ISTRUZIONI PER GLI INCARICATI

Azienda Sanitaria Locale N. 1 di Sassari

Disciplinare per l'uso di Internet e della Posta Elettronica nella ASL 1

Documento	DPS-LGR03/1
Edizione	30/06/2007

Indice del Contenuto

Premessa

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet attraverso l'infrastruttura di rete Aziendale si và sempre più diffondendo in Azienda grazie al potenziamento dei servizi informativi, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni agli operatori sanitari e agli assistiti.

I servizi informativi sono ormai diventati fondamentali per l'Azienda in quanto consentono agli operatori sanitari di comunicare, collaborare, mantenersi aggiornati e quindi di esercitare efficacemente le attività professionali.

Pertanto è necessario che siano adottate adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative, e a tutelare la riservatezza dei dati personali di tutti.

A questo proposito si richiama quanto viene riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Questo disciplinare, ispirato alle Linee guida del Garante per la posta elettronica e Internet, Gazzetta Ufficiale n. 58 del 10 marzo 2007 (si veda Allegato A), intende fornire in modo trasparente ed esauriente un'informativa sull'uso degli strumenti informatici, di Internet e della posta elettronica, affinché il personale Aziendale sia sensibilizzato ad un uso corretto di questi servizi, nonchè informato sulle politiche di sicurezza, adottate dall'Azienda, per garantire l'affidabilità e la disponibilità dei servizi e delle risorse informatiche indispensabili per il servizio sanitario ai nostri assistiti, e nel contempo tutelare la privacy di tutti.

Per eventuali segnalazioni o chiarimenti è possibile rivolgersi a: e-mail: sistemi.informativi@aslsassari.it

Azienda Sanitaria Locale n. 1 Sassari

Direzione Generale – Settore Sistemi Informativi

Responsabile Sicurezza Informatica

Dott. Piergiorgio Annicchiarico

1 Utilizzo degli strumenti informatici e della rete Aziendale

Si ricorda che l'uso degli strumenti informatici e della rete Aziendale deve avvenire nel rispetto di regole fondamentali, già oggetto di richiamo nel manuale **"IST01 – Istruzioni per la Sicurezza dei Dati"** distribuiti a suo tempo in oltre 5.000 copie a tutti gli incaricati dei trattamenti, ai sensi del D. Lgs. n. 196/2003.

In particolare l'utilizzo dei sistemi informativi e dei servizi di rete è consentito solo al personale autorizzato e per l'esclusivo svolgimento delle proprie mansioni.

1.1 Accesso ai Servizi Informatici

L'accesso ai servizi informatici deve avvenire solo utilizzando le stazioni di lavoro (Personal Computer), i computer portatili e gli strumenti software messi a disposizione dall'Azienda e solo con le proprie credenziali personali di autenticazione (userID e password).

1.2 Misure di sicurezza della rete Aziendale

Il D.Lgs 196/03 T.U. Privacy impone alla nostra Azienda l'adozione di adeguate misure di sicurezza per tutelare la privacy di tutti, l'affidabilità e la disponibilità dei servizi e delle risorse informatiche indispensabili per il servizio sanitario ai nostri assistiti.

L'informazione, la sensibilizzazione e la collaborazione del personale è un presupposto essenziale perché le misure di sicurezza adottate risultino efficaci.

La tutela del patrimonio tecnologico ed informatico si attua attraverso strategie e misure di sicurezza logica, fisica ed organizzativa, atte a prevenire, contrastare e contenere il rischio di violazioni alla riservatezza, all'integrità e alla disponibilità dei dati e dei processi necessari al compimento della missione. Ossia per:

- Minimizzare i rischi di appropriazione, danneggiamento, distruzione volontaria o involontaria, uso improprio di apparecchiature informatiche, di sistemi o dati essenziali ai fini dell'espletamento dei processi Aziendali.
- Minimizzare i rischi di accesso non autorizzato, comunicazione non autorizzata, modifica, distruzione, perdita o trattamento improprio delle informazioni di proprietà dell'Azienda.
- Minimizzare la probabilità di accesso non autorizzato, comunicazione non autorizzata, modifica, distruzione, perdita o trattamento improprio delle informazioni di terze parti comunque custodite presso i sistemi informatici Aziendali.

Queste misure intervengono a più livelli:

- **misure preventive**, in grado di contrastare una minaccia, ovvero di prevenire attacchi allo scopo di ridurre il potenziale rischio di danni.
- **misure di risposta**, in grado di rispondere agli attacchi, ovvero di evitare, contenere o minimizzare i danni.
- **misure di analisi e valutazione dei danni** subiti in seguito ad un attacco.
- **misure di ripristino**, a supporto delle attività di ricostruzione della situazione antecedente il danno.

Il monitoraggio della rete è un presupposto essenziale per riconoscere tempestivamente la presenza di problemi e di minacce al corretto funzionamento dell'infrastruttura informatica Aziendale.

Quest'attività viene effettuata nel pieno rispetto dei principi dettati dalla legge (legittimità, opportunità e necessità, garanzia) secondo le seguenti direttive:

- La gestione della rete è effettuata solo dagli incaricati autorizzati dal Responsabile Sicurezza Informatica (Operatori di Help-Desk, System Manager, Network Manager), e solo essi possono accedere ai dati di traffico.

Il monitoraggio viene fatto solo sul traffico che attraversa i varchi di collegamento a Internet e a reti esterne e sull'accesso ai sistemi informativi centralizzati (nei due sensi), per misurare le prestazioni e la disponibilità dei sistemi e delle risorse di rete e per prevenire ed intercettare comportamenti anomali e attacchi che possano compromettere l'operatività della rete e dei sistemi o l'immagine Aziendale.

2 Accesso a Internet

L'uso e la diffusione dell'accesso ad Internet sono condizionati alle best practices ed alle seguenti linee guida e disposizioni:

- Linee Guida del Governo per lo Sviluppo della Società dell'Informazione approvate dal approvate dal Consiglio dei Ministri in data 31 maggio 2002
- Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA
- Cnipa - Centro Nazionale della Pubblica Amministrazione: "Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione: Internet"
- Dlg 196/2003 Protezione in materia di trattamento dei dati personali: Misure minime di sicurezza
- Codice per l'amministrazione digitale, Dgls n. 82/05
- Linee guida del Garante per la posta elettronica e Internet, Gazzetta ufficiale no. 58 del 10 marzo 2007
- Documento programmatico della Sicurezza di ASL 1 Sassari, versione del Marzo 2007.

2.1 Autorizzazioni all'uso di Internet

L'abilitazione di accesso ad Internet soggiace ad autorizzazione. La richiesta di utilizzazione deve essere motivata dai responsabili di Unità Operativa ed inviata al Settore Sistemi Informativi (via e-mail, mediante nota di richiesta, mediante richiesta di intervento dell'Help-Desk).

2.2 Uso di Internet

La struttura informatica che rende possibile l'accesso ad Internet è un'infrastruttura appartenente all'Azienda, che deve essere usata per i legittimi scopi di lavoro da espletare nel quadro della funzione assegnata al collaboratore.

L'uso personale non deve interferire con queste funzioni, o compromettere la sicurezza o l'operatività dell'Azienda.

2.3 Comportamento durante l'accesso ad Internet

Durante l'accesso a risorse Internet da stazioni di lavoro dell'Azienda, gli utenti devono osservare tutti i regolamenti e standard di comportamento previsti per questo ambito. In nessun caso devono tentare di compromettere i sistemi, di appropriarsi o trasferire illegalmente dati o trasmettere messaggi offensivi o abusivi. Inoltre non possono rappresentare ufficialmente l'Azienda, a meno che non siano debitamente autorizzati in questo senso.

Tutti gli utenti abilitati all'uso Internet sono personalmente responsabili di intraprendere le misure necessarie per impedire l'uso non autorizzato del loro accesso ad Internet.

2.4 Trasferimento di dati e/o programmi da Internet

I dati e/o i programmi possono essere trasferiti soltanto dall'Internet alle reti dell'Azienda alle seguenti condizioni:

- Tutti i dati devono essere controllati per accertare se ci sono virus, usando la metodologia e gli strumenti Aziendali prima di essere salvati sulla rete.
- Tutti i dati, applicazioni e/o eseguibili possono servire unicamente allo scopo istituzionale e devono essere acquisiti ed usati conformemente ai regolamenti dell'Azienda alle esigenze della stessa.
- I programmi o le applicazioni eseguibili devono essere testati, facendone richiesta esplicita al Settore Sistemi Informativi (servizio di Help-Desk) per accertare l'idoneità, la compatibilità e la sicurezza prima di essere installati su qualsiasi computer collegato alla rete aziendale. Il Settore Sistemi Informativi dell'Azienda dovrà approvarne l'uso prima dell'installazione, verificandone l'impatto con il sistema Aziendale.

2.5 Collegamento ad Internet

L'unica soluzione autorizzata per accedere ad Internet è quella tramite la rete aziendale messa a disposizione dall'Azienda. Non sono autorizzati collegamenti ad Internet tramite modem dial-out o reti wireless. L'utilizzo della rete wireless è autorizzata, nel contesto di alcune sedi aziendali, solo se adeguatamente protetta da intrusioni esterne. Ogni installazione di rete wireless dovrà essere preventivamente autorizzata dal Settore Sistemi Informativi.

2.6 Cortocircuito di rete e adeguamento a standard aziendali

In nessun caso è permesso di collegare simultaneamente un computer sia alla rete interna dell'Azienda sia ad un modem (cortocircuito di rete).

I PC e/o i server, prima di essere connessi alla rete Aziendale, devono essere verificati ed adeguati in collaborazione con il Settore Sistemi Informativi agli standard Aziendali (sistemi operativi, patches, sistemi di protezione antivirus, ecc.).

2.7 Trasferimento di dati e/o programmi da Internet

L'Azienda non autorizza lo scarico e la diffusione di programmi, eseguibili, giochi, immagini non attinenti l'attività di servizio, da Internet o da altri supporti informatici.

2.8 Monitoraggio automatico

Un sistema elettronico di controllo preventivo traccia la navigazione delle singole stazioni di lavoro, identificandone l'indirizzo IP. La navigazione viene memorizzata e la conservazione dei dati avviene per un periodo minimo di trenta giorni, per il perseguimento di finalità di sicurezza del sistema. Nei casi previsti dalla legge la trascrizione dell'attività conservata nel sistema (log) potrà essere consegnata alle autorità competenti.

2.9 Filtri di navigazione

Per politica Aziendale è limitato il più possibile l'accesso a siti non istituzionali; qualora sorgesse l'esigenza di accedere a siti bloccati, l'interessato dovrà fare richiesta scritta e documentata al Settore Sistemi Informativi dell'Azienda, che provvederà, se del caso, ad autorizzarne l'accesso.

Per ragioni di sicurezza sono inoltre stati apposti specifici filtri tali per cui alcuni siti di natura violenta, pedo-pornografica, ecc. non sono accessibili da Internet.

2.10 Modalità di controllo

L'Azienda si riserva di effettuare controlli sull'utilizzo di Internet tramite i servizi ispettivi competenti e con le seguenti modalità:

- **Controllo per servizi e strutture**. L'Azienda effettua un controllo su dati aggregati riferiti alle stazioni di lavoro utilizzate dai singoli servizi o strutture al fine di verificare eventuali anomalie nel traffico Internet. Qualora le anomalie siano rilevate i servizi competenti dell'Azienda segnalano con un avviso generalizzato riferito alla stazione di lavoro l'utilizzo anomalo degli strumenti Aziendali, e invitano ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.
- **Controllo puntuale**. Qualora siano rilevate ulteriori anomalie dopo il controllo su indicato, i servizi competenti dell'Azienda procederanno ad effettuare controlli più mirati.

Si ricorda che in ogni caso l'uso illecito o non conforme alle presenti disposizioni comporta responsabilità individuale, che potrebbero sfociare in sanzioni, variabili a seconda della gravità dei fatti contestati.

Restano ferme le responsabilità civili e penali previste nell'ambito dell'ordinamento vigente.

3 Posta elettronica

L'uso e la diffusione della posta elettronica sono condizionata alle best practices ed alle seguenti linee guida e disposizioni:

- Linee Guida del Governo per lo Sviluppo della Società dell'Informazione approvate dal Consiglio dei Ministri in data 31 maggio 2002
- Direttiva del Consiglio dei Ministri – Impiego della Posta elettronica nella Pubblica Amministrazione – GU no. 8 del 21.1.2004
- Cnipa- Centro Nazionale della Pubblica Amministrazione: "Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione: Posta Elettronica (PEL)"
- Linee guida per l'uso della Posta elettronica Certificata (PEC) - DPR 11 febbraio 2005, n. 68 (G.U. 28 aprile 2005, n. 97)
- Dlg 196/2003 Protezione in materia di trattamento dei dati personali: Misure minime di sicurezza
- Codice per l'amministrazione digitale, Dgls n. 82/05
- Linee guida del Garante per la posta elettronica e Internet, Gazzetta ufficiale no. 58 del 10 marzo 2007
- Documento programmatico della Sicurezza di ASL 1 Sassari, versione del Marzo 2007.

3.1 Segretezza e riservatezza

L'Azienda considera la posta elettronica come comunicazione riservata tra mittente e destinatario e di conseguenza s'impegna a rispettare e proteggere questa confidenzialità secondo le disposizioni del D.lgs 196/03.

Tuttavia, l'Azienda si riserva il diritto di effettuare controlli sulla posta elettronica dell'utente quando è nell'interesse dell'istituto, e nei limiti di cui al paragrafo dedicato ai controlli.

3.2 Titolarità della posta elettronica

L'Azienda è titolare di tutti i dati memorizzati con l'aiuto di strumenti informatici utilizzati in ambito Aziendale, inclusa la posta elettronica.

3.3 Responsabilità dell'utente per dati trasmessi con la posta elettronica

I sistemi di posta elettronica dell'Azienda hanno, come tutti i sistemi di posta, una sicurezza limitata per ciò che attiene la confidenzialità del messaggio. Di conseguenza, gli utenti devono valutare attentamente come agire al fine di rispettare le misure minime di sicurezza del D. lgs. 196/03, in particolar modo per ciò che attiene il trattamento di dati sensibili.

3.4 Uso della posta elettronica Aziendale

La posta elettronica aziendale è un servizio che appartiene all'Azienda e deve di conseguenza essere usata esclusivamente per gli scopi legittimi di lavoro.

L'Azienda raccomanda di non usare la posta elettronica privata (p.es. hotmail, libero, tiscali, ecc.) per attività di servizio. Queste caselle di posta elettronica non possono infatti garantire i criteri di sicurezza che l'Azienda si è data.

L'utilizzazione della funzionalità di ridirezione della propria posta elettronica aziendale ad una casella di posta elettronica privata esterna non è consentito.

Nello stesso modo, per proteggere la rete dell'Azienda, non è consentito attivare la funzionalità di ridirezione da una propria casella di posta privata a quella aziendale.

In caso di assenza programmata del lavoratore, il medesimo potrà attivare un messaggio automatico di risposta alle e-mail ricevute che indichi a quale altro soggetto o struttura inviare messaggi.

3.5 Raccomandazione sull'invio di dati sensibili o giudiziari

Dato che non è possibile garantire la totale sicurezza dei sistemi di posta elettronica, l'Azienda raccomanda di non inviare tramite posta elettronica le seguenti tipologie di dati che secondo il Codice della Privacy (D.Lgs. 196/03) devono essere trattati con particolare attenzione:

Dati sensibili: dati personali idonei a rilevare lo stato di salute, l'origine razziale ed etnica, le convinzioni religiose, politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati personali che permettono di rivelare la vita sessuale di una persona.

Dati giudiziari: dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti, oppure la qualità di imputato ed indagato ex artt. 60 e 61 c.p.p..

Dati identificativi: dati personali che permettono l'identificazione diretta dell'interessato quando associati a dati sensibili o giudiziari.

Qualora si debba comunque ricorrere, per esigenze di servizio, alla trasmissione di messaggi di posta elettronica che contengono dati ed informazioni aventi le caratteristiche suddette, si raccomanda di ricorrere sempre a forme di protezione dei dati basate su "encription" e compressione dei dati con adeguata password (p.es. lunghezza minima 16 caratteri, contenenti almeno 4 cifre e almeno 4 caratteri speciali, etc.), comunicando successivamente con altra separata modalità la relativa password.

3.6 Uso inadeguato della posta elettronica

Gli utenti non devono utilizzare il servizio di posta elettronica per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi o che violino leggi e regolamenti vigenti.

In particolare, in via esemplificativa e non esaustiva:

- gli utenti non possono immettere in rete, materiale in violazione della legge sul diritto di autore o, di altri diritti di proprietà intellettuale o industriale;
- gli utenti non possono utilizzare il servizio di posta elettronica per fini commerciali e né trasmettere o ritrasmettere messaggi che possono essere considerati come molestie o che possono contribuire a deteriorare il clima di lavoro;

- gli utenti non possono trasmettere materiale e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita o criminosa passibile di responsabilità penale o civile;
- gli utenti non possono immettere in rete informazioni che possono presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio e offensivo, o contrarie alla libertà religiosa e all'autodeterminazione della sfera privata della persona.

3.7 Responsabilità dell'utente

Tutti gli utenti di posta elettronica sono personalmente responsabili dell'invio dei messaggi che vengono spediti dalla propria casella di posta elettronica e non devono quindi consegnare le userid e password a terzi.

In caso di necessità l'Azienda può creare caselle di posta elettronica condivise per le unità operative.

3.8 Caselle di posta elettronica per le unità operative

In caso di necessità l'Azienda può creare caselle di posta elettronica condivise per le unità operative. La casella avrà comunque sempre un responsabile, identificato nel responsabile dell'unità, il quale deciderà l'uso che ne deve essere fatto e gli utenti che hanno accesso alla casella.

3.9 Disclaimer

Questo messaggio deve essere accluso ai messaggi inviati da parte di caselle email dell'Azienda.

Questo messaggio, incluso l'allegato, è da considerare confidenziale. Se è stato ricevuto per errore siete pregati di informare il mittente ed eliminare il messaggio dalla vostra email. La diffusione non autorizzata del messaggio, nella sua completezza o in parte, è proibita. L'Azienda Sanitaria Locale N. 1 non può essere ritenuta responsabile per la trasmissione non autorizzata di questo messaggio o per eventuali danni causati sul vostro sistema.
This message (including any attachments) is confidential. If you have received it by mistake please notify the sender by return e-mail and delete this message from your system. Any unauthorized use or dissemination of this message in whole or in part is strictly prohibited. Azienda Sanitaria Locale N. 1 shall not be liable for the improper or incomplete transmission of the information contained in this communication nor for any delay in its receipt or damage to your system.

3.10 Dichiarazione falsa

La trasmissione dei messaggi di posta elettronica falsificati, come pure l'impersonificazione di un altro utente di posta elettronica è proibita. Nessuno deve cioè usare una casella di posta elettronica assegnata ad un altro utente o falsificare il mittente di un messaggio elettronico.

3.11 Trasmissione di immagini, giochi

E' vietato trasmettere via posta elettronica immagini che non hanno stretta attinenza con l'attività operativa aziendale. E' altresì vietato trasmettere via posta elettronica giochi o eseguibili di programmi.

3.12 Conservazione e cancellazione della posta elettronica

Il provider del servizio di posta elettronica ha il compito di eseguire procedure elettroniche per il salvataggio quotidiano del sistema di posta elettronica.

La cancellazione dei messaggi di posta elettronica è in ogni caso a totale responsabilità degli utenti.

3.13 Interruzione della consegna di posta elettronica

In determinate situazioni può essere necessario dover interrompere il servizio della posta elettronica. Misure del genere saranno unicamente adottate per cause di forza maggiore (esempio aggressioni informatiche, interruzioni del servizio da parte del provider di telecomunicazione, etc.).

3.14 Modalità di controllo

L'Azienda si riserva di effettuare controlli sull'utilizzo della posta elettronica da parte dei singoli dipendenti tramite opportuni servizi ispettivi, e con modalità casuali (p.es. sorteggio) in una percentuale massima annua del 5 % delle caselle di posta elettronica aziendali attive.

I controlli saranno volti ad accertare che l'uso della posta elettronica aziendale non sia effettuata in violazione alle norme qui prescritte; tali controlli saranno svolti con un limitato preavviso ed in presenza dell'utente, che dovrà quindi mostrare all'incaricato dell'attività ispettiva (il quale, in assenza di palesi violazioni sarà tenuto al rispetto della privacy dell'utente) il contenuto corrente della propria casella di posta elettronica.

Si ricorda che in ogni caso l'uso illecito o non conforme alle presenti disposizioni comporta responsabilità individuale, che potrebbero sfociare in sanzioni, variabili a seconda della gravità dei fatti contestati.

Restano ferme le responsabilità civili e penali previste nell'ambito dell'ordinamento vigente.