SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Ferrara

Università degli Studi di Ferrara

Procedure in materia di Privacy

(dato informatico)

Premessa

Gli strumenti informatici rappresentano da un lato un mezzo insostituibile di lavoro (se adoperati nel rispetto del principio della diligenza e correttezza) e dall'altro lato un rischio per la sicurezza del patrimonio aziendale (se utilizzati in modo non idoneo).

Si rende pertanto necessaria l'adozione da parte dell'Azienda Ospedaliera – Universitaria di Ferrara del presente documento finalizzato a disciplinare il regolare utilizzo dei predetti strumenti, con particolare riferimento alle seguenti problematiche:

1) utilizzo del computer (fisso e portatile)
2) gestione della password
3) utilizzo della rete (aziendale e internet)
4) utilizzo della posta elettronica
5) protezione
6) salvataggio
7) smaltimento
8) controlli
9) inosservanza
10) aggiornamento.

Le disposizioni di seguito devono essere conosciute ed applicate dai soggetti autorizzati che accedono agli strumenti informatici aziendali e/o connessi al perseguimento di finalità aziendali.

1) Utilizzo del computer (fisso e portatile)

Il computer che l'utente ha ricevuto in dotazione è uno strumento di lavoro da utilizzarsi nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo aziendale e/o previste dalla legge.

Il computer presenta caratteristiche hardware e software impostate dal Sistema informatico e che non possono essere modificate.

La gestione locale dei dati deve scomparire ed essere sostituita da gestione centralizzata su server.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema informatico il quale può altresì procedere alla rimozione di file o applicazioni che ritiene pericolosi per la sicurezza.

E' vietato l'uso di supporti removibili per la memorizzazione di dati sensibili.

Durante l'uso del computer l'utente deve vigilare affinché i dati in esso contenuti non siano oggetto di accesso non autorizzato.

In pausa pranzo e nel caso di prolungata assenza dall'ufficio deve essere attivata la modalità "blocca computer".

Alla fine della giornata lavorativa è necessario disconnettere il computer.

Periodicamente è opportuno "pulire" il computer mediante la cancellazione di file superati o inutili.

Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004 (interventi antipirateria).

L'utente è responsabile del computer portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo.

Ai portatili si applicano le stesse regole di utilizzo previste per i computer fissi.

II portatile deve essere presidiato direttamente oppure riposto in luogo sicuro.

L'utente non deve utilizzare abbonamenti internet privati per effettuare collegamenti alla rete.

2) Gestione della password

Per accedere alla rete è necessario utilizzare il proprio profilo personale come configurato e autorizzato dal Sistema informatico.

Il trattamento di dati personali con strumenti elettronici è consentito agli utenti dotati di credenziale di autenticazione (ad esempio password, smart card eccetera) segreta e esclusiva dell'utente stesso.

La password deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

L'utente deve creare una password priva di riferimenti banali (ad esempio è sconsigliato indicare il proprio nome, la propria data di nascita, il nome del coniuge eccetera)

L'utente deve modificare la password al primo utilizzo e, successivamente, almeno ogni sei mesi.

Nel caso di trattamento di dati sensibili e di dati giudiziari la password è modificata almeno ogni tre mesi.

L'utente autorizzato a trattare dati personali deve adottare le necessarie cautele per assicurare la segretezza e l'esclusività della password (ad esempio non scrivere la password su promemoria da appiccicarsi al computer né adottare procedure automatiche).

Nel caso in cui l'utente reputi che la password abbia perso la necessaria caratteristica di segretezza la stessa deve essere immediatamente sostituita previa comunicazione al Sistema informatico.

3) Utilizzo delle reti (aziendale e internet)

L’accesso alla rete è consentito nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo aziendale e/o previste dalla legge.

L’utente non può accedere a internet per perseguire scopi privati e/o vietati dalla legge ma solo per ragioni di lavoro al fine di raggiungere obbiettivi di studio, ricerca e documentazione.

E’ vietato connettere in rete postazioni di lavoro se non in virtù di autorizzazione del Sistema informatico.

E’ vietata l’installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l’accesso a banche dati esterne o interne all’azienda.

E’ vietato scaricare programmi da siti internet se non previa autorizzazione del Sistema informatico.

E' vietata la partecipazione a forum, chat line, bacheche elettroniche non autorizzate.

L’Azienda si riserva la facoltà di bloccare l’accesso a siti ritenuti non consoni allo svolgimento dell’attività lavorativa e/o comunque non affidabili.

4) Uso della posta elettronica

L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta al Sistema informatico.

La casella di posta è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

Nel caso di messaggi provenienti da mittenti conosciuti con allegati però sospetti (ad esempio file exe, scr, pif, bat, cmd), questi ultimi non devono essere aperti.

L'utente non deve rispondere o partecipare alle cosiddette "catene di sant'Antonio".

Nell'ipotesi di invio di allegati "pesanti" l'utente deve utilizzare un formato compresso (zip, jpg).

L'utente deve controllare i file in allegato di posta elettronica prima del loro utilizzo.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, superati, ingombranti.

E' concesso l'uso della posta elettronica come mezzo di comunicazione personale a condizione che il tempo e i mezzi impiegati siano di entità trascurabile.

5) Protezione

L’utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale.

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del programma antivirus aziendale e consentire i periodici aggiornamenti dello stesso.

Nel caso che il programma antivirus rilevi la presenza di un virus l’utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al Sistema informatico.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.

I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi.

Il trasporto dei dati genetici all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti.

6) Salvataggio

L’utente deve provvedere ad effettuare il salvataggio dati, con frequenza giornaliera, su rete o su supporto magnetico.

Nel caso di salvataggio su supporto l’utente deve sostituire periodicamente gli stessi e provvedere alla loro conservazione in un luogo sicuro.

7) Smaltimento

Tutti i supporti contenenti dati riservati devono essere smaltiti in modo da evitare la divulgazione di informazioni riservate.

I supporti rimovibili contenenti dati contenenti dati sensibili o dati giudiziari se non utilizzati sono distrutti o resi inutilizzabili.

Possono essere riutilizzati da altri soggetti se le informazioni precedentemente in essi contenute non sono intelligibili né tecnicamente in alcun modo ricostruibili.

8) Controlli

L’Azienda 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 nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dallo Statuto dei lavoratori e dal Codice Privacy.

In particolare sarà possibile verificare gli accessi a internet e i tempi di connessione senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal Garante 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 dall’Azienda se necessario per far valere o difendere un diritto in sede giudiziaria.

9) Inosservanza delle disposizioni

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

L'utente è considerato direttamente responsabile per un eventuale accesso illecito.

L'utente è considerato direttamente responsabile per l'appropriazione indebita del materiale cartaceo utilizzato per stampare i risultati della navigazione.

L'utente è considerato direttamente responsabile per il danneggiamento della rete aziendale a causa dei virus informatici introdottisi.

E' fatto salvo il diritto dell'Azienda di chiedere l'ulteriore risarcimento del danno.

10) Aggiornamento

Il presente Regolamento è soggetto a revisione con frequenza periodica e si inquadra nel più ampio obbligo di sicurezza che l'Azienda adempie al fine di proteggere i dati personali in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Al fine di scoprire e comunicare le possibili violazioni al sistema informatico è necessaria la collaborazione dell'utente nel segnalare ogni anomalia (ad esempio smarrimento o furto di informazioni, virus, violazioni di sicurezza).

A tal fine è possibile dare comunicazione al Sistema informatico affinché adotti le necessarie contromisure e per proporre altresì le integrazioni al presente Regolamento ritenute opportune.

GLOSSARIO

***

- trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

- dato personale: 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: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di 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;

- dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60-61 del codice di procedura penale;

- titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

- responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

- incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

- interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

- comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

- misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 31.