Azienda U.S.L. 106 - Teramo

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE E DEI SERVIZI INFORMATICI AZIENDALI

INDICE PER ARGOMENTI

PREMESSA

La progressiva diffusione delle nuove tecnologie ICT ed in particolare l'utilizzo della posta elettronica ed il libero accesso alla rete Internet, espone l'Azienda U.S.L. e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura tecnica e patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (diritto d'autore, privacy, ecc.), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda U.S.L. ha predisposto il presente Regolamento Informatico Aziendale per il corretto utilizzo di apparecchiature e servizi informatici, allo scopo di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che l'Azienda U.S.L., nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti e collaboratori apparecchiature informatiche e mezzi di comunicazione efficienti (Personal Computer, Notebook, casella di posta elettronica, accesso alla rete Internet, etc.), sono stati inseriti nel regolamento alcuni articoli relativi alle modalità ed alle regole che ciascun utente deve osservare nell'utilizzo delle apparecchiature informatiche.

Quanto riportato nel presente regolamento non è valido per le apparecchiature informatiche collegate a strumentazioni elettromedicali, la cui gestione è demandata ad un apposita articolazione aziendale afferente al Dipartimento Tecnico.

Art.1
Campo di Applicazione

1.1 Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (consulenti, lavoratori somministrati, collaboratori a progetto, in stage, volontari, tirocinanti, ditte esterne autorizzate, ecc.).

Art.2
Definizioni e Acronimi

2.1 Ai fini dell'applicazione del presente Regolamento si forniscono le seguenti definizioni:

- per "***utente***", si intende ogni dipendente, collaboratore, consulente, lavoratore somministrato, collaboratore a progetto, stagista, volontario, tirocinante, dipendente ditta esterna, ecc., che utilizzi le risorse informatiche (hardware, software, rete, ecc.) messe a disposizione dall'Azienda U.S.L., in possesso o meno di specifiche credenziali di autenticazione per l'utilizzo delle procedure aziendali;
- per "***ICT***", acronimo di Information and Communication Technology, (cioè Tecnologia dell'Informazione e della Comunicazione), si intende l'insieme di progettazione, sviluppo, implementazione, supporto e gestione dei sistemi informativi computerizzati e dei canali telematici di trasmissione utilizzati.
- "***S.I.A.***", è l'acronimo di Sistema Informativo Aziendale; è costituito dall'insieme delle informazioni utilizzate, prodotte e trasformate da un'azienda durante l'esecuzione dei processi aziendali, dalle modalità in cui esse sono gestite e dalle risorse, sia umane, sia tecnologiche, coinvolte. Il sistema informatico, che indica una porzione di sistema informativo, è la componente del S.I.A. che fa uso di tecnologie informatiche e automazione.
- "***S.S.I.***" è l'acronimo di Settore Sistema Informativo aziendale; è la struttura aziendale preposta al corretto funzionamento delle risorse informatiche aziendali (vedi art.3). Per "*Tecnici del S.S.I.*" si intende il personale della suddetta articolazione o altra persona da essa temporaneamente delegata (ad es. consulenti, società esterna addetta alla manutenzione, ecc.).

Art. 3
Competenze

3.1 Nell'ambito della gestione delle risorse e dei servizi informatici aziendali risultano essere direttamente coinvolte determinate UU.OO., ciascuna con specifiche competenze.

Al fine di agevolare l'utente nella risoluzione delle problematiche relative all'utilizzo dei servizi summenzionati, si riporta un elenco di tali strutture, con le singole specifiche competenze:

- Dipartimento Acquisizione Beni e Servizi: è l'unica articolazione aziendale, fatte salve eventuali deroghe che possono essere concesse di volta in volta, preposta all'acquisto di hardware, software e servizi di natura informatica. Pertanto tutte le richieste di apparecchiature, software e servizi dovranno essere inoltrate a questo dipartimento (si veda *Art.5 – Acquisto di hardware e software*). Inoltre, il Dipartimento Acquisizione Beni e Servizi è preposto alla gestione dell'inventario delle apparecchiature, che dovrà avvenire in base ad apposito regolamento.
- Dipartimento Attività Tecniche e Gestione del Patrimonio: è l'articolazione aziendale che ha in carico la predisposizione e la gestione, diretta o indiretta, di tutte le infrastrutture necessarie alla gestione ed al funzionamento degli impianti tecnologici (es. lavori edili, impianto elettrico e di condizionamento, impianto fonia e dati, cablaggio strutturato, punti rete; malfunzionamento apparati, ecc.). Fornisce inoltre parere tecnico in merito all'utilizzo di modem/router ed impianti di connessione wireless.
- Settore Sistemi Informativi: è l'articolazione aziendale preposta a garantire il corretto funzionamento del S.I.A. (Sistema Informativo Aziendale) e le cui principali competenze possono essere sintetizzate nei seguenti punti:
  - fornire parere tecnico e consulenza in merito ad acquisto e gestione di software ed apparecchiature informatiche;
  - fungere da interfaccia tecnica fra gli utenti del S.I.A. e le ditte fornitrici;
  - garantire il corretto funzionamento delle Postazioni di Lavoro;
  - mantenere un inventario delle apparecchiature informatiche in manutenzione;
  - gestire la parte informatica sia della Intranet aziendale che del sito Internet;
  - realizzare piccoli attività di programmazione in linea con le esigenze aziendali;
  - fornire a tutti gli utenti, durante il normale orario di lavoro, un Call Center di primo livello per la segnalazione di malfunzionamenti delle apparecchiature in manutenzione;
  - collaborare con le varie articolazioni aziendali per l'attivazione di nuove procedure informatiche;
  - gestire gli utenti del S.I.A. con i dovuti criteri di sicurezza e riservatezza;
  - monitorare le prestazioni della rete aziendale;
  - configurare gli apparati attivi di rete;
  - assegnare le eventuali apparecchiature informatiche a scorta;
  - gestire i contratti di manutenzione di Hardware e Software direttamente gestiti;
  - gestire le apparecchiature presenti nel Data Center aziendale;
  - garantire le copie di backup dei server di rete direttamente gestiti;
  - studiare ed ottimizzare eventuali collegamenti fra i vari sottosistemi esistenti;
  - formare il personale sul corretto uso delle risorse e delle procedure di Office Automation utilizzate.

Si precisa che il S.S.I. non è in alcun caso proprietario dei dati gestiti con il S.I.A. e che pertanto eventuali statistiche o report dovranno essere richiesti alle UU.OO. di competenza (Controllo di Gestione, Ufficio del Personale, Ragioneria, Ufficio Statistica, ecc.). Analogamente, il corretto utilizzo delle procedure applicative (contabili, sanitarie, gestione del personale, ecc.) è di competenza delle articolazioni aziendali che utilizzano il software.

Art.4
Finalità

4.1 Le apparecchiature informatiche, i programmi, e tutte le risorse informatiche che l'Azienda USL di Teramo mette a disposizione dei suoi utenti, ivi compresi i servizi di tipo Internet/posta elettronica, devono essere utilizzati esclusivamente per fini lavorativi e non personali, nel pieno rispetto della normativa vigente e delle norme del presente Regolamento al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.

4.2 Tutto il personale interessato dalle disposizioni del presente Regolamento, è tenuto a contattare il S.S.I. prima di intraprendere qualsiasi attività tecnica non esplicitamente compresa ne presente regolamento, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

HARDWARE E SOFTWARE

Art.5
Acquisto di hardware e software

5.1 Tutto l'hardware ed il software potrà essere acquistato solo previa richiesta di parere tecnico favorevole da parte del S.S.I., che controllerà le richieste di acquisto al fine di valutare la compatibilità con il S.I.A. e prevenire l'introduzione di virus e/o altri programmi dannosi.

Tutto il software in uso presso l'Azienda U.S.L. deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'Azienda U.S.L. di Teramo. Tutto il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright), e non può installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004 e succ.mod.

A tal fine le richieste di acquisto dell'hardware e del software dovranno essere redatte in duplice copia ed indirizzate al Responsabile del S.S.I. ed al Responsabile del Dipartimento Acquisizione Beni e Servizi, utilizzando l'apposita scheda allegato A al presente Regolamento, o eventuali aggiornamenti che verranno pubblicati sul sito aziendale.

Al S.S.I. spetta la verifica tecnica della compatibilità degli strumenti richiesti con l'infrastruttura di rete. Nel caso in cui gli strumenti proposti non possano, per ragioni tecniche, essere installati, saranno individuate, ove possibile e nei limite della tecnologia, soluzioni alternative, tecnicamente fattibili, d'intesa tra il S.S.I. ed il servizio richiedente. I supporti originali dei software acquistati e le relative licenze devono essere conservati presso il S.S.I., così da consentire le operazioni di verifica della disponibilità di licenze e l'eventuale re-installazione delle procedure.

Art.6
Software Installato

6.1 Il software per elaboratori è considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente rispettate da tutti. (DLG. 518/92 sulla tutela giuridica del software e L. 248/2000 "*nuove norme di tutela del diritto d'autore*").

6.2 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dai tecnici del S.S.I. per conto dell'Azienda U.S.L., perché sono i programmi per i quali l'Azienda possiede la regolare licenza d'uso, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti.

6.3 E' vietato provare ad installare arbitrariamente il software scaricato da Internet o contenuto nei vari supporti distribuiti con le riviste, con i libri e con i quotidiani anche se si tratta di software allegato a riviste del settore. Prima di installare questi programmi, qualora l'uso fosse collegato ad esigenze lavorative, sarà necessario il benestare del S.S.I..

6.4 Non è ammesso l'uso di strumenti atti a catturare o rivelare le password (password crack, keylogger, etc.) per accedere in modo non autorizzato a dati o sistemi.

6.5 E' assolutamente vietato installare, anche solo temporaneamente, programmi ottenuti o sbloccati illegalmente (programmi crackati, codici di sblocco ottenuti da internet, etc.). Un programma crackato, oltre a costituire una violazione alle norme che regolano il Diritto d'Autore, costituisce anche un'autentica minaccia alla sicurezza della rete ed all'affidabilità del calcolatore su cui viene installato. Lo sblocco del programma (crack) viene infatti effettuato modificando i codici originali del programma per aggirare le protezioni. Questo implica sostituire pezzi del programma originale con parti modificate e queste nuove aggiunte, oltre ad aggirare le protezioni, possono anche introdurre codice dannoso.

6.6 L'utente è responsabile del software installato sul proprio PC, sia software di base che software applicativo di vario genere (es. software di gestione del personale; database di archiviazione dati; etc.) e del suo corretto utilizzo; se ne raccomanda pertanto un uso diligente.

6.7 Non è consentita la disinstallazione dei programmi, sia software di base che software applicativi. I suddetti interventi sono effettuati, in caso di necessità, solo a cura dei tecnici del S.S.I. dietro segnalazione dell'utente.

6.8 Non è consentita l'installazione anche se necessaria di eventuali drivers per stampanti o altri supporti come ad esempio masterizzatori, scanner, etc.; in questo caso l'utente dovrà richiedere ai tecnici del S.S.I. di intervenire per effettuare l'installazione.

6.9 E' facoltà del S.S.I. bloccare automaticamente il download, da siti non istituzionali o non affidabili, di file potenzialmente infetti. Nel caso in cui sia necessario "scaricare" ulteriori files, anche gratuiti, dalla rete, l'utente dovrà formulare una richiesta, preventivamente autorizzata dal Responsabile della propria U.O., al S.S.I. che provvederà ad autorizzare il download ovvero ad effettuare direttamente l'installazione del programma.

6.10 L'aggiornamento del sistema operativo avviene in modo automatico attraverso la rete aziendale; qualora però il PC non fosse collegato alla rete sarà a cura dell'utente provvedere all'aggiornamento.

6.11 L'inosservanza delle disposizioni sopra elencate espone l'Azienda a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Art.7
Utilizzo del software di proprietà personale

7.1 Al fine di proteggere l'integrità dell'Azienda U.S.L., il personale non può utilizzare eventuale software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

7.2 Qualora fosse necessario per fini strettamente collegati all'attività lavorativa, l'utilizzo di software di proprietà personale, il dipendente dovrà essere autorizzato dal proprio Responsabile; l'installazione dovrà essere segnalata al S.S.I..

7.3 Nell'ipotesi di utilizzo di software realizzato direttamente dall'utente finale sarà necessario darne comunicazione al S.S.I. e, qualora vengano trattati dati sensibili, darne comunicazione anche all'ufficio privacy.

Art.8
Software Anti Virus

8.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro codice malware (worm, trojan, DoS, spyware,

backdoor, ecc. E' buona norma, ad esempio, non aprire mail o relativi allegati sospetti, non navigare su siti non professionali, e così via.

La politica di sicurezza aziendale prevede l'utilizzo presso tutti i PC di uno stesso software anti virus (al momento il *Symantec Endpoint Protection*©) che viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzati dal S.S.I.

Ogni utente è tenuto comunque a controllare la presenza e il regolare aggiornamento del software antivirus aziendale e della definizione dei virus. Nell'eventualità di PC non collegati alla rete aziendale sarà cura dell'utente provvedere al regolare aggiornamento del software.

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 S.S.I.

8.2 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.

8.3 Qualora si riscontrasse da parte del dipendente il mancato rispetto di quanto sopra indicato e quindi un comportamento non corretto, ogni danno provocato dalla presenza di un malware (virus, worm, trojan horse, backdoor, spyware, dialer etc.) potrà essere direttamente imputabile al dipendente stesso.

Art.9
Utilizzo del Personal Computer

9.1 Il Personal Computer affidato all'utente/servizio è uno strumento di lavoro deve essere custodito con cura adottando ogni precauzione per evitare ogni possibile forma di danneggiamento. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza.

Il PC dato in affidamento all'utente/servizio permette l'accesso alla intranet dell'Azienda U.S.L. ed alla rete esterna solo attraverso apposita configurazione e necessita di specifiche credenziali di autenticazione come meglio descritto nei successivo punti del presente Regolamento.

9.2 I tecnici del S.S.I. sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la manutenzione, la sicurezza e la salvaguardia del sistema stesso (ad es. aggiorna-mento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Pur rispettando tutti i criteri di riservatezza, detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché al monitoraggio dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per

garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente su richiesta da parte della Direzione Aziendale o qualora fosse necessario intervenire per la sicurezza dell'intero sistema.

I tecnici del S.S.I. 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.

9.3 Il personale incaricato del settore S.S.I. ha la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. A tale scopo sarà possibile installare sui PC client appositi software (agent), normalmente in commercio, per la rilevazione automatica della configurazione hardware e software, che tenga traccia delle modifiche effettuate e della versione dei software installati.

In ogni caso l'intervento da remoto verrà effettuato, dai tecnici del S.S.I. esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

9.4 Gli aggiornamenti del software e dei drivers necessari al buon funzionamento della postazione di lavoro saranno a cura direttamente dei tecnici del S.S.I. che provvederanno all'aggiornamento automatico per ciò che attiene la protezione anti virus ed il sistema operativo, per i PC collegati alla rete aziendale, ed interverranno dietro segnalazione dell'utente per ogni ulteriore aggiornamento necessario. Nel caso di PC non collegati alla rete sarà cura dell'utente provvedere all'aggiornamento del sistema operativo e del software anti virus.

9.5 Le stazioni di lavoro vengono predisposte e configurate dai tecnici del S.S.I. per le esigenze dell'utente finale. Ai fini della manutenzione del sistema viene creato su ogni PC un profilo utente "a*dministrator*" con relativa password. L'utente del PC si impegna a mantenere la corretta configurazione della stazione di lavoro che utilizza e a non modificare o cancellare il profilo "*administrator*" creato per la manutenzione; non è consentito pertanto all'utente modificare le caratteristiche impostate sul proprio PC né procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.) senza il preventivo consenso del S.S.I.. A tale scopo è facoltà del S.S.I. rimuovere/modificare eventuali altri utenti aventi i privilegi di amministratore di sistema.

9.6 Ogni PC deve essere fornito di password di accesso, sarà cura dell'utente utilizzatore modificare periodicamente la propria password (dandone comunicazione, qualora previsto all'interno della propria articolazione aziendale, al gestore delle password) ed avere la massima diligenza e segretezza nel custodire le credenziali di accesso al proprio PC. Qualora sul PC in

dotazione venissero trattati dati sensibili, in base alla normativa vigente, la password di accesso dovrà essere modificata ogni 3 mesi.

9.7 Nell'ambito degli acquisti e della gestione delle risorse informatiche sarà facoltà dell'Azienda U.S.L. adottare tutte quelle politiche finalizzate alla riduzione dell'impatto ambientale ed al risparmio economico; fra queste, a titolo di esempio, citiamo l'acquisto di apparecchiature a basso consumo, la condivisione di periferiche (stampanti, scanner, fax, unità di backup, ecc.), la stampa in monocromatico, il corretto smaltimento del materiale di consumo. Ciascun utente dovrà adeguarsi alle suddette politiche.

9.8 E' fatto assoluto divieto all'utente di intervenire in qualunque modo sull'hardware in dotazione. In caso di malfunzionamento delle apparecchiature assegnate, l'utente si impegna a darne tempestiva segnalazione al personale del S.S.I. La manutenzione delle apparecchiature pertanto è di assoluta pertinenza dei tecnici del S.S.I.

9.9 Ogni utente deve prestare la massima attenzione nell'utilizzo di memorie di massa esterne, avvertendo immediatamente il personale del S.S.I. nel caso in cui siano rilevati virus ed adottando quanto previsto all'art.8 del presente Regolamento relativo alle procedure di protezione antivirus.

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

9.11 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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 provarne in seguito l'indebito uso.

9.12 E' consentito agli utenti l'utilizzo di PC personali previa autorizzazione scritta del Responsabile dell'U.O. di appartenenza e comunicazione al S.S.I. La manutenzione del Pc, in questo caso, è a completo carico dell'utente sia dal punto di vista hardware che software.

Il collegamento del Pc personale alla rete aziendale ed il relativo utilizzo è possibile solamente dietro autorizzazione del Dirigente Responsabile della propria U.O., d'intesa con il tecnico del S.S.I. che provvederà alla configurazione necessaria.

Resta salvo che l'utilizzo della rete aziendale e l'accesso alla rete esterna tramite l'infrastruttura dell'Azienda comporta necessariamente che il PC proprio sia dotato di software anti virus adeguato. Sarà cura del proprietario del PC e dell'utilizzatore della postazione tenere aggiornato il software anti virus.

9.13 Il corretto smaltimento del materiale di consumo sarà a carico dell'utente , che dovrà rispettare la normativa vigente ed eventuali direttive aziendali.

9.14 Il mancato rispetto di quanto previsto al precedente punto potrebbe comportare dei seri rischi sulla sicurezza dell'intero sistema, e pertanto comportare sanzioni a carico dell'utente.

Art. 10

Utilizzo di PC portatili personali o in dotazione

10.1 L'azienda può assegnare all'utente un PC portatile solo nel caso di assoluta necessità di dispositivi mobili, e previa esauriente relazione sottoscritta dal Dirigente Responsabile dell'Unità Operativa di competenza.

10.2 L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

10.3 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento per l'uso dei Personal Computer.

Particolare attenzione è rivolta nel caso di un utilizzo temporaneo del Pc portatile assegnato, per ciò che attiene alla rimozione da parte dell'utente utilizzatore di eventuali file elaborati ed utilizzati, prima della riconsegna.

10.4 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

10.5 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, etc.

10.6 Eventuali configurazioni di connessione alla rete LAN, dirette verso la rete aziendale o verso la rete esterna, possono essere attivate esclusivamente seguendo le medesime procedure previste per l'accesso alla rete intranet/internet nel successivo art.12.

E' vietato utilizzare all'interno delle sedi dell'Azienda delle connessioni di tipo Accesso Remoto, e quindi eventuali modem, se non espressamente autorizzati dall'Ufficio Tecnico e dal S.S.I. E' prevista la connessione alla rete internet e l'accesso alla rete intranet dietro apposita configurazione del PC da parte del personale del S.S.I.

10.7 Qualora il portatile sia di proprietà personale si applicano le medesime disposizioni previste al punto 9.12 del presente Regolamento.

Art. 11

Backup e Pulizia

11.1 Ogni utente è responsabile della corretta conservazione dei dati e dei documenti elettronici che utilizza per motivi lavorativi, di qualsiasi tipo, formato e natura essi siano. Per questo motivo la tutela della gestione dei dati sulle postazioni di lavoro (Personal computer e Pc portatili) è demandata all'utente finale, che avrà l'obbligo di effettuare il salvataggio dei dati memorizzati sui computer in dotazione, con frequenza opportuna, in funzione del tipo di dati trattati, e la conservazione degli stessi in luogo idoneo. Nel caso di postazione condivisa da più utenti la corretta gestione dei salvataggi sarà cura, oltre che dei singoli utenti, anche del Dirigente Responsabile dell'Unità Operativa.

Il S.S.I. a questo scopo fornisce, qualora la postazione dell'utente ne fosse sprovvista, la possibilità di utilizzare temporaneamente un masterizzatore esterno o eventuale altro dispositivo hardware in dotazione, necessario per il salvataggio.

Nel caso si gestiscano dati sensibili, per motivi di sicurezza e di privacy è sconsigliato l'uso di supporti di massa esterni (hard disk rimovibili, penne USB, DVD RW) che comunque, se utilizzati, devono essere custoditi in archivi chiusi a chiave.

Ove possibile il S.S.I. metterà a disposizione degli utenti che ne facessero richiesta, delle partizioni di disco su file server aziendali, che l'utente potrà utilizzare, in maniera esclusiva e riservata, per il salvataggio dei dati aziendali.

11.2 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.

ACCESSO INTERNET / INTRANET E POSTA ELETTRONICA
ACCESSO PROGRAMMI GESTIONALI

Art.12
Internet e Posta Elettronica - gestione ed assegnazione delle credenziali di autenticazione per l'accesso

12.1 Tutti i dipendenti ed i collaboratori dell'Azienda possono richiedere l'accesso ad Internet e l'attivazione di una casella di posta elettronica sul dominio aziendale (www.aslteramo.it) . Tali benefici potranno essere concessi anche a strutture esterne che collaborano con l'Azienda, previa autorizzazione del Dirigente Responsabile di competenza.

12.2 Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di Posta Elettronica vengono assegnate dal personale del S.S.I., previa formale richiesta da effettuare attraverso la compilazione dell'apposito modulo Allegato B al presente Regolamento, "RICHIESTA DI CONCESSIONE/REVOCA UTILIZZO RETE INTERNET/INTRANET E SERVIZIO DI POSTA ELETTRONICA", sottoscritta dal Dirigente Responsabile della struttura presso la quale l'utente opera, o dovrà operare.

Nel caso di collaboratori a progetto e coordinati e continuativi, stagisti, etc. la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione aziendale (ovvero dal Dirigente Responsabile della struttura con la quale il collaboratore si coordina nell'espletamento del proprio incarico).

L'utilizzo del sopraindicato modulo sarà necessario anche nell'eventualità il dipendente/collaboratore/stagista cessi o abbia cessato il rapporto con l'Azienda; sarà cura del

Responsabile dell'U.O. di appartenenza dare tempestiva comunicazione al settore S.S.I. al fine di evitare un possibile uso illecito dei servizi forniti e delle credenziali di autenticazione.

La medesima modulistica sarà da utilizzare anche nei casi di trasferimento/spostamento dei dipendenti presso U.O. diverse da quelle nelle quali il soggetto prestava servizio al momento della concessione.

Sarà quindi cura del precedente Responsabile dell'U.O. di appartenenza comunicare il trasferimento del dipendente e quindi la cessazione all'utilizzo del servizio; un eventuale riattivazione sarà poi possibile dietro nuova autorizzazione concessa dal Responsabile dell'U.O. che prende in carico il dipendente.

Qualunque richiesta di concessione di utilizzo dei servizi Intranet/Internet e posta elettronica, dovesse pervenire presso il S.S.I. senza l'utilizzo del sopraindicato modulo, o eventualmente con compilazione non corretta o incompleta (es. manca firma del Responsabile, manca indicazione della password, etc.) non sarà presa in considerazione.

12.3 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (userid),assegnato dal S.S.I. , associato ad una parola chiave (password) riservata che dovrà venir custodita dall'utente con la massima diligenza e segretezza e non divulgata.

Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

Non sono ammissibili codici di accesso anonimi.

12.4 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

12.5 È necessario procedere alla modifica della parola chiave a cura dell'utente, al primo utilizzo e, successivamente, almeno ogni sei mesi (tre mesi nel caso si trattino dati sensibili). La password deve essere immediatamente modificata, nel caso si sospetti che la stessa sia stata conosciuta da altri ed abbia, quindi, perso la segretezza.

12.6 Qualora la parola chiave fosse stata dimenticata, si procederà alla sua sostituzione d'intesa con il personale del S.S.I., che provvederà, in seguito a segnalazione dell'utente, a far recapitare all'interessato le nuove credenziali di autenticazione; resta inteso che sarà cura dell'utente modificare la password al primo accesso.

12.7 Ogni U.O. dovrà essere dotata di una casella di posta istituzionale che verrà utilizzata per un più rapido scambio delle comunicazioni interne e che dovrà essere consultata con frequenza giornaliera. Sarà cura del Dirigente Responsabile dell'U.O. verificare l'esistenza di tale casella e, in caso negativo, farne richiesta al S.S.I.. In tale richiesta dovranno essere elencati i nominativi delle persona autorizzate all'utilizzo della casella di posta istituzionale.

12.8 Soggetto preposto alla custodia delle credenziali di autenticazione per l'accesso ad Internet ed alla Posta Elettronica, è il personale incaricato del S.S.I..

12.9 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.

A tale scopo si ritiene indispensabile, ove il Sistema Operativo lo permetta, l'utilizzo di sistemi di blocco della tastiera con password.

Art.13

Programmi Gestionali - gestione ed assegnazione delle credenziali di autenticazione per l'accesso

13.1 E' possibile ottenere l'assegnazione di specifiche credenziali di autenticazione a programmi gestionali specifici, dietro compilazione, a cura del Dirigente responsabile, di apposita modulistica presente nell'area intranet del sito della ASL, ovvero da richiedere al S.S.I.

13.2 Qualora l'utente sia in possesso di credenziali che gli consentano l'accesso a procedure gestionali (es. Accesso ad AS/400, Accesso sistema Rilevazione Presenze, Gestione Tessera Sanitaria, Sistema Siatel, etc.) o a dati sensibili, il sopraindicato modulo dovrà essere compilato a cura del dirigente Responsabile ed inviato al S.S.I., anche in caso di trasferimento del dipendente ad altra struttura o eventuale cessazione del rapporto di lavoro con l'Azienda.

Art. 14

Registrazione delle attività

14.1 Le operazioni effettuate servendosi di userid e password, compreso l'elenco dei siti Internet visitati, potranno essere memorizzati per finalità di sicurezza del sistema.

L'attività di registrazione avviene attraverso i file "log" di sistema a cura del S.S.I.

Nell'ambito dell'attività autorizzata alla navigazione in internet, con cadenza giornaliera, il S.S.I. provvederà ad archiviare i dati di "log" dell'uso del servizio. Durante l'uso del servizio, viene infatti tenuta traccia dell'attività di navigazione dell'utente consistente, in linea di massima, nelle seguenti informazioni di dettaglio:

- Data e ora dell'accesso;
- Identificativo o indirizzo IP dell'utente che ha richiesto l'accesso;
- Nome del sito richiamato per la consultazione;
- Esito della consultazione;
- Tipologia di operazione richiesta e informazioni sui files scaricati;
- Numero di bytes trasferiti dall'elaboratore remoto alla stazione dell'utente e viceversa.

In nessun caso è consentito ad un utente chiedere informazioni sulla navigazione degli altri utenti, nemmeno per scopi comparativi con i propri e nemmeno in forma aggregata. In nessun caso i log del sistema sono usati come strumento di controllo per la produttività degli utenti.

14.2 L'Azienda U.S.L. si riserva di utilizzare i normali programmi in commercio per la protezione di siti e l'esclusione di siti vietati o non attinenti agli scopi istituzionali dell'Azienda.

L'Azienda U.S.L. si riserva di effettuare dei controlli, anche a campione, concernenti l'utilizzo corretto degli strumenti di lavoro. I controlli possono essere fatti al momento e/o a campione, anche in tempi successivi attraverso l'esame dei log di sistema.

L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

I log potranno essere oggetto di verifica e di provvedimenti dell'Autorità giudiziaria e amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo.

Art.15
Utilizzo della rete dell'Azienda U.S.L.

15.1 La rete dell'Azienda U.S.L. si basa sul protocollo TCP/IP. Tutte le apparecchiature connesse alla Rete sono configurate per ricevere l'indirizzo IP dinamicamente dal server DHCP oppure con un IP assegnato staticamente a seconda della tipologia di apparecchiatura.

15.2 E' assolutamente vietato connettere alla rete delle macchine configurate con indirizzo IP statico, assegnato direttamente dall'utente, senza una preventiva autorizzazione del S.S.I. .

Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.

In caso di dubbio prima di collegare alla rete aziendale un PC o un Notebook (non configurati) sarà necessario farne richiesta al settore S.S.I. che effettuerà la giusta configurazione della macchina.

15.3 Non è ammessa la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, deve essere concordato con l'Ufficio Tecnico e il S.S.I. Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub).

15.4 E' fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server.

15.5 E' fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware, l'utilizzo di tali strumenti è

strettamente riservato al personale tecnico del S.S.I. al fine di monitorare le prestazioni della rete aziendale. Nel caso si riscontrasse la presenza di Pc che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale del S.S.I. procedere al blocco, se necessario, dell'attività di rete del Pc.

15.6 L'utilizzo di reti Wireless (rete senza fili, ad onde radio) deve essere autorizzato dall'Ufficio Tecnico e dal S.S.I. e, nel caso di installazione nelle vicinanze di apparecchiature medicali, comunicato al Servizio di Fisica Sanitaria che dovrà valutare la compatibilità con le apparecchiature esistenti.

15.7 Le cartelle utenti, o cartelle dei dipartimenti presenti nei server dell'Azienda sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del S.S.I.

Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. dischi fissi interni o esterni al PC) non sono soggette a salvataggio da parte del personale incaricato del S.S.I. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente, si riporta all'art.11 "Backup e Pulizia", del presente Regolamento.

Art. 16
Connessione ad Internet tramite dispositivi Dial-Up

16.1 È vietato l'utilizzo di accessi ad Internet mediante dispositivi di Accesso Remoto (modem, WLan, ecc.), anche tramite abbonamenti privati. L'Azienda si riserva la facoltà di controllare, individuare ed interdire il ricorso a sistemi Dial-Up nonostante il suddetto divieto.

16.2 Per motivi di sicurezza, l'utilizzo di Internet è ammesso ed autorizzato solo attraverso la rete locale di trasmissione dati aziendale. Solo in rarissimi ed eccezionali casi, autorizzati unicamente dal Direttore del S.S.I. di concerto con il Direttore dell'U.O. del Dipartimento Tecnico, è ammesso l'accesso remoto ad Internet attraverso un modem di trasmissione dati

L'utente è informato del potenziale rischio per la sicurezza dell'intero sistema informativo aziendale connesso alla realizzazione di collegamenti non autorizzati.

Art. 17
Virtual Private Network

17.1 E' possibile l'abilitazione di reti VPN per la gestione da parte di utenti esterni alla Intranet aziendale, normalmente per la diagnostica e manutenzione da remoto di software o hardware.

Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere; per garantire la sicurezza che i dati inviati in Internet

non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia. L'abilitazione e le credenziali di accesso vengono forniti dal personale del S.S.I. dietro richiesta del Responsabile dell' U.O. interessata che dovrà segnalare tempestivamente eventuali modifiche o cessazione di rapporti con la ditta esterna autorizzata.

Art. 18

Navigazione in Internet

18.1 Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

18.2 Non possono essere utilizzati modem privati per il collegamento alla rete.

18.3 E' possibile usufruire del servizio Internet utilizzando le credenziali di accesso fornite secondo le modalità previste nel presente Regolamento.

18.4 L'accesso alla rete Internet è da intendersi quale "strumento di lavoro". In tal senso, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- il download, da siti non istituzionali o comunque non ritenuti affidabili, di files eseguibili potenzialmente dannosi o infetti. Qualora, per motivi di lavoro, fosse necessario scaricare uno di questi file da un sito non accessibile, il SSI potrà autorizzarne, anche solo temporaneamente, il download previa richiesta sottoscritta anche dal Dirigente responsabile dell'U.O.
- il download di files 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;
- ricerche e/o consultazioni di siti unicamente per scopi personali;
- ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- trasferire sulla stazione dell'utente programmi e/o files di dati relativi a progetti od obiettivi estranei all'attività lavorativa dell'utente o per finalità personali;
- ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Azienda;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Dirigente Responsabile della propria U.O. e comunque nel rispetto delle normali procedure di acquisto;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- 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) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

È vietato l'uso del servizio nei casi che configurano un più grave reato:

- Diffusione di virus, cavalli di troia o altri programmi, la cui azione consista nel sabotaggio, distruzione o alterazione del contenuto informativo delle stazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- Per attività di furto di dati di altri utenti, organismi e/o aziende;
- Per attività di hackeraggio e pirateria informatica in generale;

18.5 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda U.S.L. potrà adottare di uno specifico sistema di blocco o filtro automatico (sistema di Web Filtering) che prevenga determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

18.6 La consultazione, ai soli fini lavorativi, di specifici siti non istituzionali sarà possibile attraverso l'abilitazione all'accesso che dovrà essere richiesta compilando uno specifico modulo sottoscritto anche dal Dirigente Responsabile dell'U.O.; è necessario indicare l'esatto indirizzo del sito internet da abilitare ed il motivo della richiesta. Sarà facoltà dell'Azienda U.S.L. nominare un'apposita commissione per valutare l'ammissibilità della richiesta.

18.7 L'Amministrazione utilizza, attraverso personale tecnicamente competente, strumenti elettronici sia per esigenze produttive e/o organizzative (per es. per rilevare anomalie o per manutenzioni), sia per esigenze di sicurezza sul lavoro.

Nelle suddette ipotesi l' Amministrazione si avvarrà legittimamente, nel rispetto dell'art. 4, comma 2, della legge 300/1970 (Statuto dei Lavoratori) di sistemi informatici ed elettronici che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò sarà possibile anche in presenza di attività di controllo discontinue.

L'Amministrazione, inoltre, nell'esercizio delle sue prerogative datoriali di direzione e organizzazione del lavoro, si riserva periodicamente, e almeno su base annuale, di porre in essere le seguenti attività:

- selezione del personale autorizzato alla navigazione online;
- valutazione dell'impatto dei controlli sui lavoratori;
- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate incoerenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti (inseriti in una

sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);

- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati attraverso i registri di log (almeno 90 giorni, estensibili a 180 giorni) strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

Gli eventuali controlli, compiuti dal personale incaricato del S.S.I. su richiesta dell'Amministrazione, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati in base alla normativa vigente.

Art. 19
Corsi On Line

19.1 Sarà possibile per i dipendenti seguire dei Corsi On Line secondo le modalità di seguito riportate:

- preventiva autorizzazione da parte del Responsabile dell'U.O.;
- preventiva autorizzazione del Responsabile dell'Ufficio Formazione;

L'orario del Corso dovrà essere compatibile con la gestione della rete aziendale, dovrà essere svolto nella fascia oraria in cui il traffico di rete risulta minore, pertanto sarà facoltà del personale S.S.I. l'abilitazione.

Art.20
Posta Elettronica

20.1 Per lo svolgimento delle mansioni lavorative, viene attribuita, a tutti i dipendenti che abbiano fatto richiesta una casella di posta elettronica aziendale.

L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile dell'U.O. di appartenenza, tramite il medesimo modulo utilizzato per l'accesso alla rete intranet/internet, previsto nel precedente punto 11.1.

Si raccomanda di utilizzare l'email esclusivamente per finalità legate all' attività lavorativa.

20.2 Le caselle di posta sono nominative e vengono assegnate utilizzando il seguente formato:

nome.cognome@aslteramo.it

Possono essere assegnate, qualora si rendesse necessario per esigenze organizzative del lavoro, dietro richiesta del Responsabile dell'U.O. , delle caselle di posta istituzionali del tipo:.

urp@aslteramo.it

direzione.generale@aslteramo.it

Come già detto al pa. 12.7, detta casella di posta istituzionale che verrà utilizzata per un più rapido scambio delle comunicazioni interne e che dovrà essere consultata con frequenza giornaliera. Sarà cura del Dirigente Responsabile dell'U.O. verificare l'esistenza di tale casella e, in caso negativo, farne richiesta al S.S.I.. In tale richiesta dovranno essere elencati i nominativi delle persona autorizzate all'utilizzo della casella di posta istituzionale.

E' previsto, come standard per ogni casella di posta, un dimensionamento massimo pari a 40 MB; qualora fosse necessario un dimensionamento maggiore misigna farne richiesta al S.S.I.

20.3 L'accesso alla casella di posta elettronica è possibile attraverso la Home Page del sito aziendale (www.aslteramo.it) utilizzando le apposite credenziali di autenticazione fornite come indicato in precedenza; sarà possibile entrare nell'area riservata, da qui cliccando sulla voce WEB MAIL , si accede alla propria casella di posta.

In questo modo l'utente potrà consultare la propria casella direttamente via web, collegandosi al Server; tutto ciò offre all'utente la possibilità di accedere ovunque ci si trovi alla propria posta.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga saturano lo spazio disponibile. Si ricorda a tal fine che sarà necessario eliminare anche i messaggi contenenti allegati di grandi dimensioni presenti nelle cartelle POSTA INVIATA, POSTA ELIMINATA; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella POSTA ELIMINATA utilizzando la voce SVUOTA CARTELLA POSTA ELIMINATA.

20.4 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 pertanto:

- E' vietato utilizzare l'indirizzo e caselle di posta elettronica aziendale, nel formato previsto nome.cognome@aslteramo.it, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.
- E' vietato utilizzare la login / password di un altro utente per accedere in sua assenza alla sua posta elettronica.
- È vietato inviare catene telematiche (le cosiddette "catene di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, non si devono in alcun caso attivare gli allegati di tali messaggi.

20.5 Nel caso di prolungata assenza dell'utente e in caso di urgenza, qualora si renda necessario per esigenze lavorative, accedere alla posta elettronica o alla postazione di lavoro dell'utente, a giudizio del Responsabile dell'unità operativa, quest'ultimo potrà richiedere l'abilitazione al S.S.I., ovvero se esiste al gestore delle password.

20.6 E' possibile ottenere per via informatica, nelle comunicazioni esterne ed interne all'azienda, una segnalazione di verifica sia relativamente al recapito del messaggio che all'avvenuta lettura; si ricorda però che la conferma dell'avvenuta lettura del messaggio da parte del destinatario è a sua propria discrezione, essendo il servizio di posta elettronica in uso presso l'Azienda non ancora certificato.

Di norma, pertanto, per avere una garanzia di avvenuta ricezione è conveniente chiedere al destinatario di confermare esplicitamente.

20.7 Si raccomanda:

- di prestare attenzione alla dimensione degli allegati che, di norma, non devono mai superare i 10 MB.
- di utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar)
- nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
- di dare immediata segnalazione al personale del S.S.I. nel caso si riscontrassero dei casi di phishing (è un tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, ad esempio numeri di carta di credito, password, dati relativi al proprio conto e così via.Gli autori delle frodi sono in grado di inviare milioni di messaggi di posta elettronica fraudolenti che, in apparenza, sembrano provenire da siti Web sicuri, come la propria banca o la società di emissione della carta di credito, che richiedono di fornire informazioni riservate).

20.8 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

20.9 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 o non affidabili).

20.10 Si fa presente che il protocollo TCP/IP utilizzato per i sistemi di posta elettronica non usa la crittografia né non garantisce contro la lettura non autorizzata dei messaggi lungo il percorso fino al destinatario. Pertanto è vietato utilizzare la posta elettronica per inviare all'esterno comunicazioni che contengono dati sensibili in chiaro.

20.11 E' fatto divieto di inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

20.12 E' prevista la possibilità di adottare all'interno del sistema informativo aziendale l'utilizzo di un sistema Anti Spam che potrebbe comportare il blocco, in entrata o in uscita, di eventuali messaggi ritenuti nocivi, indesiderabili o potenzialmente infetti. Pertanto è buona norma, nel caso di messaggi importanti, utilizzare la posta elettronica certificata, se disponibile, o almeno richiedere la conferma di recapito/lettura delle mail inviate.

Art. 21

Cessazione della disponibilità dei servizi informatici aziendali

21.1 Ai sensi del presente regolamento, la disponibilità dei servizi informatici aziendali cesserà nei seguenti casi:

- qualora non sussistesse più la condizione di dipendente o di collaboratore esterno, tirocinante, etc;
- qualora non fosse confermata l'autorizzazione all'uso fornita dal Responsabile;
- qualora vengano accertati, secondo i procedimenti aziendali:
    a. un uso non corretto dei servizi informatici aziendali da parte dell'utente comunque un uso estraneo alla sua attività lavorativa;
    b. manomissioni e/o interventi sul hardware e/o sul software;
    c. diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
    d. accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
    e. violazione di quanto stabilito nel presente regolamento.

Art.22

Osservanza della normativa aziendale

22.1 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.

Art.23

Aggiornamento e revisione

23.1 Il presente Regolamento è soggetto a revisione periodica. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni o modifiche al presente Regolamento tramite comunicazione alla Direzione Aziendale.