer di un collega assente solo ed esclusivamente per improrogabili necessità di lavoro (quale, ad esempio, la temporanea impossibilità di utilizzo del proprio personal computer per cause tecniche o la necessità di utilizzare particolari software non installati sulla propria macchina), previa autorizzazione del Dirigente responsabile dell' Unità Operativa, ed utilizzando esclusivamente le proprie credenziali di accesso.

13) L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro in uso, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima.

14) L'utente è tenuto a custodire il PC con la massima diligenza, curando di spegnerlo sia al termine della giornata lavorativa, sia nel caso di assenze prolungate dall'ufficio, al fine di evitare accessi da parte di terzi non autorizzati, salvo diverse indicazioni.

15) Non è consentito l'utilizzo di sistemi di crittografia o di qualsiasi altro programma di sicurezza non previsto esplicitamente dal Responsabile della sicurezza informatica.

16) Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte del SIT.

17) Alla cessazione dall'incarico ovvero dal servizio, i soggetti di cui all'art. 1 devono accertarsi che i dati presenti sul PC, relativi all'attività svolta, e che dovessero essere necessari per future attività, vengano messi a disposizione del SIT. Analogamente, dovranno essere consegnate al SIT, in busta chiusa, eventuali password aggiuntive utilizzate per l'accesso a file, cartelle, ecc.

Art. 9

Stampanti

1) Il SIT mette a disposizione, per le attività di stampa/copia, stampanti multifunzione/dipartimentali di rete condivise fra più utenti, anche non necessariamente facenti capo alla stessa Unità Operativa, purché dislocati nello stesso piano/sede.
2) Le stampanti multifunzione/dipartimentali di rete non saranno assegnate alle singole Strutture, ma saranno gestite in maniera centralizzata dal SIT.
3) Non saranno assegnate stampanti singole personali, fatte salve le stampanti adibite a particolari procedure (stampa etichette, stampe per sportelli front-end, stampe CUP, stampe PS ecc.). Tutto il personale, incluso quello con qualifica Dirigenziale, dovrà utilizzare le apparecchiature di rete. Le stampanti singole ancora in funzione potranno essere utilizzate fino alla loro messa in fuori uso.
4) Il SIT si riserva la facoltà di effettuare controlli (in forma riservata) sul utilizzo delle apparecchiature di stampa e, qualora si rilevassero anomali ed eccessivi volumi di stampe/copie prodotte, di inviare segnalazioni ai Direttori/Dirigenti delle strutture interessate.

Art. 10

Backup dei dati

1) L'Archiviazione dei dati presenti sul personal computer è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. I dati ed i documenti di lavoro archiviati devono essere esclusivamente quelli necessari all'attività lavorativa e/o istituzionali aziendali.
2) E' vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.
3) L' Azienda AUSL di Pescara attiva un sistema di server finalizzato a garantire la sicurezza dei dati. Tale scopo si consegue attraverso il salvataggio dei dati su uno spazio protetto aggiuntivo in rete rispetto a quello disponibile sul personal computer assegnato.

4) Su richiesta del Dirigente responsabile di UO, il SIT predispone una o più specifiche directory di salvataggio riservate alla stessa UO.

5) Su autorizzazione del Dirigente responsabile di UO, ciascun utente può memorizzare dati (esclusi quelli estranei all'attività lavorativa) all'interno della directory del proprio servizio o UO appositamente predisposta. Tale utilità consente, inoltre, la possibilità che più utenti possano operare su files condivisi.

6) Sui server aziendali possono essere archiviati e salvati solo dati relativi all'attività lavorativa e/o istituzionale. Ciascun Dirigente stabilisce per la propria area o servizio quali dati possono essere salvati sui server, nel rispetto delle disposizioni vigenti in tema di riservatezza. I files contenenti dati sensibili sono ospitati in apposite directory accessibili solo ad i utenti appositamente autorizzati.

7) Il SIT può in qualsiasi momento rimuovere dal sistema dei server qualsiasi file ritenuto pericoloso per l'integrità del sistema e non conforme alle prescrizioni del regolamento, anche senza preventiva comunicazione ai soggetti di cui all'art. 1. Inoltre, la struttura Informatica può diramare in qualsiasi momento avvisi rivolti alla generalità degli utenti, o a gruppi più ristretti, a seconda dei casi, per segnalare la presenza di files non consentiti con l'invito a rimuoverli entro un termine perentorio. Decorso inutilmente il termine, i files sono rimossi dalla struttura Informatica, con conseguente segnalazione al Direttore nella cui area è avvenuta la violazione per i necessari provvedimenti.

Art. 11

Utilizzo della Posta Elettronica nominativa

1) La posta elettronica è uno strumento di lavoro e, come tale, va utilizzato secondo criteri di diligenza e correttezza, nonché sulla base delle prescrizioni del presente Regolamento.

2) L'Azienda AUSL di Pescara fornisce a ciascun dipendente in servizio un indirizzo di posta elettronica nominativo esposto ad Internet. (Modulo richiesta account All. 1)

3) L'assegnazione degli account di posta elettronica implica l'obbligo di utilizzare tale mezzo di comunicazione per lo svolgimento della propria attività lavorativa e/o istituzionale anche in funzione della dematerializzazione prevista dal CAD (Codice dell'Amministrazione Digitale – D. Lgs. 7 marzo 2005, n. 82), che promuove l'utilizzo di reti telematiche come strumento di interazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati. (circolare D.G. n. 6311I13 del 24/4/2013)

4) L'indirizzo di posta elettronica assegnato deve essere utilizzato dal personale esclusivamente per fini di lavoro.

5) L'Azienda AUSL di Pescara stabilisce, inoltre, le seguenti prescrizioni interne finalizzate ad un corretto utilizzo della stessa posta elettronica nominativa:

    a) non è consentito utilizzare la posta elettronica per fini personali; sono proibiti utilizzi impropri quali l'invio di messaggi diffamatori, osceni, di profanazione, lettere minatorie o di offesa razziale, messaggi commerciali o di propaganda, le

cosiddette "catene di S. Antonio";

b) il personale è tenuto a non dare seguito a messaggi con dubbi oggetti e provenienza (c.d. messaggi di posta indesiderata) in cui vengano richieste informazioni riguardanti dati personali riservati e/o credenziali di autenticazione (fenomeno di spam/phishing). I messaggi e-mail di phishing sono pensati per rubare le credenziali personali di accesso ai sistemi informatici, chiedono dati personali sensibili o reindirizzano a siti web contraffatti dove viene chiesto di fornire credenziali e dati riservati personali. In questi casi seguire le seguenti regole:

   - non aprire messaggi e-mail ritenuti posta indesiderata (Spam). Cancellarli e vuotare la cartella di posta eliminata
   - non rispondere ai messaggi e-mail di Spam, perché confermereste di avere un account di posta attivo con l'unica conseguenza di aumentare la quantità di messaggi indesiderati
   - non aprire gli allegati contenuti nei messaggi e-mail ritenuti SPAM
   - non fornire dati personali sensibili o riservati via e-mail
   - Non accedere a collegamenti/link per essere rimosso dalla lista dei destinatari di e-mail indesiderate. In svariati casi, si ottiene l'effetto contrario con spam ancora maggiore
   - sospettare in generale di qualunque e-mail che inviti a cliccare su link/collegamenti presenti nel corpo del messaggio
   - non divulgare/non reinoltrare messaggi di natura ripetitiva (c.d. catene di S. Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi o quando nel testo si legge di bambini sfortunati, di malati terminali, etc. sono al 99% dei falsi.

c) Per ridurre il fenomeno dello spamming è opportuno, in quei casi di invio di un e-mail a molti destinatari, utilizzare il campo "CCN, copia carbone nascosta " (o "BCC, blind carbon copy" in alcuni programmi di posta) al posto del campo "A". Quest'ultimo può essere lasciato vuoto o essere riempito con il proprio indirizzo di posta elettronica.

d) ciascun dipendente, nelle comunicazioni a mezzo posta elettronica con i vari livelli organizzativi dell'Ente, è tenuto ad utilizzare un linguaggio appropriato ed una forma espositiva adeguata, secondo il comune sentire;

e) l'invio di messaggi di posta elettronica ad un elevato numero di destinatari è consentito solo qualora richiesto da specifiche esigenze di lavoro; è fatto salvo, in ogni caso, l'invio di circolari o analoghi messaggi usualmente indirizzati a tutto il personale o a specifici gruppi di posta;

f) L'invio di circolari per mezzo di posta elettronica a tutto il personale o comunque a grandi gruppi di utenza deve essere preventivamente concordato con il SIT e seguire modalità tecniche indicate di volta in volta.

g) si applicano all'utilizzo della posta elettronica le ordinarie regole di riservatezza e di segreto per ragioni d'ufficio; i documenti di lavoro possono essere inviati ad indirizzi di posta elettronica esterni solo se necessario per l'attività

lavorativa;

h) tramite l'indirizzo di posta elettronica possono essere inviati *file* allegati; l'invio deve essere commisurato alla capacità delle infrastrutture adottate al fine di non causare l'indisponibilità dei sistemi e dei dati, a tal fine si stabilisce che la dimensione massima degli allegati non puo' superare i 35 MB. In ogni caso è fortemente consigliata la conversione degli allegati in formati compressi quali .zip, .jpg, o altro.

i) la cassetta di posta elettronica non deve essere impropriamente utilizzata come archivio storico online dei documenti ricevuti. Tale consuetudine contribuisce pericolosamente alla saturazione delle risorse di memorizzazione del server di posta e alla conseguente interruzione del servizio. Per cui è fissato un limite massimo (Quota) di spazio di 750 MB per ogni cassetta postale. Al raggiungimento del 75% della Quota, verrà notificato all'utente l'approssimarsi del limite Quota. Al raggiungimento del 100% della Quota, non sarà più possibile inviare messaggi. Al raggiungimento del 120% della Quota, non sarà più possibile inviare/ricevere messaggi. Al raggiungimento della quota contribuiscono tutte le cartelle inclusa la cartella della posta eliminata.

j) Eventuali esigenze specifiche ed eccezionali che dovessero richiedere Quota maggiore devono essere rappresentate e validamente motivate dal Dirigente dell'Unità Operativa al SIT che di volta in volta provvederà a valutare alternative possibili o ad accordare la richiesta di ampliamento della Quota.

k) tutti gli utenti sono tenuti a curare la manutenzione della propria cassetta postale e quindi ad eliminare i messaggi di posta elettronica non più necessari ed a salvare sul proprio PC o comunque su dispositivi di memorizzazione locali le e-mail che comportano il superamento della quota stabilita di 750 MB.

l) il personale è tenuto a non aprire *file* allegati di incerta provenienza o che contengano estensioni di tipo .exe, .com, .vbs, .htm, .scr, .bat, .js , .pif. In qualunque altra situazione di incertezza contattare il SIT.

m) ciascun dipendente ha a disposizione una funzionalità che consente di inviare automaticamente, in caso di assenza, messaggi di risposta contenenti i riferimenti di posta elettronica o telefonici di altro dipendente a cui potrà rivolgersi il richiedente per particolari informazioni ("Regole fuori sede");

n) ciascun dipendente può delegare un altro dipendente quale "fiduciario", al fine di verificare i contenuti dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate alla attività lavorativa; con la delega il "fiduciario" è autorizzato ad inoltrare al Direttore o Responsabile di Struttura di riferimento i messaggi ritenuti rilevanti per lo svolgimento dell'attività lavorativa; di tale attività il "fiduciario" è tenuto a dare informativa, alla prima occasione utile, al dipendente interessato;

o) in caso di contemporanea assenza del dipendente delegante e del "fiduciario", ovvero nel caso in cui non sia stata rilasciata alcuna delega, e sussistendo urgenza e comprovata necessità, la casella di posta elettronica può essere visionata, con le stesse modalità indicate alla lettera precedente, dal Direttore o Responsabile di Struttura di riferimento del dipendente interessato; di tale eventualità deve essere data informativa al predetto dipendente;

6) L' Azienda AUSL di Pescara provvede ad archiviare le email aziendali di ciascun dipendente secondo le modalità e i tempi stabiliti dalle leggi in vigore.

Art. 12

Utilizzo della Posta Elettronica condivisa

1) Per esigenze lavorative l'Azienda AUSL di Pescara può disporre l'utilizzo di caselle di posta elettronica condivise da più dipendenti di Servizio/Ufficio, attraverso le quali gli utenti interni o esterni possono interfacciarsi con i servizi/uffici dell'Amministrazione.
2) fermo restando l'applicazione delle prescrizioni di cui al precedente art. 8, si stabiliscono le seguenti ulteriori prescrizioni interne finalizzate ad un corretto utilizzo della posta elettronica condivisa:
    a) il dipendente che risponde alle richieste avanzate attraverso le caselle di posta condivise dovrà apporre in calce alle stesse la propria sigla, al fine di garantire la massima trasparenza per l'utente;
    b) le risposte fornite tramite le caselle di posta elettronica condivise possono essere consultate da ciascun dipendente che abbia l'accesso alla stessa casella di posta;
    c) le risposte fornite sono archiviate con le stesse modalità e gli stessi tempi previsti per le caselle di posta elettronica nominativa.

Art. 13

Accesso ed utilizzo di Internet

1) L'azienda AUSL di Pescara consente l'accesso ad Internet a tutti i dipendenti delle sue Strutture centrali e periferiche promuovendo la digitalizzazione delle attività e dei servizi dell'Amministrazione. (Modulo richiesta account All. 1)
2) Internet e i servizi di rete devono essere utilizzati esclusivamente per motivi legati all'esecuzione della prestazione lavorativa e/o per motivi istituzionali.
3) Si stabiliscono le seguenti prescrizioni interne finalizzate ad un corretto utilizzo della rete Internet e dei servizi di rete:
    a) il Sistema Informativo predispone quanto necessario per l'applicazione di particolari prodotti di filtraggio (URL filtering) allo scopo di impedire l'accesso ad una serie di siti non pertinenti, utilizzando blacklist di siti non consultabili a priori, quali ad esempio, siti pornografici e siti contenenti attività ludiche - sulla base di elenchi precostituiti ed aggiornati da società specializzate;
    b) è consentita l'effettuazione di adempimenti personali online nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, o per tenere rapporti con istituti bancari e assicurativi, nei tempi strettamente necessari

allo svolgimento delle transazioni, come indicato nella Direttiva n° 2 del 26 maggio 2009 emanata dal Ministro per la Pubblica Amministrazione e l'Innovazione;

c) è vietato "scaricare" o "prelevare" dalla rete Internet (download) files musicali o multimediali del tipo MP3, AVI, MPG, DIVX, Quicktime o altro formato e/o programmi per la fruizione di contenuto audio/video, non pertinenti con la specifica attività di servizio o comunque non legati a finalità istituzionali;

d) sono altresì vietate operazioni di invio di file alla rete Internet (upload) se non pertinenti con la specifica attività di servizio o comunque non legati a finalità istituzionali;

e) il personale è tenuto al rispetto della regolamentazione sul diritto d'autore, per quanto riguarda eventuali programmi scaricati dalla rete Internet.

f) è vietato l'utilizzo di qualsiasi mezzo alternativo (modem o altro) al collegamento predisposto dall'Ente per connettersi ad Internet;

g) è vietato l'accesso alla rete aziendale dall'esterno via modem o altro mezzo di accesso remoto senza l'autorizzazione del Responsabile della sicurezza informatica;

h) è vietato lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo

4) Tutti gli accessi ad Internet sono cronologicamente registrati e tracciati in appositi file (LOG), così come prevede in generale la norma in materia e le misure minime di sicurezza informatica. Il file di LOG sono sottoposti a rigide misure di protezione, anche ai fini della tutela della Privacy.

Art. 14

Controlli disposti dall' 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 controlli prolungati, costanti o indiscriminati, la Azienda adotta idonei strumenti di controllo graduato, atti a indirizzare i singoli dipendenti verso un uso corretto e pertinente della posta elettronica e di Internet. verifiche sulla funzionalità e sicurezza del sistema oltre che dal rilevamento di anomalie nell'utilizzo delle Rete

2) sono attivate in via preliminare forme di controllo anonimo, 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.

3) A fronte di un rilevato utilizzo anomalo, il controllo può concludersi con un avviso rivolto ai Dirigenti afferenti alla realtà lavorativa interessata avente come scopo quello di invitare i dipendenti ad attenersi scrupolosamente alle istruzioni impartite circa l'utilizzo degli strumenti di lavoro. In assenza di successive anomalie non si effettueranno controlli su base individuale

4) In caso di successivi ripetuti utilizzi anomali, saranno effettuati controlli individuali sui dipendenti afferenti alle specifiche aree lavorative o strutture organizzative coinvolte.

5) Per il personale dirigente il comportamento andrà segnalato al responsabile del Dipartimento/Servizio/UOC in cui svolge la propria attività tale personale per l'adozione degli atti di competenza, nonché alla Direzione Aziendale

6) Per il personale non dipendente, cui non è applicabile il CCNL, il comportamento andrà segnalato alla Direzione Aziendale per l'adozione degli atti di specifica competenza

Art. 15

Sanzioni disciplinari

1) Il mancato rispetto o la violazione delle regole contenute negli articoli del presente Regolamento è perseguibile con le sanzioni disciplinari previste dalla contrattazione collettiva, nel rispetto dei principi di gradualità e proporzionalità, fermo restando eventuali responsabilità penali, civili, amministrative o contabili.

Art. 16

INFORMATIVA AI SENSI DELL'ART. 13 D.LGS. 196/03

1) L' A.S.L. di Pescara in persona del Direttore Generale e legale rappresentante è TITOLARE del trattamento dei dati personali, sensibili e giudiziari di cui gli operatori del SIT vengono a conoscenza durante il controllo sul legittimo uso della posta elettronica, di internet e dei file della rete interna. (*Vedi Allegato 3*)

2) FINALITA' del trattamento è la verifica del corretto utilizzo nel rapporto di lavoro della posta elettronica, della rete Internet e degli strumenti utilizzati dai dipendenti della Azienda U.S.L. di Pescara per rendere la prestazione lavorativa.

3) MODALITA' del trattamento: gli operatori del SIT o personale tecnico esterno autorizzato dal Dirigente responsabile del SIT effettueranno il trattamento dei dati con strumenti informatici.

4) COMUNICAZIONE DEI DATI: il trattamento di verifica è effettuato con gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo lavoratore; la comunicazione, nel caso in cui si accerti un uso indebito della

singola postazione, sarà data al Direttore della Struttura alla quale appartiene il dipendente per la valutazione del caso sotto il profilo disciplinare.

5) DIRITTI DELL'INTERESSATO: Il dipendente potrà far valere i diritti di cui all'art. 7 del D.Lgs. 196/03 facendo pervenire richiesta scritta all'Ufficio relazioni con il Pubblico.

Art. 17

Disposizioni finali

1) Il presente Regolamento è stato redatto dalla UOC Affari generali e Legali e dalla UOSD Sistemi Informativi Aziendali.
2) Il suddetto regolamento 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:
    a) attraverso la pubblicazione sull'area INTRANET del sito istituzionale del sito aziendale;
    b) mediante trasmissione a mezzo posta elettronica a tutti i dipendenti.
4) E' fatto obbligo a chiunque spetti di osservarlo.

UNITA' SANITARIA LOCALE DI PESCARA

U.O.S.D. SISTEMI INFORMATIVI E TELECOMUNICAZIONI

Via R. Paolini, 47 – 65124 Pescara
Tel. 085/4253091-2-3-4 Fax 085-4253098

MODULO RICHIESTA ACCOUNT

Accesso alla postazione informatica ed ai servizi di rete, attivazione casella di posta elettronica aziendale, accesso ad Internet

(la presente richiesta va inviata all'indirizzo di posta elettronica **helpdesk@ausl.pe.it** o recapitata presso l'UOSD Sistemi Informativi e Telecomunicazioni)

Dati personali del richiedente

Cognome e Nome:_____

*Codice Fiscale:*_____

Matricola: _____

Qualifica: _____

Scadenza: _____ (solo nel caso di contrattisti a termine o collaboratori indicare obbligatoriamente la data di scadenza)

Struttura di riferimento per il recapito delle credenziali

Dipartimento/UOC: _____

Sede: _____

Recapito Telefonico: _____

Richiami normativi

OBBLIGHI E RESPONSABILITÀ DEL RICHIEDENTE

Il richiedente si impegna a non utilizzare login ed accessi per scopi diversi da quelli istituzionali aziendali e a non cedere le proprie credenziali ad altri per alcun motivo. Ogni singolo Utente è responsabile dell'attività espletata tramite il proprio account.
Il richiedente si impegna a non utilizzare i servizi di rete per effettuare attività che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i regolamenti vigenti.
Il richiedente si impegna ad implementare, sulla propria postazione di lavoro, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili.
Il richiedente prende atto che è vietato servirsi, del servizio di posta elettronica per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.
Il richiedente, inoltre, si impegna a non divulgare messaggi di natura ripetitiva (c.d. catene di S. Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi.
Il richiedente autorizza l'Azienda al trattamento dei suoi dati personali (compresi i log file sul server proxy, che contengono i dati del traffico WEB), in conformità alle norme legislative e regolamentari vigenti.
L'Azienda si riserva la facoltà di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, le eventuali violazioni alle presenti condizioni di utilizzo.

INFORMATIVA AI SENSI DELL'ART.13 DEL D.LGS. 196/03

In osservanza con quanto previsto dal D.Lgs. n.196/03, siamo a fornirLe le dovute informazioni in ordine alle finalità e modalità del trattamento dei Suoi dati personali, nonché l'ambito di comunicazione e diffusione degli stessi, alla natura dei dati in nostro possesso e del loro conferimento.

FINALITÀ DEL TRATTAMENTO:

Per il rilascio di account di posta elettronica, per l'accesso ad Internet e per l'accesso alla postazione informatica ed ai servizi di rete

MODALITÀ DEL TRATTAMENTO:

Il trattamento sarà svolto in forma automatizzata e cartacea ad opera di soggetti espressamente incaricati.

AMBITO DI COMUNICAZIONE E DI DIFFUSIONE:

I suoi dati, oggetto del trattamento, potranno essere comunicati ad altre strutture dell' Azienda e/o terzi.
Il conferimento dei dati è per Lei obbligatorio per poter usufruire dei servizi oggetto della richiesta.
Il richiedente ha il diritto di conoscere, in ogni momento, quali sono i Suoi dati e come essi vengono utilizzati, nonché il diritto di farli aggiornare, integrare, rettificare o cancellare, chiederne il blocco ed opporsi al loro trattamento rivolgendo un'istanza indirizzata al Responsabile del trattamento U.O.S.D. SISTEMI INFORMATIVI E TELECOMUNICAZIONI Via R. Paolini, 47 – 65124 Pescara. Titolare del trattamento è l'Azienda ASL di Pescara con sede legale in Via R. Paolini, 47 – 65124 Pescara.

Pescara, _____

Firma del richiedente _____ Firma del Responsabile della Struttura: _____

PARTE RISERVATA ALL'UFFICIO C.E.D.

Username : _____

Data attivazione: _____

Note: _____ Firma del Sistemista _____

Allegato n. 1

UNITA' SANITARIA LOCALE DI PESCARA

U.O.S.D. SISTEMI INFORMATIVI E TELECOMUNICAZIONI

Via R. Paolini, 47 – 65124 Pescara
Tel. 085/4253091-2-3-4 Fax 085-4253098

MODULO RICHIESTA APPARECCHIATURE INFORMATICHE

(la presente richiesta va inviata all'indirizzo di posta elettronica **helpdesk@ausl.pe.it**)

Struttura richiedente *

Dipartimento/UOC _____

Sede _____

Voce di conto: _____

Responsabile di Struttura: _____

Referente da contattare: _____

Recapito Telefonico _____ Email: _____

Apparecchiature richieste *

QT.	Descrizione

Finalità della richiesta e sede di installazione *

Eventuali apparecchiature da ritirare

QT.	Descrizione	N. Inventario

Eventuali fondi finalizzati all'acquisto: _____

Pescara, _____

Firma del richiedente: _____ Firma del Responsabile della Struttura: _____

*** campi necessari per la valutazione della richiesta.**

Allegato n. 2

Regione Abruzzo - ASL Pescara INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI INERENTE L'UTILIZZO DELLA POSTA ELETTRONICA, DI INTERNET E DEGLI STRUMENTI UTILIZZATI DAI DIPENDENTI DELLA AZIENDA U.S.L. DI PESCARA PER RENDERE LA PRESTAZIONE LAVORATIVA Art. 13 D.Lgs.vo n. 196 del 30.6.2003	Pagina 1 di 1 Versione 10/2015

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Gentile Dipendente,

visto l'art. 4, comma 1, L.n. 300/1970, così come sostituito dall'art. 23 del d.lgs. n. 151/2015, la Asl di Pescara ha regolamentato la materia inerente gli impianti audiovisivi e gli strumenti utilizzati dai dipendenti per rendere la prestazione lavorativa.

L'art. 4, sopra richiamato, introduce una distinzione a seconda che oggetto di regolamentazione siano: a) gli "impianti audiovisivi"; oppure, b) gli "strumenti di lavoro utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze" (come pc., tablet, smartphone, telefoni aziendali, badge, ecc.).

I "controlli sugli impianti", sono vietati salvo il raggiungimento di un accordo sindacale o la richiesta di una espressa autorizzazione amministrativa alla Direzione Territoriale del Lavoro (DTL) o al Ministero del Lavoro e, comunque, sono ammissibili solo per una delle finalità indicate al punto 1. del presente articolo. Suddetti controlli sono oggetti di uno specifico regolamento aziendale.

I "controlli sugli strumenti di lavoro", (come, pc., tablet, smartphone, telefoni aziendali, badge, ecc.)

sono consentiti senza la necessità di effettuare alcuna specifica procedura e sono oggetto del Regolamento aziendale di cui la presente Informativa forma parte integrante e sostanziale.

I dati raccolti, attraverso l'uso degli strumenti di lavoro, potranno essere utilizzati per le sole finalità connesse al rapporto di lavoro, quindi anche a fini disciplinari nei confronti del lavoratore.

Ai sensi dell'art. 13 del decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali), La informiamo che i dati personali e sensibili che La riguardano acquisiti attraverso certificazioni mediche nel corso di accertamenti o visite o da altre fonti, saranno trattati nel rispetto del Codice sulla Privacy e degli obblighi di riservatezza a cui è tenuta l'AUSL di Pescara.

I trattamenti di dati, in questione, effettuati dalla AUSL di Pescara nell'esercizio delle sue funzioni istituzionali sono ricompresi nei seguenti ambiti di attività:

IMPIANTI AUDIOVISIVI E STRUMENTI UTILIZZATI DAI DIPENDENTI DELLA AZIENDA U.S.L. DI PESCARA PER RENDERE LA PRESTAZIONE LAVORATIVA

Alla luce dell'art. 4, comma 1, L.n. 300/1970, così come sostituito dall'art. 23 del d.lgs. n. 151/2015, la regolamentazione della materia indicata nell'art. 1 del Regolamento aziendale, prevede la possibilità di controllo a distanza dell'attività dei lavoratori – attraverso i "controlli sugli strumenti di lavoro" - per i seguenti motivi: a) esigenze organizzative e produttive; b) sicurezza del lavoro; c) tutela del patrimonio aziendale.

FINALITA' DEL TRATTAMENTO

Attiene al la verifica del corretto utilizzo nel rapporto di lavoro del servizio di Posta Elettronica, di Internet, oltre che dell'uso dei seguenti strumenti: pc., tablet, smartphone, telefoni aziendali, badge, ecc.

I "controlli sugli strumenti di lavoro" sono consentiti senza la necessità di effettuare alcuna specifica procedura, ma facendo ricorso ad idonea Informativa.

MODALITA' DI TRATTAMENTO DEI DATI PERSONALI

L'Amministratore di Sistema, gli operatori del S.I.T., e/o il personale tecnico esterno autorizzato dal Direttore del S.I.T., effettueranno il trattamento dei dati con strumenti informatici.

OBBLIGATORIETA' DEL CONFERIMENTO DEI DATI

COMUNICAZIONE DEI DATI

Il trattamento di verifica, con i fini e le modalità sopra richiamati, è consentito dalla legge ed è effettuato con gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo lavoratore.

La comunicazione, nel caso in cui si accerti un uso indebito degli "strumenti di lavoro" (pc., tablet, smartphone, telefoni aziendali, badge, ecc.) e/o di Internet e/o della Posta elettronica, sarà data al Direttore responsabile della UO/Servizio/Ufficio alla quale appartiene il dipendente, per la valutazione del caso sotto il profilo Regolamento.

ESTREMI IDENTIFICATIVI DEL TITOLARE E DEI RESPONSABILI

Il Titolare del trattamento dei dati personali è la AUSL di Pescara, con sede in V. R. Paolini, 47 a Pescara, nella persona del suo Direttore Generale.

Il Responsabile del trattamento dei dati personali, ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali, è il Dirigente Responsabile dell'Ufficio URP, ove può prendere visione dell'elenco aggiornato dei Responsabili.

DIRITTO DI ACCESSO AI DATI PERSONALI – ART. 7

Il dipendente ha diritto di ottenere: la conferma dell'esistenza o meno dei propri dati personali, anche se non ancora registrati e la loro comunicazione in forma intelligibile; la loro provenienza e le finalità e modalità di trattamento; la cancellazione, trasformazione e anonimizzazione o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti e successivamente trattati. L'attestazione che le operazioni di aggiornamento, rettifica, cancellazione o blocco dei dati sono state portate a conoscenza anche di coloro ai quali i dati sono stati comunicati, salvo il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi sproporzionato all'obiettivo.

Per l'esercizio dei diritti di cui all'art. 7 ella può rivolgersi all'Ufficio URP (Ufficio Relazioni con il Pubblico) della AUSL di Pescara, sito in V. R. Paolini, 47 a Pescara.

Legge n. 300/1970. Art. 7 - Sanzioni disciplinari

1. 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.

2.Il datore di lavoro non può adottare alcun provvedimento Regolamento nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

3.Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato .

4.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.

5.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.

6.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 Regolamento 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 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 Regolamento resta sospesa fino alla pronuncia da parte del collegio.

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

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

Allegato B Originale

I Direttori della U.U.O.O. proponenti, con la sottoscrizione, a seguito dell'istruttoria effettuata, attestano la regolarità tecnica e amministrativa nonchè la legittimità del presente provvedimento

Il Dirigente Responsabile U.O.S.D. Sistemi Informativi e Telecomunicazioni
Ing. Marco De Benedictis

Il Direttore U.O.C. AFFARI GENERALI E LEGALI
dott. ssa Francesca Rancitelli

Il Direttore della U.O. proponente attesta che la spesa risulta imputata sulla voce di conto del bilancio aziendale

Il Dirigente Responsabile U.O.S.D. Sistemi Informativi e Telecomunicazioni
Ing. Marco De Benedictis

Il Direttore U.O.C. AFFARI GENERALI E LEGALI
dott. ssa Francesca Rancitelli

Ai sensi del D. Lgs. 502/92 e successive modificazioni ed integrazioni, i sottoscritti esprimono il seguente parere sul presente provvedimento:

□X favorevole

□ non favorevole per le seguenti motivazioni

IL DIRETTORE AMMINISTRATIVO
(Avv. Domenico Carano)

□ X favorevole

□ non favorevole per le seguenti motivazioni

IL DIRETTORE SANITARIO
(Dr.ssa Lucia Romandini)

IL DIRETTORE GENERALE
dr. Claudio D'Amario

Il presente provvedimento viene pubblicato all'albo on line dell'Ausl di Pescara in data 13 GEN. 2016 ove rimarrà affisso per un periodo non inferiore a n. 15 giorni consecutivi

---

□ X Il presente provvedimento è immediatamente esecutivo a seguito della pubblicazione all'albo on line dell'Ausl di Pescara

□ Il presente provvedimento è soggetto al controllo da parte della Giunta Regionale

---

Il presente provvedimento viene trasmesso:

per l'esecuzione a:

- UOSD Sist. Informativi e Telec.
- UOC Affari Generali e Legali
-
-

per conoscenza a:

-
-
-

alla Giunta Regionale in data con nota prot.

alla Conferenza dei Sindaci in data con nota prot.

al Collegio Sindacale in data con nota prot.

U.O.C. Affari Generali e Legali
Il funzionario incaricato

U.O.C. Affari Generali e Legali
Il Responsabile Affari Generali
(dott. Fabrizio Veri)