FONDAZIONE IRCCS
ISTITUTO NAZIONALE
DEI TUMORI

20133 Milano - via Venezian, 1 - tel. 02.2390.1 - codice fiscale 80018230153 - partita i.v.a. 04376350155

Premesso

che il provvedimento del Garante per la protezione dei dati personali 1° marzo 2007 (in GU n. 58 del 10 marzo 2007) raccomanda l'adozione da parte dei datori di lavoro di un disciplinare interno per l'uso di internet e della posta elettronica;

il Consiglio di Amministrazione con deliberazione n. ..... del ..... ha approvato il presente

REGOLAMENTO SULL'UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE E DELL'ACCESSO ALLA RETE (INTRANET E INTERNET)

Obiettivo

Contenuto ed obiettivo dell' adozione del presente regolamento sono:

- la tutela dei beni patrimoniali aziendali;
- la garanzia del regolare svolgimento del servizio interno ed esterno di posta elettronica;
- la garanzia di un accesso alla rete aziendale e a internet per tutti i fruitori, in condizione di regolarità, sicurezza e tutela dei dati personali e sensibili propri e delle persone eventualmente oggetto delle comunicazioni;
- tutela del copyright sia della Fondazione che di terzi.

Oggetto

Costituisce oggetto del presente regolamento l'utilizzo della rete intranet, internet e della posta elettronica (e-mail) da parte di chiunque abbia un'utenza abilitata all'accesso alla rete aziendale

Definizioni

utente: colui che in possesso di credenziali di autenticazione alla rete aziendale fruisce di posta elettronica, accesso a intranet e internet;
credenziali di autenticazione: coppia costituita da nome-utente e password utilizzate per l'accesso alla rete aziendale
nome-utente: codice per l'identificazione dell'utente (formato dall'unione tra cognome e nome senza spazi);
password: parola chiave riservata conosciuta solamente dall'utente titolare;
dati personali (codice Privacy): qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
dati sensibili (codice Privacy): i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di ogni altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
internet (rete aziendale): rete di scambio e condivisione di documenti esclusivamente all'interno di una stessa azienda;
internet: sistema integrato di interconnessione tra computer che permette la trasmissione di informazioni a livello mondiale;
posta elettronica (e-mail): strumento utilizzato per ricevere ed inviare messaggi elettronici;
disclaimer: dichiarazioni di tipo legale che afferma l'estraneità di colui il quale produce un documento nei confronti di chiunque dovesse usare in modo improprio le informazioni in esse contenute;
spam: ricezione di grandi quantità di messaggi indesiderati (generalmente commerciali);
virus (informatico): programma creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito;

download: trasferimento di informazioni da un sistema o da un congegno informatico a un altro, in genere meno potente (esempio da internet a PC);
log file: file contenete la registrazione cronologica delle operazioni di un dato sistema informatico man mano che esse vengono eseguite;
crittografia: metodo per rendere un messaggio o un file "offuscato" in moda da non essere comprensibile a persone non autorizzate a leggerlo;
postazioni di lavoro: strumenti informatici messi a disposizione dall'azienda consistenti in computer (comprensivo di schermo, tastiera e mouse), stampante, scanner;
FTP: protocollo di trasferimento file.

Art. 1
Norme di comportamento

A norma del vigente Codice di comportamento per i dipendenti delle Pubbliche Amministrazioni, durante l'orario di lavoro il dipendente dedica la propria attività allo svolgimento delle mansioni affidategli nel rispetto dei principi di diligenza e correttezza.
Il dipendente è altresì responsabile del diligente e corretto uso dei beni aziendali che gli sono stati affidati per lo svolgimento delle proprie mansioni.
Il mancato rispetto delle regole contenute nel presente regolamento, ferma la responsabilità civile, penale e amministrativa, è perseguibile con provvedimenti disciplinari ai sensi dei contratti nazionali vigenti per il personale SSN.

Art. 2
Controlli

La Fondazione si riserva la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del dipendente nell'uso degli strumenti elettronici, accesso a internet e uso della posta elettronica.
Le verifiche si svolgeranno, con le modalità indicate negli articoli successivi, nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dai CCNL, dallo Statuto dei lavoratori e dal Codice Privacy.
A seguito delle verifiche informatiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.
Eventuali informazioni di natura sensibile potranno essere trattate dalla Fondazione se necessario per far valere o difendere un diritto in sede giudiziaria.

Art. 3
Tutela della rete aziendale

L'utilizzo dei PC, della rete aziendale, delle informazioni in esse contenute, dei programmi applicativi e il trattamento dei dati personali con strumenti elettronici è consentito agli utenti in possesso di credenziali di autenticazione (nome-utente e password) strettamente personali e non cedibili a terzi.

Gli utenti sono responsabili delle postazioni di lavoro a loro assegnate, pertanto non devono lasciarle incustodite e accessibili durante una sessione di lavoro.

Per garantire la riservatezza e la sicurezza dei dati personali trattati, l'utente deve inoltre:

- utilizzare password lunghe almeno otto caratteri contenenti almeno una lettera maiuscola, e un carattere speciale;
- modificare la password al primo utilizzo e, successivamente, almeno ogni tre mesi. Il sistema avviserà comunque l'utente dell'approssimarsi della data di scadenza della password;

s.c. Affari Generali e Legali
Il Direttore *ad interim*

- adottare le necessarie cautele per assicurare la segretezza e l'esclusività della password (ad esempio non scrivere la password su promemoria da appiccicare al computer, non adottare procedure di memorizzazione automatiche);
- Modificare immediatamente la password nel caso si ritenga che la stessa abbia perso le necessarie caratteristiche di riservatezza.

Le credenziali di autenticazione non utilizzate per più di 6 mesi sono disabilitate.

Inoltre a scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, è:

- vietato istallare modem o altri apparecchi non autorizzati;
- vietato collegare alla rete PC portatili non autorizzati;
- vietato istallare programmi non autorizzati.

Qualora il singolo utente abbia necessità specifiche provvede per il tramite e con l'ausilio dei competenti tecnici ICT tramite servizio di Help Desk.

Art. 4
Accesso a internet

L'accesso a internet è consentito nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo istituzionale e/o previste dalla legge.

Pertanto:

- non è consentito navigare in siti o registrarsi a siti non attinenti allo svolgimento delle mansioni;
- non è consentito il download di programmi, di file musicali, di file multimediale anche se gratuiti, salvo autorizzazione preventiva ed espressa;
- è vietato scaricare o immettere nella rete aziendale materiale di qualsiasi genere non attinente all'attività lavorativa o comunque di provenienza illecita;
- è vietato partecipare a forum non autorizzati e utilizzare chat line.

L'utente è considerato direttamente responsabile per un eventuale accesso illecito, per l'appropriazione indebita del materiale cartaceo utilizzato per stampare i risultati della navigazione e per il danneggiamento della rete aziendale a causa dei virus informatici introdottisi in seguito ad un uso non accorto degli strumenti informatici messi a disposizione.

È fatto salvo il diritto della Fondazione di chiedere l'ulteriore risarcimento del danno.

La Fondazione INT si riserva, a scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, di filtrare, inibendone l'accesso, i siti ritenuti non idonei a garantire la sicurezza ovvero la pertinenza agli scopi istituzionali, mediante l'utilizzo di parole chiave o di appositi filtri informatici ovvero di controlli successivi random non associabili all'utente diretto.

La Fondazione si riserva altresì la facoltà di bloccare eventuali download di file multimediali, musicali o comunque non pertinenti con gli scopi aziendali.

La Fondazione si riserva controlli anonimi, in accordo con il Codice sulla Privacy, tramite utilizzo di file di log, sul corretto utilizzo di internet basandosi su dati aggregati riferiti all'intera struttura aziendale o a sue aree o a gruppi di utenti. Solo nel caso in cui sussista il sospetto di ripetute violazioni del contenuto del presente articolo, possono essere eseguiti controlli sulla singola postazione di lavoro. Tali controlli non saranno preceduti da alcun avviso agli interessati da parte della Fondazione. Nel caso in cui, a seguito di tali controlli, venisse confermato l'effettivo utilizzo indebito dell'accesso a internet, la Fondazione si riserva di porre in atto le tutele più opportune a difesa dei propri interessi, nel rispetto delle disposizioni vigenti.

Nel caso in cui si presentasse l'esigenza di accedere a siti che risultassero bloccati, l'utente provvede per il tramite e con l'ausilio dei competenti tecnici ICT tramite servizio di Help Desk.

Art. 5
Casella di posta elettronica

La Fondazione INT si impegna a fornire, ove richiesta con le opportune procedure, una casella di posta elettronica a tutto il personale dipendente, ad uso esclusivamente istituzionale, al seguente indirizzo:

nome.cognome@istitutotumori.mi.it

è altresì possibile richiedere caselle di posta condivise tra gruppi di utenti del tipo:

nomegruppo@istitutumori.mi.it

La casella di posta, assegnata all'utente o al gruppo di utenti, è uno strumento di lavoro e come tale deve essere utilizzata ai fini istituzionali. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Fermo restando quanto sopra, è tollerato un uso personale limitato, tale da non intralciare o danneggiare o interferire in alcun modo con l'attività istituzionale né in termini di tempo dedicato né in termini di quantità/qualità delle informazioni e dei messaggi scambiati.

In ogni caso:

- è vietato inviare o memorizzare messaggi a contenuto offensivo, discriminatorio;
- è vietato usare la posta elettronica per documenti riservati e confidenziali;
- per non correre il rischio di essere infettati da virus, dovranno essere cancellati, senza aprirli, messaggi insoliti o provenienti da mittenti sconosciuti, inoltre dovrà essere disattivata la funzione anteprima automatica e il riquadro di anteprima;
- in caso di assenza del dipendente, la continuità dell'attività lavorativa sarà garantita da sistemi di risposta automatici ai messaggi di posta elettronica ricevuti;
- è il dovere del dipendente, che si assenta dal servizio, rendere possibile l'accesso ai files e alla casella di posta elettronica ricevuti;
- è dovere del dipendente, che si assenta dal servizio, rendere possibile l'accesso ai files e alla casella di posta elettronica da parte del responsabile dell'ufficio; a tal fine il dipendente è tenuto a indicare un fiduciario prontamente reperibile per la lettura dei messaggi di posta elettronica; in questo caso verrà riportata l'indicazione dell'utente -diverso dal titolare- che ha aperto o inviato il messaggio.

L'utente dovrà provvedere alla manutenzione della propria casella di posta al fine di evitare una eccessiva espansione della stessa che comporterebbe spreco di risorse aziendali. Pertanto è cura dell'utente di archiviare o cancellare periodicamente documenti inutili, superati, ingombranti.

A scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, la Fondazione si riserva di filtrare la corrispondenza in entrata mediante appositi filtri antispam e antivirus come ritenuti idonei con rispetto al livello tecnologico raggiunto dai prodotti specifici presenti sul mercato.

Inoltre sono filtrati messaggi in ricezione, provenienti anche da utenti conosciuti, con allegati aventi particolari estensioni (es: exe,bat, cmd, com, ecc...)

La Fondazione nel rispetto delle disposizioni normative in materia, si riserva la possibilità di effettuare controlli sulle caselle di posta elettronica aziendale qualora sussista il legittimo sospetto che sia stato violato il contenuto del presente articolo. Tali controlli non saranno preceduti da alcun avviso agli interessati da parte della Fondazione. Nel caso in cui, a seguito di tali controlli, venisse confermato

l'effettivo utilizzo indebito della casella di posta elettronica aziendale, la Fondazione si riserva di porre in atto le tutele più opportune a difesa dei propri interessi, nel rispetto delle disposizioni normative vigenti.

Art. 6
Divieti e limitazioni dell'uso della posta elettronica

È fatto divieto di utilizzo della "lista tutti" da parte di personale non autorizzato dalla Direzione, attraverso gli uffici specificatamente individuati.

Gli uffici che abbiano l'esigenza, occasionale, di inoltrare comunicazioni a tutti gli utenti, dovranno utilizzare l'apposita lista di distribuzione "lista tutti", inviando apposita richiesta del dirigente della struttura richiedente alla s.c. ICT tramite servizio di Help Desk.

Al fine di assicurare la fruibilità del servizio per tutti gli utenti della Fondazione, la dimensione massima consentita per l'invio o la ricezione di messaggi di posta elettronica è di 10 MByte.

La dimensione massima per le mail inviate a "lista tutti" è invece fissato ad 1 MByte.

È fatto divieto di inoltro di mail non pertinenti l'attività istituzionale quali, a mero titolo di esempio:

- comunicazioni di smarrimento oggetti
- auguri di festività varie
- saluti di fine attività
- pubblicità varie

È altresì vietato rispondere o partecipare alle cosiddette "catene di S. Antonio" qualunque ne sia il contenuto.

Poiché la posta elettronica è in chiaro, è vietato veicolare tramite e-mail dati personali ovvero sensibili relativi a persone o pazienti. Qualora ciò sia necessario per motivi istituzionali, i dati stessi devono essere veicolati in forma anonima o crittografati ovvero secondo le procedure di sicurezza indicati da competenti uffici ICT.

Art. 7
Disclaimer e firma

Costituisce obbligo dell'utilizzatore autorizzato, di collaborare in modo diligente con il datore di lavoro apponendo su tutte le mail obbligatoriamente in uscita verso l'esterno il testo ufficiale disclaimer quale rilasciato dall'Ente, tramite gli uffici competenti dell'ICT. È disponibile sul Forum della Fondazione apposita procedura di apposizione del disclaimer.

L'Ente rilascia il format autorizzato per l'apposizione della firma di ciascun mittente.

Art. 8
Importazione di files

La Fondazione autorizza l'importazione di files di provenienza esterna (es. FTP), attinenti l'attività istituzionale, alle condizioni tecnico operative tali da garantire la sicurezza e la provenienza certa degli stessi.

L'utente che abbia tali necessità provvede per il tramite e con l'ausilio dei competenti tecnici ICT tramite servizio di Help Desk.

Art. 9
Trattamento di dati sensibili e supporti rimovibili di dati

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifrature o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente intelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessi solo in caso di necessità (art. 22 comma 6, codice Privacy).

Gli utenti sono responsabili dei dati memorizzati sui supporti rimovibili (chiavetta USB, floppy disk, CD-ROM, DVD, ecc...).

Per i supporti contenenti dati sensibili, con riferimento alle vigenti norme del Codice sulla Privacy, l'utente provvederà alla loro custodia in luoghi sicuri al fine di evitare accessi non autorizzati o trattamenti non consentiti o alternativamente provvederà alla crittografia dei dati in essi contenuti.

I supporti contenenti dati sensibili se non più utilizzati devono essere distrutti o resi inutilizzabili, alternativamente possono essere riutilizzati previa cancellazione definitiva dei dati precedentemente contenuti.

Art. 10
Forum

La Fondazione mette a disposizione di persone o gruppi associativi o ricreativi di genere compatibile con le proprie finalità istituzionali, che ne facciano richiesta, apposito spazio virtuale nel forum al seguente indirizzo di rete internet:

http://forum

La Fondazione mette a disposizione di tutte le Organizzazioni sindacali delle aree della dirigenza e del comparto, e per ciascuna separatamente, apposito spazio "bacheca virtuale da utilizzarsi per le comunicazioni sindacali di competenza. La disponibilità di tali spazi equivale alla messa a disposizione delle bacheche fisicamente disponibili all'interno della struttura istituzionale.

Ad ogni nuovo messaggio inserito sulla "bacheca virtuale" seguirà notifica automatica alla mailing list "Lista Tutti", per effetto della quale i dipendenti riceveranno sulla casella di posta aziendale un messaggio proveniente da Bacheca INT contenente i dettagli del nuovo argomento inserito ed il link per accedervi.

Le Organizzazioni Sindacali dovranno designare uno o più referenti delegati alla gestione della bacheca, i cui nominativi andranno comunicati all'Amministrazione.

Le Organizzazioni Sindacali sono direttamente responsabili del contenuto delle comunicazioni pubblicate sulla "bacheca virtuale".

s.c. Affari Generali e Legali
Il Direttore *ad interim*