Sistema Socio Sanitario
Ospedale Maggiore
Regione Lombardia
ASST Crema

VERBALE DI DELIBERAZIONE n. 485

U.O. Sistema Informativo Aziendale

Responsabile del procedimento: Antonella Barbieri

VERBALE DI DELIBERAZIONE
DEL DIRETTORE GENERALE

Il giorno 28 Dicembre 2017 presso la sede legale, il Direttore Generale f.f. Dott. Guido Avaldi ha adottato la seguente deliberazione

OGGETTO: **APPROVAZIONE DEL REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI DELLA ASST DI CREMA**

con l'assistenza del Direttore Amministrativo f.f. che svolge le funzioni di Segretario.

Si attesta che la copia del presente atto viene pubblicata mediante affissione all'Albo, ove rimarrà per 15 giorni consecutivi.

Dal 29/12/2017 al 12/01/2018

f.to Il Direttore Amministrativo
f.f.

Crema, 29/12/2017

IL DIRETTORE GENERALE

RILEVATO

- che risulta sempre più intenso l'utilizzo di risorse informatiche sia per lo svolgimento delle attività sanitarie che per lo svolgimento delle attività amministrativo contabili;

- che questo rilevante impiego richiede che l'utilizzo delle citate risorse avvenga in maniera legittima e nel rispetto della normativa che ne disciplina l'uso al fine di garantire la sicurezza dei dati gestiti e la sicurezza degli stessi sistemi di gestione;

ESAMINATA

- l'allegata proposta di "Regolamento per il corretto utilizzo degli strumenti informatici e telematici dell'ASST di Crema", predisposta dall'U.O. SIA. al fine di precisare le regole a cui i dipendenti devono ottemperare quando li utilizzano e definire le relative responsabilità;

RAVVISATA

- l'opportunità di adottare il suddetto Regolamento quale strumento volto a garantire la sicurezza del sistema informatico dell'Azienda e di conseguenza una gestione sicura dei dati trattati;

Acquisiti i pareri favorevoli per competenza, del Direttore Amministrativo f.f., del Direttore Sanitario e del Direttore Sociosanitario

DELIBERA

Per le motivazioni di cui in premessa:

1. di approvare l'adozione del "Regolamento per il corretto utilizzo degli strumenti informatici e telematici dell'ASST di Crema" in conformità al testo allegato alla presente deliberazione;

2. di stabilire che il seguente atto costituisca parte integrante della presente deliberazione:

   - copia del Regolamento per il corretto utilizzo degli strumenti informatici e telematici dell'ASST di Crema (All.1 composto da nove pagine).

Letto, confermato e sottoscritto:

f.to Il Direttore Generale f.f.
dott. Guido Avaldi

f.to Il Direttore Amministrativo f.f.
dott. Alessandro Cominelli

f.to Il Direttore Sanitario
dott. ssa Ermanna Derelli

f.to Il Direttore Sociosanitario
dott.ssa Mariagloria Mencatelli

REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI DELL'ASST DI CREMA

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa. La realtà Aziendale ha visto aumentare:

- il numero dei servizi informatizzati, con la conseguente necessità di maggiori accessi ad Internet;
- la realizzazione dell'interconnessione di tutti i personal computer e quindi l'accesso alla rete Intranet interna.

Tutto questo ha avuto importanti ricadute sui problemi di sicurezza. Si rende quindi necessario attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi e definire le responsabilità degli utilizzatori delle risorse nel rispetto del testo unico sulla privacy e delle norme vigenti a disciplina del loro utilizzo. L'adozione di queste politiche viene fatta nell'intento di garantire:

- la massima efficienza delle risorse informatiche e del loro utilizzo;
- la riservatezza delle informazioni e dei dati;
- un servizio continuativo nell'interesse dell'Azienda;
- il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- la massima sicurezza nello scambio di dati ed informazioni tra l'Azienda e le altre istituzioni.

E' compito dell'ASST:

- adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici;
- implementare meccanismi di controllo e monitoraggio per evitare intrusioni o abusi, anche mediante installazione di firewall, capaci di monitorare, impedire ed interrompere accessi e uscite sulle porte aperte del sistema durante la connessione ad una rete oppure on line;
- responsabilizzare e formare gli utenti circa i rischi penali, civili e amministrativi connessi all'uso indebito dei mezzi informatici o alla riproduzione non autorizzata di software;
- evitare che i propri utenti, utilizzando gli strumenti informatici dell'Azienda, compiano abusi legati all'utilizzo improprio delle risorse della Rete Internet ed Intranet e dei dati ivi contenuti.

Premesso che l'utilizzo delle risorse informatiche e telematiche Aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, l'ASST di Crema ha adottato il presente regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Il Regolamento Aziendale di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda. Con la Direttiva 26 maggio 2009, n. 2, la Presidenza del Consiglio dei Ministri ha fornito indicazioni in merito all'uso corretto degli strumenti informatici da parte dei lavoratori.

Utilizzo del Personal Computer

II Personal Computer affidato al dipendente è **uno strumento di lavoro;** ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

- L'accesso all'elaboratore è protetto da una password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password è attivata per l'accesso alla rete.
- Non è consentita l'attivazione della password d'accensione (bios).
- Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte del personale al SIA;
- Non è consentito installare autonomamente software, poiché sussiste il grave pericolo di propagare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Tali programmi verranno automaticamente cancellati ed ogni violazione verrà automaticamente segnalata.
- Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'ASST di Crema (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 e successive modifiche ed integrazioni recante nuove norme di tutela del diritto d'autore).
- Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004.
- E' vietato avviare applicativi da chiavetta USB o da qualunque altro supporto esterno, inclusi applicativi via web.
- Gli operatori del Sistema Informativo possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete condivise.
- Non è consentita l'installazione sul personal computer in dotazione di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …) se non preventivamente autorizzato dal SIA.
- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del SIA nel caso in cui siano rilevati virus informatici.
- Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste o necessarie all'attività lavorativa.
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili e dell'archivio della posta settimanalmente. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante.
- La tutela della gestione locale di dati sulle stazioni di lavoro personali – personal computer - che gestiscono localmente documenti e/o dati – è demandata all'utente finale che dovrà

effettuare, con frequenza opportuna, i salvataggi su supporti ottici e/o di rete e la conservazione degli stessi in luogo idoneo.

- Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, gli studi medici e gli ambulatori diurni. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provare in seguito l'indebito uso. In tali frangenti ogni responsabilità sarà addebitata al proprietario delle credenziali.
- Non è possibile spostare personal computer, stampanti ed ogni altro apparato informatico collegato direttamente o indirettamente alla rete, la richiesta deve essere inoltrata al SIA.

Utilizzo di PC portatili

- L'utente è responsabile del PC portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro; il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
- Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
- Non è possibile utilizzare abbonamenti Internet privati per collegamenti alla rete.
- Non è possibile configurare sul portatile utenze personali per accedere alla rete ASST, alle stampanti di rete, alle cartelle condivise ed ai programmi ufficiali.
- E' necessario collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus.
- I pc portatili appartenenti all'ASST non possono essere collegati a reti esterne per evitare la ricezione ed eventuale successiva diffusione di virus informatici.
- E' vietato collegare in rete personal computer portatili non di proprietà dell'ASST (ad esempio consulenti, stagisti, ecc), salvo diversa esplicita preventiva autorizzazione scritta del Dirigente del Settore da inoltrare al SIA.

Utilizzo di dispositivi esterni di memorizzazione dati

chiavette usb, hard disk esterni, macchine fotografiche digitali, iPOD, lettori MP3, ecc.

- E' vietato l'uso dei dispositivi esterni di memorizzazione su tutti i personal computer della rete, salvo diversa autorizzazione. Viene comunque sconsigliato l'uso di tali dispositivi su postazioni con l'accesso da parte di utenti generici, stagisti, consulenti e su postazioni di front-office con servizi rivolti ai cittadini o ritenute strategiche al funzionamento dell'Azienda.
- E' vietato l'uso di dispositivi personali esterni all'Azienda. Il personale dell'ufficio SIA, non essendo in grado di verificare l'attendibilità di tali supporti, non potrà procedere ad eventuali richieste di verifica presenza virus.
- I supporti magnetici e digitali riutilizzabili (Cd, DVD, cassette, chiavi USB …) contenenti dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto

possa essere recuperato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione. I supporti contenenti dati personali devono essere custoditi in archivi chiusi a chiave.

- Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
- Eventuali danni derivanti dalla mancata osservanza del rispetto delle presenti norme saranno imputati al dipendente.

Particolari dispositivi esterni

- E' vietato l'uso e/o l'installazione di software di collegamento/condivisione dati con i personal computer o portatili dei dispositivi, quali telefoni cellulari, navigatori satellitari, ecc., salvo preventiva autorizzazione da parte del SIA.
- E' vietato il collegamento alla rete dati ASST di dispositivi con connessioni di tipo Wireless, Bluetooth o di altra tipologia per scambio dati.

Protezione antivirus

- Il sistema di protezione contro virus informatici è monitorato dal SIA. L'aggiornamento dell'antivirus sui PC connessi in rete avviene in modo automatico.
- Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico Aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..).
- Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al SIA.
- Ogni dispositivo di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.
- Si raccomanda di porre particolare attenzione all'utilizzo di cd/dvd, chiavette USB e memorie di massa.
- Il dispositivo di proprietà dell'Azienda che risulta infetto da virus deve essere OBBLIGATORIAMENTE e TEMPESTIVAMENTE consegnato direttamente dall'utente al personale del SIA.

Gestione delle Password

- Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dal Sistema Informativo.
- L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
- L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di

presidiare l’accesso alla medesima: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

- La password deve essere immediatamente sostituita, dandone comunicazione al Sistema Informativo, nel caso si sospetti che la stessa abbia perso la segretezza.

Uso della posta elettronica

L’abilitazione alla posta elettronica è automatica e contestuale all’assunzione quindi non deve essere preceduta da nessuna richiesta.

- La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro individuale. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- Le password di ingresso al sistema di Web mail sono previste ed attribuite dall’Amministratore del Sistema. E’ consentita la modifica solo su richiesta degli utenti al SIA.
- La dimensione massima delle caselle postali è limitata; superata tale quota è comunque garantita la ricezione di nuovi messaggi, non vengono salvati i messaggi inviati e non è possibile cancellare in autonomia messaggi per liberare spazio.
- Per la trasmissione di file all'interno dell’azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 10 MB.
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto gli allegati ingombranti.
- Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.jpg).
- Nel caso in cui si debba inviare un documento all’esterno dell’ Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software è fornito ed è installato su tutti i Pc aziendali.
- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus è necessario cancellare i messaggi senza aprirli.
- Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.
- E' obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
- E’ vietato inviare catene telematiche (o di Sant’Antonio). Se si ricevono messaggi di tale tipo, è necessario non attivare gli allegati di tali messaggi e non rispondere ad essi al fine di evitare danni alla rete e limitare l'efficienza del sistema di posta.
- L’iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- E’ vietato configurare account di posta elettronica diversi da quelli aziendali sul proprio personal computer.

Uso della rete Internet e dei relativi servizi

II servizio Internet ha l'obiettivo primario di favorire la comunicazione verso l'esterno, oltre che favorire il reperimento e la divulgazione di informazioni utili per lo svolgimento della propria professione. In particolare il servizio Internet si articola nelle seguenti finalità:

- consentire l'accesso alla rete internet World Wide Web da parte degli utenti della Azienda preventivamente autorizzati;
- permettere la gestione del sito ufficiale della Azienda, rivolto al pubblico, cui possono accedere gli utenti di internet;
- permettere la pubblicazione sul sito ufficiale della Azienda di raccolte di informazioni, documenti e dati.

- II PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
- L'abilitazione ad Internet deve essere preceduta da regolare richiesta del Responsabile di funzione/unità operativa al Sistema Informativo.
- Non possono essere utilizzati modem privati per il collegamento alla rete.
- E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Sistema Informativo e l'uso di Internet per lo scarico di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso professionale.
- E' vietato all'utente accedere a siti che offrano contenuti audio/video tramite streaming (stazioni radio – televisione on line, youtube, ecc.).
- E' vietato all'utente accedere a servizi per l'invio e la condivisione di files (DropBox, DropSend, WeTransfer …).
- E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
- E' 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, decriptare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.
- E' vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni remote banking, attività di broking (brokeraggio) e trading, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Dirigente nel rispetto delle normali procedure di acquisto.
- E' vietata la consultazione della posta elettronica privata e di qualunque altro riferimento estraneo al sistema di posta elettronica dell'Azienda.

Accesso dall'esterno alla rete intranet

L'accesso alle risorse del sistema intranet dall'esterno è consentito solo tramite VPN (Virtual Private Network). Su richiesta scritta ed assunzione di responsabilità l'Amministratore di Sistema può, verificati i requisiti di sicurezza, concedere le credenziali di accesso alla rete VPN.

Non osservanza della normativa Aziendale e delle disposizioni in materia di Privacy

- E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, così come altresì indicato nella lettera di incarico per il trattamento dei dati di cui al D. Lgs. n. 196 del 30 giugno 2003.
- Il mancato rispetto o la violazione delle regole contenute nel D.Lgs. n. 196 del 30 giugno 2003 è perseguibile con le azioni civili e penali previste.
- Il mancato rispetto o la violazione delle norme contenute nel presente regolamento può comportare l'applicazione di sanzioni disciplinari, in ottemperanza alle disposizioni disciplinari di cui ai CCNL.
- Il presente regolamento, che costituisce un'appendice ai codici disciplinari dell'Azienda, ai sensi dell'art. 54 – comma 5 – del D. Lgs. n. 165/2001 è soggetto a pubblicazione nella rete intranet dell'ASST in conformità a quanto previsto dall'art. 3 dei predetti codici disciplinari.

Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione al Sistema Informativo.
Il presente Regolamento è soggetto a revisione ogni qualvolta se ne rappresenti la necessità.