Identificativo: 01 Rev.0

Data: 30/11/2017

ASL AL

AL REGOLAMENTO AZIENDALE DI UTILIZZO DELLE POSTAZIONI DI LAVORO

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 nuova realtà Aziendale ha visto aumentare il numero dei servizi informatizzati, con la conseguente necessità di maggiori accessi ad Internet ed in ultimo 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 del documento programmatico sulla sicurezza (DPS). L'adozione di queste politiche viene fatta nell'intento di:

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

E' compito dell'Ente:

- 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, se del caso, 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, 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'Ente, 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'Azienda Sanitaria Locale AL ha adottato il presente regolamento, promosso dal S.O.C. Sistema Informativo, alla luce del "Piano programmatico Aziendale sulla sicurezza informatica", 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, ma anche alle modalità di controllo da parte dei datori di lavoro; (le disposizioni sono consultabili sul Sito Aziendale), al fine di evitare abusi quanto all'uso privato di internet e della posta elettronica. La Direttiva sottolinea l'ampia distribuzione di tali risorse tra i dipendenti, che ne favorisce il diffuso utilizzo anche per finalità diverse da quelle lavorative.

Tali prescrizioni si aggiungono e integrano le norme già previste dal **"Piano programmatico sulla sicurezza informatica" adottato dalla Azienda Sanitaria Locale AL con delibera n. 896 del 30.03.2009.**

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; Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza;

1.2. Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte della S.C. Sistema Informativo;

1.3. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte del personale della S.C. Sistema Informativo;

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 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 e dell'archivio della posta settimanalmente. Particolare attenzione deve essere prestata alla duplicazione dei dati: è' infatti assolutamente da evitare un'archiviazione ridondante;

1.7. I PC assegnati al personale non sono soggetti a backup; si sconsiglia di salvare dati lavorativi in locale se non per periodi limitati di tempo. I dati lavorativi devono essere conservati nelle apposite aree di rete messe a disposizione e soggette a backup. 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 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; ogni utilizzo di questi supporti da parte dell'utente oltre che essere considerato una violazione di tale divieto, è sotto la responsabilità dell'utente;

1.8. Le gestioni locali dei dati dovranno cessare per essere sostituite da gestioni centralizzate su server;

1.9. I dati idonei a rivelare lo stato di salute e la vita sessuale dei pazienti devono essere salvati solo all'interno dei software in dotazione specifici per il loro trattamento. Tali dati non devono essere conservati sui PC in dotazione degli utenti o nelle aree di rete condivise. Tale divieto vale in modo particolare per i dati di natura genetica dei pazienti;

1.10. Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Aziendale;

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

1.12. 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.

1.13. In caso di necessità urgenti di sicurezza, gli Amministratori di Sistema possono accedere ai dati contenuti nel PC dell'utente. L'accesso avverrà tramite le credenziali privilegiate dell'amministratore. L'utente dovrà essere avvisato di tali interventi straordinari.

2 Utilizzo della rete dell'ASL AL

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 Sistema Informativo Aziendale;

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

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 dalla Area del Sistema Informativo. Al riguardo è individuato un modulo di "Concessione/Revoca/Modifica abilitazioni applicative" che i Responsabili dei trattamenti utilizzeranno per le comunicazioni del caso alla S.O.C. Sistema Informativo;
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 alla Area del Sistema Informativo, nel caso si sospetti che la stessa abbia perso la segretezza.
3.5. La prima password viene inviata in busta chiusa all'utente che, al primo utilizzo, sarà forzato alla sua modifica.
3.6. La password deve rispettare i requisiti di complessità riportati nel documento "Modalità gestione password di rete";

4 Utilizzo di PC portatili

4.1. 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;
4.2. 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;
4.3. I PC portatili utilizzati all'esterno (convegni, visite in Azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto;
4.4. Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari;
4.5. Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus;
4.6. Non utilizzare abbonamenti Internet privati per collegamenti alla rete;
4.7. In caso di necessità urgenti di sicurezza, gli Amministratori di Sistema possono accedere ai dati contenuti nel PC portatile dell'utente. L'accesso avverrà tramite le credenziali privilegiate dell'amministratore. L'utente dovrà essere avvisato di tali interventi straordinari.

5 Uso della posta elettronica

5.1. Il servizio di posta elettronica è concesso esclusivamente agli incaricati abilitati come supporto per il raggiungimento dei fini lavorativi e istituzionali dell'Ente.
5.2. L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa al Sistema Informativo, che dovrà oggettivamente motivare la richiesta.
5.3. Il sistema è soggetto ad un controllo preventivo su ogni casella tramite strumenti di filtro di protezione antispam/antivirus
5.4. La dimensione della casella di posta rilasciate dall'amministratore di sistema è in funzione delle risorse disponibili e delle esigenze di servizio

5.5. 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;
5.6. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli;
5.7. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd .vbs .js), questi ultimi non devono essere aperti;
5.8. Evitare la diffusione incontrollata di sistemi per propagare messaggi che inducono il destinatario a produrne molteplici copie da spedire, a propria volta, a nuovi destinatari. "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) che limitano l'efficienza del sistema di posta;
5.9. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.jpg);
5.10. 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 CED previa richiesta;
5.11. L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile;
5.12. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
5.13. 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 25 MB.;
5.14. 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);
5.15. È fatto divieto di trasmissione a mezzo posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di dati personali (D.lgs 196/03)
5.16. In caso di necessità urgenti di sicurezza, gli Amministratori di Sistema possono accedere ai dati contenuti nella casella di posta elettronica dell'utente. L'accesso avverrà tramite le credenziali privilegiate dell'amministratore. L'utente dovrà essere avvisato di tali interventi straordinari.
5.17. Trascorso un mese dalla data di termine del rapporto di lavoro, la casella di posta elettronica dell'ex dipendente viene cancellata.

6 Uso della rete internet e dei relativi servizi

Il 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:

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

6.1. L'abilitazione ad Internet deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa al Sistema Informativo;
6.2. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa;
6.3. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa;
6.4. Non possono essere utilizzati modem privati per il collegamento alla rete;

6.5. E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Area del 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 d'ufficio;

6.6. E' fatto divieto all'utente accedere a siti che offrano contenuti audio/video tramite streaming (stazioni radio – televisione on line youtube, ecc.);

6.7. 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);

6.8. 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.

7 Documentazione dell'attività di navigazione

7.1. L'accesso ai siti internet da parte di un qualsiasi utente può essere documentato automaticamente in un log, che riporta i dettagli della navigazione, che elenca i siti e i documenti che l'utente ha consultato;

7.2. I log sono memorizzati in modo protetto sul server di sistema e potranno eventualmente essere visionati da:

a) Responsabili di Servizio; (report del sevizio)
b) Amministratore di Sistema (solo per fini legati alla sicurezza informatica).

8 Finalità

8.1. Le finalità del servizio intranet sono:

a) semplificazione e potenziamento delle modalità di comunicazione ed informazione interna su oggetti, temi ed attività la cui conoscenza sia funzionale al miglior svolgimento dell'attività dell'Amministrazione nel caso sia utile dare notizia in terna e soprattutto sull'attività dei singoli servizi con particolare riguardo sia alle procedure concernenti l'elaborazione di atti normativi e di indirizzo, sia alle procedure concernenti l'attività amministrativa e gestionale. Pertanto, lo scopo della rete intranet è quello di rendere più facile il reperimento di informazioni utili per lo svolgimento dei compiti istituzionali mediante l'attivazione di un unico "serbatoio di informazioni" dove viene semplificato, in virtù di un sistema digitale di gestione degli stessi, l'accesso ai dati e documenti di interesse comune;
b) favorire l'efficienza e l'economicità dell'attività amministrativa e della gestione, attraverso la semplificazione dei processi organizzativi interni, il rafforzamento della cooperazione tra gli uffici e la condivisione delle esperienze lavorative;
c) creare e sviluppare sinergie e scambi di informazioni con il sito internet, agevolando il flusso di informazioni, al fine di offrire ai cittadini l'accesso ai documenti pubblici nonché l'interscambio di informazioni e dati con altre Pubbliche Amministrazioni;
d) rappresentare il portale della comunicazione interna dell'Ente.

9 Accesso dall'esterno alla rete internet

9.1. L'accesso alle risorse del sistema intranet dall'esterno è consentito 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

10 Accesso area riservata

10.1. In questa zona del sito esiste un' area protetta e personalizzata i cui contenuti relativi a documenti, dati, programmi, modulistica, accesso esterno alla posta elettronica Aziendale sono riservati ad utenti con ruoli e permessi diversi, muniti di idonee credenziali d'accesso alla rete.

11 Protezione antivirus

11.1. 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..);

11.2. Ogni utente è tenuto a controllare la presenza ed il regolare funzionamento del software antivirus aziendale. 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 alla Area del Sistema Informativo;

11.3. 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;

11.4. Il CED ha predisposto una specifica casella di posta elettronica denominata admin@aslal.it a cui inviare notizie di anomalie o problematiche varie relative a virus ed antivirus.

12 Osservanza delle disposizioni di Privacy

12.1. E' obbligatorio attenersi alle disposizioni di cui al Regolamento sulle misure minime di sicurezza e al Documento di Programmazione e sicurezza di cui alle delibera n. 896 del 30.03.2009.visualizzabile nel sito Internet dell' Azienda www.aslal.it.

13 Non osservanza della normativa aziendale

13.1. 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.

14 Aggiornamento e revisione

14.1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione alla Area del Sistema Informativo;

14.2. Il presente Regolamento è soggetto a revisione ogni qualvolta se ne rappresenti la necessità.