Disciplinare Interno
per l’utilizzo delle Risorse Informatiche

Indice

Premessa

L'ASL mette a disposizione del personale e di eventuali collaboratori esterni i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- Strumenti di informatica individuale, quali Personal Computer (PC) installati sul posto di lavoro, computer portatili ecc..
- Servizi di Posta Elettronica e Internet.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le normative vigenti.

Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare, al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'ASL, nonché l'ambito di eventuali verifiche effettuate dall'ASL sulla funzionalità e sicurezza del propri sistemi informativi.

In particolare, l'utilizzo delle risorse informatiche non inerente all'attività lavorativa, può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza delle infrastrutture dell'ASL.

Con il presente Disciplinare si intendono ribadire, anche a seguito dell'emanazione della Direttiva n. 2/09 del Dipartimento della Funzione Pubblica, alcune disposizioni generali in ordine al divieto di uso privato delle attrezzature e degli strumenti informatici messi a disposizione dalla ASL e si introducono disposizioni specifiche finalizzate a rendere operativo l'uso privatistico delle attrezzature. Saranno i Dirigenti ad adottare le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità delle risorse informatiche assegnate alle singole Strutture o Servizi.

Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare, dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali. Tra questi rientrano le "Linee guida del Garante per Posta elettronica e Internet" emesse in data 1 marzo 2007.

Va, infine, evidenziato che l'ASL si riserva di verificare, nei limiti consentiti dalle norme legali e contrattuali e con modalità diffuse ed uniformi, il rispetto delle presenti istruzioni e l'integrità dei propri sistemi.

L'ASL non effettua registrazioni per il controllo dell'attività lavorativa del dipendente, ma solo registrazioni volte a salvaguardare la sicurezza e il mantenimento dell'efficienza dei sistemi. I dati registrati a tale scopo dai sistemi non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

- Campo di applicazione

Le regole del presente disciplinare devono essere rispettate da tutto il personale dell'ASL indipendentemente dal tipo di incarico svolto e dalla Sede dell'attività.
E' demandato a ciascuno dei Dirigenti di struttura il compito di verificare e monitorare il rispetto delle regole di seguito evidenziate.

- Normativa di riferimento

Il presente Disciplinare interno è redatto in conformità alla normativa in materia di protezione dei dati personali, nonché alla normativa di seguito riportata:

- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori", tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela dei programmi per elaboratori, all'art. 171 della Legge n°633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n° 248/2000 "Nuove norme di tutela del diritto di autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne le copie.
- Legge 20 maggio 1970, n.300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori); in particolare l'art.4 vieta di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori
- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"
- Codice Penale art. 616 Violazione, sottrazione e soppressione di corrispondenza- "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino ad un anno e con la multa da sessanta a un milione. Se il colpevole, senza giusta causa rivela, in tutto o in parte, il contenuto della corrispondenza, è punito se dal fatto deriva nocumento ed il fatto non costituisce un più grave reato, con la reclusione fino ai tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella telegrafica, epistolare, telefonica, informatica, o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.
- Decreto Legislativo 30 giugno 2003, n° 196 "Codice in materia di protezione dei dati personali", garantisce che il trattamento dei dati personali si svolga nel

rispetto dei diritti e delle libertà fondamentali nonché della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure logiche, fisiche e organizzative che devono essere adottate al fine di:

1. evitare possibili distruzioni, perdite e alterazioni di dati;
2. garantire che l'accesso ai dati sia effettuato dalle sole persone incaricate al trattamento e quindi autorizzate
3. garantire che il trattamento avvenga per le finalità e nelle modalità consentite.

Le misure di sicurezza sono applicate garantendo il rispetto di quanto disposto dalle "Linee guida del Garante per posta elettronica e internet" emesse dall'autorità Garante per la protezione dei dati personali il 1 marzo 2007.

1 Utilizzo del Personal Computer

1.1 Il Personal Computer affidato al dipendente è **uno strumento di lavoro.** Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione dall'ASL. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'utente è, altresì, responsabile dello stato di efficienza delle attrezzature informatiche, che gli sono state affidate in uso, segnalando tempestivamente al SIA ogni eventuale problema tecnico e in caso di dubbio, sulla sicurezza della postazione di lavoro.
Le segnalazioni al SIA devono arrivare al Fax 0783317042 o alla mail sia@asloristano.it

1.2 L'attivazione della password d'accensione (bios) è consentita solo dietro espressa autorizzazione del Dirigente della struttura di appartenenza che inoltrerà apposita richiesta al SIA.

1.3 Qualunque modifica delle caratteristiche hardware e software impostate sui PC, deve essere autorizzata dal Dirigente della struttura di appartenenza, previo parere tecnico del SIA.

1.4 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio

1.5 Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa

1.6 Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante

1.7 La tutela della gestione locale di dati su 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 magnetici e/o di rete e la

conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili

1.8 Le gestioni locali dei dati dovranno scomparire per essere sostituite da gestioni centralizzate su server

1.9 Non è consentita l'installazione di programmi diversi da quelli autorizzati Dirigente della struttura di appartenenza, previo parere tecnico del SIA.

1.10 Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004

1.11 Gli operatori del SIA 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, previa autorizzazione del Dirigente interessato.

1.12 Non utilizzare in azienda risorse informatiche private senza autorizzazione del Dirigente della struttura di appartenenza, previo parere tecnico del SIA. In caso di autorizzazione all'utilizzo di risorse private, l'utente è comunque tenuto al rispetto delle configurazioni standard dell'ASL.

1.13 Proteggere, in caso di abbandono momentaneo della postazione di lavoro, la postazione richiamando le funzioni di sicurezza del S.O. ed assicurandosi dell'attivazione della funzione Lock Workstation o in alternativa impostando lo screen saver che si attivi dopo 4/6 minuti di inattività o chiudere la sessione di lavoro.

1.14 In caso di smarrimento o furto delle risorse informatiche provvedere immediatamente a sporgere regolare denuncia alla competente autorità giudiziaria ed inviarne copia al SIA, al quale occorre comunicare immediatamente anche i dati aziendali che erano contenuti nel computer.

Le suddette norme comportamentali devono essere sempre rispettate anche nel caso di risorse informatiche non direttamente fornite dal SIA, ma acquisite a vario titolo.

2. Utilizzo della rete dell'ASL

2.1 L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale

2.2 E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati

2.3 E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Dirigente interessato, previo parere tecnico del SIA.

2.4 E' vietato condividere cartelle in rete (né dotate di password, né sprovviste di password).

2.5 E' vietato monitorare ciò che transita in rete.

2.6 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.

3. Gestione delle Password

3.1 Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dal SIA su richiesta del Dirigente della Struttura di appartenenza del Dipendente. Al riguardo è individuato un modulo di "Concessione/Revoca/Modifica abilitazioni applicative" che i responsabili dei trattamenti utilizzeranno per le comunicazioni del caso al SIA.

3.2 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

3.3 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

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

3.5 Cambiare la password obbligatoriamente ogni tre mesi o immediatamente se compromessa.

3.6 Comporre la password con almeno 8 caratteri alfanumerici, o nel caso lo strumento elettronico non lo consenta, con un numero di caratteri pari al consentito.

3.7 Usare, preferibilemente, nella composizione della password almeno un carattere numerico, uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale.

3.8 Non permettere ad altri utenti di operare con il proprio identificativo utente.

3.8 Non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi.

Sebbene la password sia personale e riservata è bene tenere presente che in caso di prolungata assenza ed impedimento dell'utente, che renda indispensabile e indifferibile si applica quanto previsto per il servizio di posta elettronica nel § 2.2.3. Pertanto, il Responsabile della struttura di appartenenza dell'utente, può richiedere al SIA che venga effettuato il reset della password dell'utente stesso. Al termine del tempo strettamente necessario al recupero delle informazioni di lavoro protette da password, il suddetto Responsabile dovrà richiedere al SIA un nuovo reset della password che, questa volta, sarà comunicato al tempestivamente ed esclusivamente all'utente interessato.

4. Gestione di banche dati locali

Nel caso in cui sorga la necessità di elaborare delle banche dati, diverse da quelle centralizzate, in formato per esempio excell o access, è necessario adottare misure di sicurezza più idonee a garantire il rispetto della normativa privacy sia sotto il profilo della identificazione ed autenticazione, del back up e ripristino dei dati che della disponibilità degli stessi. Pertanto, è necessario concordare con il SIA le modalità operative di gestione di tali banche dati.

5. Supporti di memorizzazione dati

Nel caso in cui siano utilizzati supporti informatici quali floppy disk, cd-rom o pen drive per la memorizzazione di dati sensibili e/o personali, devono essere osservate le seguenti misure di sicurezza al fine da salvaguardare la riservatezza dei dati:

- I supporti informatici devono essere conservati in un luogo sicuro al fine di evitare accessi non autorizzati e trattamenti non consentiti
- I supporti informatici se non utilizzati devono essere distrutti o resi inutlizzabili
- I supporti informatici possono essere riutilizzati solo dopo aver provveduto a cancellare i dati in essi contenuti; l'operazione deve essere fatta in modo che i dati precedentemente memorizzati non siano tecnicamente in alcun modo recuperabili. In caso contrario è necessario distruggere i supporti.

6. Utilizzo di PC portatili

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.

6.1 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.

6.2 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.

6.3 I PC portatili utilizzati all'esterno (convegni, ed altro), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6.4 Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

6.5 Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server)/Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale, utilizzare la password in modo rigoroso.

6.6 Disconnettersi dal sistema RAS al termine della sessione di lavoro.

6.7 Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus.

6.8 Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

7. Uso della posta elettronica

L’ASL adotta tecnologie dell’informazione e della comunicazione nei rapporti interni ed, in particolare, mette a disposizione del personale indirizzi di posta elettronica individuale e/o d’ufficio.

La Direzione Generale, per motivi tecnici e di sicurezza ed, in particolare per prevenire o curare malfunzionamenti, può autorizzare l’effettuazione in caso di necessità, un analisi in tempo reale delle componenti di traffico (file di log) riferite alle postazioni di lavoro che accedono alla rete.

Nell’uso della posta elettronica, devono osservare le seguenti norme comportamentali:
7.1 La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse

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

7.3 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.

7.4 Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.

7.5 Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.jpg).

7.6 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 specifico è fornito dal SIA previa richiesta.

7.7 non è consentito l’utilizzo della posta elettronica aziendale per la partecipazione a dibattiti, forum, mailing-list, ecc., che determinano un sovraccarico della rete e creano disservizi agli utenti. L’iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

7.8 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

7.9 La Posta Elettronica costituisce uno strumento ordinario e obbligatorio, salvo casi eccezionali debitamente motivati, per la trasmissione di file all'interno dell’Azienda.

7.10 E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

7.11 Non è consentito, per nessuna ragione, spedire o rispedire posta che contenga materiale pubblicitario.

7.12 E' illecito scambiare messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale.

7.13 Mantenere riservata la password di accesso al servizio di Posta elettronica, provvedendo a modificarla almeno ogni sei mesi ed immediatamente qualora si sospetti che sia venuta a conoscenza di terzi. Ciò al fine di evitare che un utente malintenzionato divulghi informazioni di qualsiasi tipo riconducibili ad un mittente inconsapevole. Tali norme vanno osservate anche per i messaggi di posta salvati nella memoria locale della propria postazione di lavoro (es. file.PST).

7.14 Il personale ASL in caso di assenza programmata (ad es. ferie o altro), deve adottare le misure organizzative più idonee per assicurare la corretta gestione dei messaggi necessari al normale svolgimento dell'attività lavorativa ed alla conseguente continuità della stessa. L'Azienda mette a disposizione apposite funzionalità di sistema che consentono di impostare un messaggio di risposta automatica (Out of Office Replay). In caso di assenza programmata, l'utente è quindi tenuto ad attivare messaggi di risposta automatica che comunicano l'assenza e devono contenere i riferimenti (sia elettronici che telefonici) di Uffici e/o utenti cui rivolgersi in caso di necessità.
Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (ad es. per malattia) ed il lavoratore non possa attivare la procedura sopra descritta, l'azienda si riserva la possibilità di attivare analogo accorgimento, avvertendo gli interessati.

Nel caso di assenza improvvisa o prolungata, e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica o di altri dati aziendali che siano nell'esclusiva disponibilità del dipendente (es. file.PST), il Responsabile della Struttura di appartenenza dell'utente può richiedere, per iscritto, al SIA che venga effettuato il reset della password dell'utente stesso. Della modifica, alla prima occasione utile, deve essere tempestivamente informato l'utente interessato in modo da metterlo in condizione di cambiare la password.

8. Uso della rete Internet e dei relativi servizi

8.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
8.2 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
8.3 Non possono essere utilizzati modem privati per il collegamento alla rete.
8.4 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Sistema Informativo.
8.5 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).
8.6 E' consentito l'uso di internet per svolgere attività che non rientrano tra i compiti istituzionali solo in casi particolari in cui sia necessario assolvere ad incombenze

amministrative o burocratiche (es. effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari o assicurativi) per le quali occorrerebbe altrimenti allontanarsi dal luogo di lavoro. Nei casi succitati l'utilizzo di internet è consentito solo per il tempo strettamente necessario ad effettuare le transazioni.

9. Cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti una modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Azienda qualsiasi risorsa assegnata, sia le attrezzature informatiche sia le informazioni di interesse aziendale secondo quanto di seguito specificato:

- La casella di posta individuale sarà mantenuta attiva per il tempo necessario a gestire il passaggio di consegne.
- L'utente **non può cancellare** le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete, senza l'autorizzazione della Direzione Generale.
- Qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità dell'Azienda.

10 Protezione antivirus

10.1 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..).

10.2 Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.

10.3 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 segnalare l'accaduto al SIA (sia@asloristano.it).

10.4 Ogni dispositivo magnetico 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.

11 Non osservanza della normativa aziendale

11.1 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.