Allegato alla delibera n. ___del ____

DISCIPLINARE SULL'UTILIZZO DI INTERNET E POSTA ELETTRONICA DELL'AZIENDA OSPEDALIERO - UNIVERSITARIA DI FERRARA

Premessa

Nel pieno rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali (art. 2, comma 1, del Testo Unico – D.Lgs. n° 196/2003) l'Azienda Ospedaliero - Universitaria di Ferrara adotta il presente "Disciplinare sull'utilizzo di Internet e Posta Elettronica".
La normativa e gli atti di riferimento del presente Regolamento sono i seguenti:

- D.Lgs n°196 del 2003 e successive modificazioni e integrazioni (Codice in materia di Protezione dei dati personali), di seguito indicato come Testo Unico;
- Codice per la amministrazione digitale (D.Lgs n° 82/2005 e s.m.i);
- Provvedimento a carattere generale del Garante per la protezione dei dati personali dell'1/03/2007 ad oggetto: "Lavoro: le linee guida del Garante per posta elettronica e internet", pubblicato in G.U. n° 58 del 10/03/2007;
- Statuto dei lavoratori (L. n° 300/1970);
- Direttiva n° 2 DD 26/05/2009, c.d. "Direttiva Brunetta", del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate. Le proposte verranno esaminate dall'ICT.
Il presente "Disciplinare" è soggetto a revisione con frequenza almeno annuale da parte del Dipartimento Interaziendale ICT.

Art. 1
Oggetto

Il "Disciplinare" ha per finalità di stabilire le norme per l'accesso e l'utilizzo dei seguenti servizi dell'Azienda Ospedaliero - Universitaria di Ferrara, di seguito denominata "Azienda":
1) Posta elettronica;
2) Rete internet;
3) Computer aziendali;

di seguito indicati nel loro complesso come "Servizi Informatici Aziendali" (d'ora in poi S.I.A.).
Il presente "Disciplinare" è rivolto esclusivamente ai dipendenti dell'Azienda e loro equiparati.
Tutte le altre figure (ad es. collaboratori esterni, fornitori, ospiti, ecc...), eventualmente autorizzate, saranno oggetto di un separato disciplinare a cura del Dipartimento interaziendale ICT.
I S.I.A. sono regolamentati, oltre che dalle presenti norme, anche da eventuali altri regolamenti per l'accesso a servizi particolari.

Art.2
Definizioni

Nel presente "Disciplinare" i termini di seguito elencati hanno le correlate definizioni:

- BLACK-LIST: elenco dei siti non accessibili agli utenti;
- CATENA DI S. ANTONIO: invio di messaggi di posta elettronica che istighino il destinatario a propagare i messaggi ricevuti ad una pluralità di destinatari, senza attinenza con l'attività lavorativa;
- HOSTING: ospitare sui propri server web le pagine di un sito web esclusivamente di soggetti terzi, rendendolo così accessibile da Internet;
- HOUSING: concessione in locazione ad un utente della possibilità di inserire un suo server all'interno dell'infrastruttura IT aziendale;
- INDIRIZZO IP: numero che identifica univocamente un dispositivo collegato ad una rete informatica;
- INTERNET PROVIDER: azienda che fornisce all'Azienda Ospedaliero - Universitaria Ferrara il canale di accesso alla rete Internet;
- LOG: registrazione elettronica automatica generata da applicazioni o dispositivi, riguardante informazioni sulle attività eseguite all'interno degli impianti aziendali;
- MAIL SPAMMING: invio massivo di messaggi di posta elettronica non desiderati e diretti ad una pluralità di destinatari, aventi generalmente contenuto commerciale o comunque non attinente l'attività lavorativa;
- POSTAZIONE DI LAVORO: personal computer (PC), o altro idoneo dispositivo, collegabile alla rete aziendale tramite il quale l'utente accede ai servizi;
- SUPPORTO INFORMATICO: qualsiasi componente in grado di conservare stabilmente dati informatici;
- UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
- UTENTE INTERNET: persona autorizzata ad accedere al servizio "Internet" con l'esclusione dei siti previsti nella "black-list";

Art. 3
Incaricati al trattamento dei dati personali

I S.I.A. sono strumenti di lavoro forniti dall'Azienda, che ne fissa le modalità di utilizzo: gli utenti sono tenuti ad osservarle scrupolosamente.
Gli utenti sono nominati, ai sensi del Testo Unico u.v., "incaricati al trattamento dei dati personali" a cui hanno accesso o che sono trattati mediante i S.I.A..
I dati devono essere trattati limitatamente alle operazioni indispensabili per le finalità per i quali sono stati raccolti e nei limiti delle funzioni degli incaricati, e comunque nel rispetto dei principi di pertinenza e non eccedenza stabiliti dalle norme vigenti.

Art. 4
Identificazione dell'utente per l'accesso ai servizi

L'utilizzo dei S.I.A. richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) ed una parola chiave segreta (password).
L'Azienda si riserva, a seguito di evoluzione delle tecnologie, di introdurre, anche solo in particolari contesti, sistemi di autenticazione "forte", basati, ad esempio, su smart card o caratteristiche biometriche, nel rispetto delle normative vigenti.
Per accedere ai S.I.A., un nuovo utente dovrà fornire i propri dati identificativi, prendere visione del presente regolamento e compilare e sottoscrivere in forma completa in ogni sua parte i moduli di richiesta di abilitazione di volta in volta predisposti e disponibili sulla intranet aziendale (http://inospfe.azospfe.it).

Il modulo dovrà essere consegnato alla struttura aziendale deputata alla creazione degli accessi ai sistemi o servizi di cui si richiede l'abilitazione, timbrato e firmato in modo leggibile dal responsabile della struttura organizzativa alla quale l'utente appartiene.
L'incompleta compilazione e autorizzazione del modulo sopra citato, ne comporterà l'automatico annullamento.
L'Azienda si riserva, a seguito di evoluzione della tecnologia, di sostituire la modulistica cartacea con sistemi di autorizzazione elettronica.
La password non potrà essere ceduta a terzi neppure temporaneamente, dovrà essere mantenuta segreta e dovrà essere obbligatoriamente modificata dall'utente in ogni caso in cui egli abbia fondati sospetti che la segretezza della password sia venuta meno.
Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. L'utente non deve lasciare incustodita o facilmente accessibile la postazione di lavoro una volta collegata al sistema, e deve disattivare la connessione qualora si debba allontanare. Inoltre non deve rendere accessibili in alcun modo le informazioni concernenti la propria password.
La userid identificativa dell'utente alla cessazione del rapporto di lavoro viene archiviata e non potrà essere riassegnata ad altro utente.
Non sono previsti codici di accesso anonimi, salvo nei casi in cui sia prevista una successiva procedura di identificazione personale per l'accesso alle procedure e/o ai dati veri e propri.
L'utente deve conservare la password con la massima riservatezza e con la massima diligenza.
La password:

- non deve essere banale né contenere riferimenti facilmente riconducibili all'utente;
- dovrà essere lunga almeno 8 caratteri tra i quali: lettere minuscole, lettere maiuscole, numeri, caratteri speciali;
- dovrà essere modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni tre mesi.

Alla scadenza dei tre mesi, nel caso in cui l'utente non avesse provveduto a modificare la propria password, la sua abilitazione verrà sospesa.
L'utente avrà ancora due mesi per riattivare il proprio profilo semplicemente cambiando la password con le modalità opportune e in modo autonomo.
Alla scadenza di questi ulteriori due mesi, il codice di identificazione personale (userid) verrà disattivato.
Nel caso in cui l'utente dimentichi la propria password, o nel caso in cui l'account venga bloccato a causa di un numero elevato di tentativi d'accesso con una password sbagliata, per riottenere l'accesso ai servizi l'utente dovrà inviare una richiesta di reimpostazione della password al Dipartimento Interaziendale Tecnologie Informatiche (d'ora in poi I.C.T.), firmata e con in allegato una fotocopia del tesserino di riconoscimento aziendale o di un documento di identità valido.
Nel caso di disattivazione del codice di identificazione personale, per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo "Richiesta di abilitazione ai servizi informatici aziendali" e consegnarlo all'I.C.T., firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.
Dopo sei mesi di non utilizzo dei servizi la userid e la password verranno automaticamente disattivati.
Nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, l'I.C.T. a seguito di segnalazione provvederà alla disattivazione di userid e password.
Nel caso in cui l'utente a seguito di variazione di Servizio o di funzione debba accedere a servizi e/o risorse diverse da quelle previste inizialmente l'I.C.T. a seguito di segnalazione provvederà all'aggiornamento dei privilegi dell'utente.
L'utente si impegna a comunicare immediatamente all'I.C.T. il furto, lo smarrimento, la perdita ovvero l'appropriazione a qualsivoglia titolo da parte di terzi della password.
Nel caso di prolungata assenza dell'utente, egli dovrà utilizzare, qualora siano tecnicamente disponibili, funzioni che consentano di inviare messaggi automatici di risposta per "fuori sede" e che contengano le coordinate per un contatto alternativo con la struttura.

È facoltà del dirigente responsabile dell'utente richiedere all'I.C.T., nel caso di sue assenze prolungate o improvvise e in condizioni di urgenza e necessità, l'accesso ai suoi dati e messaggi di posta elettronica e consultare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Di tale fatto deve rimanere traccia su apposito verbale informando il lavoratore alla prima occasione utile.
Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", relativamente al punto 5.2/b, ove si definisce la figura del fiduciario, si ritiene che i suggerimenti ivi contenuti non siano funzionalmente adottabili dall'Azienda.

Art. 5
Finalità e limitazioni d'uso

Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", l'accesso ai S.I.A. è da intendersi quale "strumento di lavoro".
È pertanto vietato l'uso dei S.I.A. nei seguenti casi:

- per l'utilizzo di procedure aziendali con modalità e finalità non attinenti ai propri doveri d'ufficio;
- per ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- per trasferire sulla postazione dell'utente programmi e/o file di dati relativi a progetti od obiettivi estranei all'utente o per finalità personali (come ad esempio file il cui contenuto sia protetto da diritto d'autore);
- per ricerche e/o consultazioni, all'interno dell'orario di lavoro, in maniera ripetuta e unicamente per scopi personali, di siti il cui contenuto informativo non sia attinente con l'attività lavorativa dell'utilizzatore;
- per ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Azienda.

È comunque vietato l'uso dello strumento nei casi configurati dalla normativa vigente come reato, in particolare:

- diffusione di virus, "cavalli di troia" o altri programmi la cui azione consista nel sabotaggio, distruzione, alterazione o visione del contenuto informativo delle postazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- per attività di furto di dati aziendali o di altri utenti, organismi e/o aziende;
- per attività di hackeraggio e pirateria informatica in generale.

I servizi aziendali potranno richiedere l'accesso a particolari siti istituzionali in "modalità privilegiata", ovvero senza disporre delle credenziali per la generica navigazione Internet oppure con una disponibilità di banda superiore al normale.
L'I.C.T. provvederà ad evadere queste richieste compatibilmente con le risorse tecniche a disposizione.

Art. 6
Rilevazione statistica delle attività

Accesso ad Internet

Le operazioni di accesso ad Internet potranno essere memorizzate per finalità di sicurezza del sistema con la gradualità prevista dalla normativa vigente.
La rilevazione statistica delle attività avviene attraverso i file di "log" generati dai sistemi.
I log non sono accessibili per la consultazione e la loro tenuta avviene a cura degli Amministratori di Sistema nominati secondo le modalità previste dalla normativa vigente e dai regolamenti aziendali in merito. Questi log non sono oggetto di operazioni di backup.
Nell'ambito dell'attività autorizzata alla navigazione in Internet, l'I.C.T. provvede ad effettuare elaborazioni statistiche utilizzando i dati di "log" dell'uso del servizio, che contengono:

- data e ora dell'accesso;
- nome del sito richiamato per la consultazione;
- esito della consultazione;
- tipologia di operazione richiesta e informazioni sugli eventuali file scaricati;
- numero di byte trasferiti dall'elaboratore remoto e viceversa.

Qualora l'I.C.T. riscontri le seguenti anomalie:

- traffico superiore del 20% rispetto alla media dell'ultimo semestre;
- utilizzo di porte e/o protocolli non utilizzati dai programmi aziendali;
- contemporanea presenza di sessioni parallele dirette al medesimo sito remoto;
- traffico dati diretto a siti presenti nella black-list;

agli utenti verrà inviato un avviso generalizzato che informa della sospensione, per un periodo limitato e definito nella stessa informativa, dei controlli anonimi e del fatto che i log di sistema verranno utilizzati per l'individuazione di tali anomalie. Durante questo periodo, in aggiunta alle informazioni enunciate in precedenza, verrà rilevato anche l'indirizzo IP di partenza della navigazione. Al termine del periodo di osservazione questi log saranno distrutti a cura dell'I.C.T..
In ogni caso non verranno estratte statistiche a livello individuale, bensì su base aggregata per area, settore o ufficio. In nessun caso i log del sistema generati sono usati come strumento di controllo dell'operato dell'utente. Da essi non è ricavabile alcuna informazione relativa al tempo trascorso nelle varie navigazioni dai singoli utenti.
L'Azienda utilizzerà le risultanze dell'elaborazione statistica dei log per aggiornare una black-list finalizzata ad impedire la navigazione verso siti vietati o non attinenti agli scopi istituzionali dell'Azienda.
Qualora un sito bloccato venga segnalato, attraverso l'apposita pagina di richiesta di sblocco, di interesse aziendale e riconosciuto come tale dall'I.C.T, lo stesso sarà rimosso dalla black-list e la rimozione avrà efficacia nei confronti di tutti gli utenti.
I log potranno essere oggetto di provvedimenti dell'Autorità Giudiziaria e Amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo. A seguito di specifica richiesta da parte delle Autorità preposte essi verranno memorizzati in forma non anonima, conservati e consegnati secondo le istruzioni ricevute da parte delle Autorità stesse.

Posta elettronica

Non viene tenuto alcun log relativo all'attività svolta dagli utenti con il servizio di posta elettronica.
L'unico log generato dal sistema è di tipo diagnostico con la finalità di individuare eventuali problemi in invio e ricezione della posta e la sua conservazione è limitata nel tempo a 30 giorni solari da un sistema automatico di cancellazione. Questo log non è oggetto di operazioni di backup.
I messaggi inviati e ricevuti in modalità web vengono conservati sul server di posta fino alla loro cancellazione da parte dell'utente. I messaggi inviati e ricevuti mediante software client installato su PC restano memorizzati esclusivamente sul PC dell'utente.

L'Azienda sta valutando l'introduzione di un sistema di gestione della posta elettronica aziendale che consenta l'archiviazione dei messaggi e-mail inviati e ricevuti a scopo di ripristino degli stessi a seguito di distruzione, danneggiamento, perdita sia volontaria che accidentale, ritenendo la posta elettronica una banca dati di interesse strategico.

Accesso remoto alle postazioni

Gli strumenti di accesso remoto utilizzati dall'I.C.T. non costituiscono in alcun modo controllo a distanza dell'attività del lavoratore.
Ogni accesso remoto da parte di personale tecnico autorizzato ad una stazione di lavoro avviene solo per finalità di assistenza tecnica al fine di aggiornare/ripristinare le condizioni di funzionamento ottimali e/o di installarne delle nuove.
Ogni accesso avviene dietro consenso dell'utente espresso mediante la pressione di un tasto (o mediante altre azioni che denotino volontarietà e consapevolezza degli utenti); ciò quindi implica la presenza dell'utente davanti al monitor che ha piena visione delle operazioni svolte dall'addetto all'assistenza remota e ha facoltà di interromperle in ogni istante.
L'accesso remoto alle postazioni è ammesso senza consenso dell'utente se esse si trovano in modalità disconnessa ("logout"), e in tal caso l'utente remoto accede al sistema con le proprie credenziali senza accedere ai contenuti dei profili personali degli utenti del PC.
Nel caso in cui, per problematiche tecniche urgenti ed improcrastinabili, si renda necessario accedere con le credenziali di uno specifico utente, e questi non sia disponibile, verrà resettata la sua password e lo stesso dovrà provvedere alla sostituzione della password al primo collegamento.
In questi particolarissimi casi l'ICT documenterà dettagliatamente ogni operazione effettuata con le credenziali dell'utente, ed informerà lo stesso con la massima tempestività.
In nessun caso l'ICT chiede la password di accesso degli utenti, che comunque non è conosciuta dal personale tecnico.

Art. 7
Configurazioni hardware e software

Le postazioni di lavoro utente vengono predisposte e configurate per il corretto uso dei S.I.A. dall'I.C.T..
L'utente si impegna a mantenere la corretta configurazione della postazione di lavoro che utilizza.
Le politiche relative ai software di gestione della sicurezza sono gestite centralmente e non è richiesta all'utilizzatore alcuna operazione manuale in merito.
A tal fine le postazioni di lavoro sono normalmente configurate per consentire l'accesso dell'utente solamente in modalità non privilegiata. Nel caso in cui a causa di particolari requisiti tecnici si renda necessario elevare i privilegi informatici dell'utente, quest'ultimo è maggiormente tenuto a preservare la configurazione della propria macchina così come impostata dall'I.C.T..
Qualora durante un intervento di manutenzione, i tecnici I.C.T. rilevino postazioni utente non conformi agli standard aziendali autorizzati, in mancanza di una specifica precedente deroga, gli stessi procederanno d'ufficio a ripristinare tali postazioni secondo gli standard definiti.
Nel caso in cui l'utente ritenga siano necessarie modifiche alla configurazione, ivi compresa l'installazione di nuovi programmi, dovrà formulare una richiesta all'I.C.T. che provvederà ad autorizzare o meno la richiesta, in quanto ogni modifica implica potenziali ricadute sulle corrette funzionalità delle procedure aziendali.
L'utente è responsabile delle attrezzature informatiche a lui assegnate, anche temporaneamente, e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, soprattutto nel caso di attrezzature portabili.
Sui dispositivi portabili condivisi tra più persone non devono essere memorizzati dati personali e sensibili nonché credenziali di accesso alla rete e ai sistemi centrali. Questi ultimi dispositivi devono essere restituiti, al termine del periodo di utilizzo concordato, alla struttura che li ha assegnati.

Art. 8
Dismissione o cessione di supporti informatici

I supporti informatici non più necessari e contenenti dati devono essere resi inutilizzabili prima di dismetterli.
Questa operazione può essere effettuata distruggendo i supporti o sottoponendoli a cancellazioni logiche definitive con appositi software.
I supporti che dovessero essere ceduti a terzi vanno puliti sottoponendoli a cancellazioni logiche definitive con appositi software.
All'ICT sono affidate le attività di supporto e supervisione al riguardo.

Art. 9
Modalità di prestazione dei servizi

L'Azienda si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità d'interromperli per le manutenzioni ordinarie o in caso di situazioni straordinarie (ad es. attacco informatico) che possano compromettere integrità, disponibilità e riservatezza dei dati aziendali.
Qualora possibile le interruzioni saranno preventivamente comunicate agli utenti.
Per migliorare la qualità o la sicurezza dei servizi e dei sistemi informatici attualmente predisposti, l'Azienda valuterà con attenzione eventuali osservazioni, suggerimenti ed indicazioni che gli utenti faranno pervenire all'I.C.T..
L'operatività specifica del personale ICT, per la peculiare attività che svolge, in particolare per quanto riguarda la sperimentazione di nuove tecnologie da introdurre eventualmente in Azienda, è disciplinata in apposito documento di incarico.

Art. 10
Backup e protezione dati sensibili

L'I.C.T. provvede al salvataggio periodico delle banche dati prodotte dai Sistemi Informatici Centralizzati. La periodicità è indicata nelle Linee programmatiche aziendali sulla sicurezza dei dati.
Gli utenti possono richiedere all'I.C.T. la creazione di cartelle condivise tra più utenti. L'I.C.T., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede alla creazione sui propri server di tale cartella ed alle configurazioni sui PC degli utenti interessati. Tale cartella viene altresì inserita nei backup automatici.
Costituiscono dati di rilevanza aziendale soltanto quelli memorizzati sui server in proprietà gestiti dall'I.C.T..
Gli utenti non devono avere dati personali o sensibili memorizzati sui PC aziendali. Se ciò avviene, l'Azienda non è responsabile di tali dati e non ne garantisce il periodico salvataggio né tantomeno il ripristino in caso di necessità.
Rimane comunque responsabilità dell'utente la cura e la protezione di eventuali file contenenti dati riservati e/o sensibili memorizzati sul proprio PC.

Art. 11
Pubblicazione di contenuti e realizzazione di siti personali

Non è consentito all'utente di produrre, pubblicare o manutenere siti web diversi da quello ufficiale aziendale mediante la rete aziendale e/o i S.I.A., salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.

È altresì vietato utilizzare il sito aziendale, sia mediante la pubblicazione che l'inserimento di link a siti esterni, per pubblicizzare e/o promuovere attività non confacenti o addirittura in concorrenza con le attività erogate dall'Azienda Ospedaliero - Universitaria di Ferrara.
È diritto di ogni servizio chiedere di inserire uno spazio informativo (tecnicamente consistente in una o più "pagine", collegate tra loro ed alla "home page" aziendale) sul sito aziendale, di cui è direttamente responsabile anche per il contenuto e la correttezza delle informazioni.
A tale proposito i servizi dovranno fare richiesta all'Ufficio Comunicazione segnalando gli identificativi delle persone che potranno inserire informazioni sul sito e chi sarà il responsabile che ne autorizzerà la pubblicazione.
A tal fine l'I.C.T. provvederà a creare uno spazio web sul sito interno e/o sul sito pubblico, collegandolo alla pagina iniziale, o nella sottopagina eventualmente di riferimento.
L'I.C.T. mette a disposizione il proprio supporto tecnico per la soluzione di eventuali problemi relativi all'applicazione delle procedure previste dal presente articolo, fatto salvo il fatto che l'inserimento e l'aggiornamento delle informazioni sono sempre a carico dei singoli servizi.
È fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza espressa autorizzazione del responsabile dell'Ufficio Comunicazione.
Si applicano in ogni caso le norme dei Codici deontologici professionali.
È di norma vietato realizzare funzioni di hosting e/o housing, salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.

Art. 12
Connessione a provider diversi da quelli aziendali

È vietato l'utilizzo, all'interno dell'Azienda di accedere alla rete Internet mediante diverso provider rispetto a quello scelto ufficialmente dall'Azienda.
Il divieto si estende anche alla connessione tramite "internet key" o sistemi analoghi non forniti dall'I.C.T..
Qualora sia disponibile una connessione di rete aziendale, cablata o wireless, questa è da considerarsi fortemente prioritaria rispetto all'utilizzo di altri sistemi di connessione.
Il presente articolo è stato redatto tenuto in debito conto che la violazione di quanto disposto potrebbe esporre la rete aziendale, ed i sistemi a questa connessi, a gravi problematiche di sicurezza.

Art. 13
Servizio di Posta Elettronica

Il Servizio Informatico fornisce due distinte tipologie di account di e-mail:
- account di servizio, il cui nome richiama il servizio in cui lavora l'utente;
- account legati al nominativo dell'utente richiedente.

L'account di servizio deve comunque essere associato ad almeno un altro account nominativo di utente e non può essere utilizzato per l'invio di messaggi, ma solo in ricezione. Sarà compito dell'I.C.T. fare in modo che i messaggi inviati a detto indirizzo siano smistati a tutti gli appartenenti al gruppo a cui è associato l'account di equipe.
Ogni account nominativo di posta ha uno spazio dedicato a disposizione di 200MB. Il raggiungimento di tale limite implica l'impossibilità di utilizzare, in tutto o in parte, il servizio. Il raggiungimento del 90% dell'occupazione dello spazio disponibile viene segnalato all'utente mediante un messaggio di posta elettronica.
Gli utenti possono richiedere all'I.C.T. l'estensione dello spazio dedicato. L'I.C.T., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede all'assegnazione di una diversa dimensione dello spazio dedicato alla posta.

Tutti i possessori di una casella di posta elettronica nominativa sono tenuti, quando possibile, a consultare quotidianamente la propria corrispondenza ed a provvedere tempestivamente allo scarico della stessa. Si ricorda che la consultazione via web non comporta lo scaricamento della posta dal server aziendale, operazione possibile soltanto con un client appositamente configurato sulla propria stazione di lavoro.
Per ottenere un account di posta elettronica è necessario seguire le indicazioni previste all'art. 4 del presente "Disciplinare".
È possibile consultare la posta elettronica non ancora scaricata o inviare nuovi messaggi collegandosi direttamente al sito internet aziendale, per consentire agli utenti fuori sede di continuare ad utilizzare il servizio.
Per inviare e ricevere e-mail relative ad argomenti inerenti l'attività lavorativa è obbligatorio utilizzare l'account aziendale.
È vietato l'utilizzo dell'account di posta elettronica aziendale per comunicazioni estranee all'attività lavorativa.
È consentito un moderato utilizzo di provider esterni di posta elettronica per comunicazioni personali, esclusivamente in modalità web, con l'avvertenza che l'Azienda non può fornire supporto in caso di impossibilità di raggiungere i siti web di tali provider a causa delle particolari configurazioni della rete finalizzate a massimizzare la sicurezza.

Art. 14
Comunicazioni di massa

È fatto obbligo agli utenti segnalare all'I.C.T. l'eventuale ricevimento di messaggi, sia da utenti interni che esterni, appartenenti ad una delle seguenti categorie:

- "mail spamming" e "catene di S. Antonio";
- aventi contenuto diffamatorio per l'Azienda od i suoi dipendenti;
- aventi contenuto moralmente deplorevole, scandaloso, propagandistico per correnti politiche o fazioni religiose;
- aventi contenuto non attinente l'attività lavorativa ed il cui ricevimento sia "non gradito" all'utente;
- aventi il fine di "intasare" le caselle di posta elettronica.

La segnalazione va indirizzata esclusivamente via e-mail all'indirizzo security@ospfe.it, inoltrando la e-mail sospetta.
Gli utenti interni che attuano uno dei comportamenti vietati verranno segnalati al Dipartimento Risorse Umane per le eventuali sanzioni disciplinari.
Per quanto riguarda comunicazioni da inviare in maniera massiva a tutte le caselle di posta aziendali, in genere per comunicazioni che rivestono particolare importanza per un congruo numero di utenti, l'autorizzazione deve essere ottenuta dall'Ufficio Comunicazione, che valuterà e approverà il testo proposto per l'invio.

Art. 15
Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente "Disciplinare", la disponibilità dei servizi informatici aziendali cesserà per l'utente nei seguenti casi:

1) qualora non sussistesse più la condizione di dipendente o di collaboratore esterno. Questo evento dovrà essere comunicato tempestivamente da parte del responsabile del servizio cessante all'I.C.T., in modo da poter eliminare dai S.I.A. tutte le abilitazioni;
2) qualora non fosse confermata o venisse revocata l'autorizzazione all'uso fornita dal Responsabile; il quale dovrà comunicare l'evento come al punto precedente;
3) qualora avvenisse il trasferimento di un utente da un servizio ad un altro. Il Responsabile del servizio cessante dovrà comunicare tempestivamente la cessazione del rapporto, mentre il Responsabile del servizio subentrante dovrà autorizzare le nuove abilitazioni con le procedure descritte all'art. 4 del presente "Disciplinare";

Art. 16
Comportamenti che danno luogo a segnalazione

Ai sensi del presente "Disciplinare", potranno essere segnalati al Dipartimento Risorse Umane, che valuterà le eventuali sanzioni disciplinari, gli assegnatari dei S.I.A. che porranno in essere uno o più dei seguenti comportamenti in aggiunta a quelli già indicati nell'art. 13:

a) installazione non autorizzata di hardware o software;
b) alterazione non autorizzata della configurazione hardware o software della stazione di lavoro;
c) comunicazione o diffusione di credenziali di accesso a sistemi e procedure informatiche, nonché altre informazioni tecniche riservate;
d) scarico non autorizzato di materiale informatico estraneo all'attività lavorativa;
e) violazione in genere di norme del Codice Penale, nella parte in cui tratta dei reati informatici;
f) violazione di quant'altro stabilito nel presente "Disciplinare".

Art. 17
Informativa

Il Titolare del trattamento dei dati è l'Azienda Ospedaliero - Universitaria di Ferrara.
I Responsabili del trattamento dei dati personali, a mezzo di strumenti informatici dell'Azienda, sono:

- L'I.C.T. (nella persona del Direttore del Dipartimento) per quanto attiene alla gestione dei dati effettuata mediante i sistemi informativi aziendali, circa le modalità tecnologiche e gli strumenti utilizzati per l'erogazione del servizio, ivi compreso il profilo della sicurezza;
- I Responsabili del trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento, per quanto attiene alle decisioni riguardo alla finalità ed alle modalità organizzative di utilizzo dei sistemi o servizi di competenza;
- i terzi che, in relazione ai servizi chiamati ad espletare per conto dell'Azienda, siano dalla stessa autorizzati all'utilizzo di sistemi informatici aziendali.

I diritti previsti dall'art. 7 del D.Lgs. 196/03 e in particolare il diritto di conoscere i dati che riguardano l'utente, il diritto di aggiornarli e il diritto di cancellare i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi ai Responsabili del trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento.
Il presente "Disciplinare" inizierà ad essere applicato dalla data dall'adozione del relativo provvedimento di approvazione e potrà essere soggetto in qualsiasi momento a modifiche ed aggiornamenti, dovuti ad

innovazione tecnologica e/o a modifiche organizzative aziendali, nonché per il mutato quadro normativo di riferimento.
Tali variazioni saranno rese note a tutti i dipendenti tramite l'emanazione di nuovi provvedimenti deliberativi.

Norma transitoria

Nell'attesa dell'implementazione di un sistema aziendale di gestione e archiviazione della posta elettronica, l'I.C.T. rende disponibile su richiesta uno spazio disco, sottoposto a procedura di backup, finalizzato unicamente al salvataggio di quei messaggi di posta che l'utente ritiene essenziali per la propria attività lavorativa, o che contengano comunque informazioni che l'utente ritenga di dover salvaguardare.
Tale spazio disco avrà una capacità standard pari a 50MB, fatta salva la possibilità di elevare questo limite a seguito di specifica motivata necessità.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Ferrara

ISTRUZIONI PER GLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI DELL'AZIENDA Ospedaliero - Universitaria DI FERRARA

Le seguenti istruzioni sono parte del sistema di sicurezza che l'Azienda Ospedaliero - Universitaria di Ferrara adotta al fine di gestire, nel rispetto della vigente normativa, i dati trattati.
Si descrivono di seguito alcuni aspetti particolarmente rilevanti in materia precisando che si ritiene indispensabile che chiunque tratti dati personali e/o sensibili in Azienda Ospedaliero - Universitaria di Ferrara prenda visione delle Linee programmatiche aziendali sulla sicurezza dei dati, la cui copia è reperibile presso il Dipartimento Interaziendale ICT.
Si precisa altresì che le presenti istruzioni non esauriscono le misure di sicurezza aziendali: a tale proposito è necessario altresì osservare quanto disposto dal vigente Regolamento recante il Sistema di gestione dei dati personali nell'azienda Ospedaliero-Universitaria di Ferrara "Arcispedale S. Anna" in Applicazione Del Decreto Legislativo 196/2003, reperibile sul sito Internet aziendale, alla sezione Amministrazione Trasparente e relativi allegati.

Istruzioni in tema di sicurezza

Documentazione cartacea

L'incaricato, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi controllando che i documenti siano sempre completi ed integri.
In caso di abbandono, anche temporaneo, dell'ufficio, l'incaricato non deve mai lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto): è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, ecc.).
Laddove si utilizzi un contenitore chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di incaricati autorizzati.
Occorre in particolare accertarsi che nessun visitatore o terzo estraneo (addetto alla manutenzione, alle pulizie, ecc. o un collega non autorizzato) possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti.
Al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate.

Utilizzo del sistema informatico
Tutti i dipendenti dell'Azienda Ospedaliero - Universitaria di Ferrara e tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale possono essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale.
Tutti gli appartenenti alle suddette categorie possono avere accesso al servizio di posta elettronica e richiedere l'accesso ad Internet che sarà autorizzato o meno – in base alla mansione e a considerazioni organizzative – dal responsabile del trattamento di riferimento.
La parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi.
La parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato.
A tutti gli utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima.
L'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.
Tutti i Personal Computer devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi al Dipartimento Interaziendale Tecnologie Informatiche (ICT).
In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password.

MF
20

E' vietato:
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra aziendali o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili) e altre e-mails che non siano di lavoro;
- allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive;
- manomettere o cambiare le configurazioni delle attrezzature aziendali se non esplicitamente autorizzati dai competenti servizi;
- installare attrezzature non autorizzate e collegarle alla rete aziendale se non dietro esplicita autorizzazione dei servizi competenti;
- intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia se non espressamente autorizzati o se non previsto dalla propria mansione.

Per nessuna ragione i dati contenuti e gestiti nel sistema informativo aziendale saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300)

Istruzioni per l'utilizzo degli strumenti di lavoro

Telefono e fax

Nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chiunque risponda all'apparecchio.
In caso di risposta negativa è necessario chiedere in alternativa un numero riservato.
Occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati
In caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza
Qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata.
L'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati

Fotocopiatrice e stampante

In caso di stampa o duplicazione non riuscite di documentazione contenente dati personali/sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi)
Qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili
Occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso

Supporti di memorizzazione

E' vietato l'utilizzo di supporti rimovibili, come ad esempio floppy disk, cd rom o chiavi USB, per lo scambio di dati sensibili; qualora vi fosse assoluta necessità di utilizzarli è indispensabile assicurarsi che essi non vengano riutilizzati e vengano distrutti dopo il loro utilizzo, se vengono riutilizzati occorre verificare che il precedente contenuto sia stato reso assolutamente irrecuperabile – le normali procedure di cancellazione di un dato informatico non sono normalmente sufficienti a garantire ciò, potendosi in molti casi recuperare anche dati cancellati con procedure e strumenti particolari -

ULTERIORI INDICAZIONI OPERATIVE

1) Rapporti di front office

Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza

Obbligo di riservatezza e segretezza: l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata (e con questo la comunicazione ad organi di informazione)
Controllo dell'identità del richiedente: nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario)
Identificazione dell'interessato e controllo dell'esattezza dei dati: in alcuni casi è necessaria l'identificazione del soggetto interessato per esigenze di garanzia di correttezza del trattamento (soprattutto per quanto riguarda la raccolta di dati anagrafici di cittadini stranieri), facendo attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato medesimo

2) Corretta comunicazione dei dati

La richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge (in casi dubbi rivolgere sempre richiesta di chiarimenti al Responsabile)
La comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato dal titolare o dal responsabile
L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.