IMMEDIATAMENTE ESEGUIBILE

ORIGINALE

SISTEMA SANITARIO REGIONALE
ASL VITERBO

REGIONE LAZIO

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO N° : 217 del 24 FEB. 2015

DIREZIONE GENERALE

OGGETTO: Approvazione Regolamento Aziendale Privacy e Regolamento utilizzo delle risorse e dei servizi informatici. Integrazione Gruppo di Lavoro di cui alla delibera n.320 del 13.03.2012

MARCUCCI MANUELA
L'Estensore

RESPONSABILE ANTICORRUZIONE
Delibera CS 222/2014
Dott. Paolo Pezzato

Parere del Direttore Amministrativo : Drssa Daniela Donetti

☑ FAVOREVOLE ☐ NON FAVOREVOLE (con motivazioni allegate al presente atto)

Firma _____ Data 24 FEB. 2015

Parere del Direttore Sanitario : Dr. Antonio Bray

☑ FAVOREVOLE ☐ NON FAVOREVOLE (con motivazioni allegate al presente atto)

Firma Antonio Bray Data 24 FEB. 2015

Il funzionario addetto al controllo di budget con la sottoscrizione del presente atto, attesta che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico.

Voce del conto economico su cui si imposta la spesa : _____

Visto del Funzionario addetto al controllo di budget : Firma _____ Data _____

AUSL VITERBO
IL DIRETTORE F.F.
ECONOMIA & FINANZE
(Dott.ssa Annunziata Minopoli)

Il Dirigente e il Responsabile del procedimento attestano a seguito dell'istruttoria effettuata che il presente atto è pienamente conforme sia nella forma che nella sostanza a tutte le leggi e norme di ogni ordine e grado vigenti in materia per cui se ne attesta la legittimità assumendone di conseguenza - ex art 4 c. 2 L 165/01 - la relativa responsabilità.

Responsabile del procedimento : MARIO QUINTARELLI
Data _____ Firma _____

Il Dirigente
Data _____ Firma _____

A.U.S.L. VITERBO
DIREZIONE SANITARIA P.O.C.
DIRIGENTE AMMINISTRATIVO
DOTT. MARIO QUINTARELLI

Atto Soggetto al controllo della Corte dei Conti | |

SISTEMA SANITARIO REGIONALE
ASL
VITERBO

REGIONE
LAZIO

DIREZIONE GENERALE

OGGETTO: Approvazione Regolamento Aziendale Privacy e Regolamento utilizzo delle risorse e dei servizi informatici. Integrazione Gruppo di Lavoro di cui alla delibera n.320 del 13.03.2012

IL COMMISSARIO STRAORDINARIO

PREMESSO che con delibera n. 320 del 13/03/2012 la Direzione Generale ha provveduto alla nomina del Coordinatore Aziendale quale Responsabile della Privacy, nonché della nomina del Gruppo di Lavoro Aziendale della Privacy;

PRESO ATTO che con deliberazione n. 862 del 09/08/2012 la Direzione Generale ha individuato i Responsabili del trattamento dei dati quali i Direttori di U.O.C. ed U.O.S.D. ed i Responsabili delle UU.OO.SS. URP Rete Accesso e S.I.I.A.;

PRESO ATTO altresì che a seguito della delibera di cui sopra si è provveduto a confermare la nomina dei Responsabili delle strutture individuate con nota prot. n. 168 del 10/01/2013, invitando gli stessi a nominare i rispettivi incaricati, (come risultano agli atti del Responsabile della Privacy);

CONSIDERATO che con delibera n. 168 del 13/02/2012 è stato approvato il Documento Programmatico sulla Sicurezza dei dati e il nuovo regolamento della Privacy (Decreto Legislativo 196/2003 e successive modifiche ed integrazioni) e che la Direzione Generale ha ritenuto indicare negli obiettivi di Budget 2014 "Migliorare il sistema di sicurezza amministrativa – Definizione del Piano Aziendale della Privacy";

VISTO il provvedimento del Garante per la protezione dei dati personali n.610 del 18.12.2014 del registro dei provvedimenti riguardante il trattamento dei dati personali in ambito sanitario;

PRESO ATTO che in adempimento di quanto sopra stabilito si è provveduto alla formulazione del regolamento sulla Privacy, a cura del Responsabile della Privacy, nonché del regolamento per l'utilizzo delle risorse e dei servizi informatici aziendali quest'ultimo a cura del Dirigente SIIA;

RITENUTO pertanto dover procedere all'approvazione dei sopraccitati regolamenti, nonché alla integrazione e modifica della delibera n. 320 del 13/03/2012 relativamente alla composizione del Gruppo di Lavoro di cui trattasi, individuando in qualità di Presidente il Direttore Sanitario Aziendale il Dott. Antonio Bray, un componente dell'ufficio legale dell'ASL e il Responsabile della Prevenzione della Corruzione Aziendale il Dott. Paolo Pezzato;

DELIBERA

Per i motivi indicati nella premessa che si intendono integralmente richiamati

- di approvare il regolamento Aziendale Privacy, nonché il Regolamento per l'utilizzo delle risorse e dei servizi informatici, che fanno parte integrante del presente atto;
- di integrare il Gruppo di Lavoro della Privacy con il Direttore Sanitario Aziendale Dott. Antonio Bray in qualità di Presidente e un componente dell'ufficio legale dell'ASL e il Dott. Paolo Pezzato quale Responsabile della Prevenzione della Corruzione Aziendale che risulta essere così composto:
  - Direttore Sanitario Aziendale - Presidente — Dott. Antonio Bray
  - Direttore Sanitario COB o suo delegato - componente — Dott. Giuseppe Cimarello
  - Direttore Sanitario POF o suo delegato- componente — Dott. Franco Bifulco
  - Direttore UOC AGGE delle Risorse Umane – componente — Dott.ssa Francesca Gubiotti
  - Direttore UOC Distretto 3 o suo delegato – componente — Dott.ssa Antonella Proietti

o Coordinatore Aziendale Privacy - componente	Dott. Mario Quintarelli
o Dirigente SIIA o suo delegato - componente	Dott.ssa Patrizia Boninsegna
o Dirigente URP e Rete Accesso o suo delegato – componente	Dott.ssa Daria Natalini
o Dirigente SAIO o suo delegato- componente	Dott. Roberto Riccardi
o Responsabile della prevenzione della Corruzione – componente	Dott. Paolo Pezzato
o Rappresentante ufficio legale dell'ASL – componente	

- di individuare i dipendenti Sig.ra Carla Marino e Sig. Stefano Lucci componenti l'Ufficio di Segreteria del Gruppo Aziendale per la privacy;
- ogni riunione del gruppo di lavoro dovrà essere convocata dal presidente con specifico o.d.g. relativo ad obiettivi previsti dalla vigente normativa,
- al termine della riunione verrà redatto apposito verbale nel quale verranno proposte specifiche soluzioni o richieste interpretazioni autentiche che interessano gli obiettivi del gruppo aziendale in argomento;
- di dichiarare il presente atto immediatamente eseguibile

La presente deliberazione sarà pubblicata all'Albo dell'Azienda nei modi previsti dall'art.31 della L. R. Lazio n.45/96.

Il Direttore Amministrativo
(Dr.ssa Daniela Donetti)

Il Direttore Sanitario Aziendale
(Dr. Antonio Bray)

Il Commissario Straordinario
(Dr. Luigi Macchitella)

REGOLAMENTO PRIVACY

Art. 1 — Oggetto

Il presente regolamento contiene disposizioni attuative della L. 31.12.1996 n. 675 e s.m.i. e del Codice della Privacy D.Lgs 30 giugno 2003 n. 196, nell'ambito delle strutture, servizi e Presidi della AUSL Viterbo, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la medesima.

L'Azienda assicura l'adozione di misure di sicurezza anche preventive idonee ad evitare situazioni di rischio e non conformità o di alterazione di dati. L'Azienda adotta le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell' artt. 7 e 8 della legge 196/2003.

Art.2 — Dati Personali

I dati personali (art. 4 comma 1, lett. b) di cui D.Lgs 196/2003 si riferiscono ad informazioni relativi a persona fisica, persona giuridica, ente od associazione identificati o identificabili anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un codice di identificazione del soggetto.

Il dato sensibile, ai sensi dell'art. 4 comma 1, lett. d) del D.lgs 196/2003, è quel dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti politici, sindacati, associazioni od organizzazioni di carattere religioso, nonché il dato personale idoneo a rivelare lo stato di salute e la vita sessuale dell'interessato.

Art. 3 — Trattamento dei dati personali

Con l'espressione "trattamento", ai sensi dell'art. 4, comma 1, lett. a) del D.lgs 196/2003 si intende qualunque operazione o complesso di operazioni, svolte, con o senza l'ausilio di mezzi elettronici o comunque automatizzati, alla raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione , il blocco, la comunicazione, la diffusione, la cancellazione o la distruzione dei dati.

Il trattamento dei dati attiene alla responsabilità del Titolare del trattamento e delegato ai Responsabili e agli Incaricati del trattamento.

Il trattamento dei dati personali deve avvenire nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità della persona, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda.

L'Azienda non consente il trattamento di dati da parte di personale non autorizzato.

Il trattamento dei dati sensibili è invece consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Nei casi in cui una disposizione specifichi le finalità di rilevante interesse pubblico, ma non la tipologia di dati sensibili e di operazioni eseguibili, il trattamento è consentito previa

autorizzazione solo in relazione ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare di cui all'art. 20, comma 2 del D.lgs 196/2003.

Trattamenti con uso di apparecchiature informatiche di cui in allegato al presente regolamento

Art. 4 — Titolare del trattamento dei dati personali

Il Titolare del trattamento, ai sensi art. 4 comma i lettera f) D.lgs 196/2003, è l'AUSL di Viterbo legalmente rappresentata dal Direttore Generale. Il Titolare, avvalendosi operativamente del Coordinatore del Gruppo Privacy di cui all'art. 17 del presente regolamento, provvede, nei casi previsti dalla legge a:

- Assolvere l'obbligo di notificazione al Garante art. 37 D.lgs 196/2003;
- Identificare i dirigenti responsabili dei trattamenti
- Identificare e classificare le procedure di trattamento (anagrafe dei trattamenti)
- Richiedere al Garante l'autorizzazione al trattamento dei dati sensibili, ove necessaria;
- Adottare, per quanto di competenza, le misure necessarie a garantire la sicurezza dei dati personali;
- Impartire ai Responsabili le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza;
- Verificare periodicamente l'osservanza dell'attività svolta dai Responsabili rispetto alle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.
- Provvedere alla formazione degli incaricati del trattamento dei dati personali, attraverso la previsione di interventi formativi, al fine di renderli edotti dei rischi che incombono sui dati delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare medesimo.

Art. 5 — Rapporti con il Garante

Ogni rapporto con il Garante (notificazioni, richieste di autorizzazione, comunicazioni) rientra nella competenza del Titolare che vi provvede tramite il Coordinatore del Gruppo Aziendale Privacy.

Art. 6 — Responsabili del trattamento dei dati personali

I Responsabili del trattamento dei dati personali compiono quanto necessario nel rispetto delle vigenti disposizioni in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel piano di sicurezza dei dati personali elaborato dall'Azienda. Ogni responsabile del trattamento dei dati è nominato per iscritto dal Titolare del trattamento, a sua volta nomina per iscritto gli incaricati del trattamento.

I Responsabili sono tenuti a:

- Fornire al Gruppo Aziendale per la Privacy le richieste di notificazione al Garante Privacy;

- Comunicare tempestivamente al Gruppo Aziendale Privacy tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
- Comunicare al Gruppo Aziendale Privacy l'inizio di ogni nuovo trattamento nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza, ai fine della compilazione dell'aggiornamento dell'anagrafe dei trattamenti di dati personali aziendale.

Art. 7 —Criteri per l'individuazione dei Responsabili del trattamento

I Responsabili del trattamento sono individuati fra i soggetti che per competenza ed esperienza, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

All'interno dell'Azienda sono indicati in coloro che ricoprono funzioni dirigenziali ed in particolare:

- Direttori di Struttura Complessa e di strutture Dipartimentali, o altri dirigenti, per i quali si rende opportuna la designazione di Responsabili del trattamento in virtù, delle particolarità organizzative e funzionali delle attività di competenza. L'elenco completodei responsabili è contenuto nella delibera di approvazione del DPS Aziendale Aziendale e disponibile presso l'Ufficio del Coordinatore del Gruppo Privacy:

Art. 8 — Nomina dei Responsabile del trattamento

La nomina dei Responsabili del trattamento viene effettuata con atto deliberativo del Direttore Generale. L'atto di nomina dovrà essere notificato per iscritto ai soggetti individuati (allegato 1).

Art. 9 — Incaricati del trattamento

Gli incaricati sono identificati dai responsabili in tutti coloro che sono autorizzati ad effettuare operazioni di trattamento dei dati. Essi, in relazione alle funzioni loro assegnate, hanno accesso ai soli dati la cui conoscenza sia strettamente necessaria al trattamento. Gli incaricati devono eseguire i trattamenti nel rispetto delle procedure secondo le disposizioni date dal Responsabile del trattamento, con nomina per iscritto (Allegato 2).

Art. 10 Trattamento di dati affidati all'esterno

Agli Enti e agli organismi e agli altri soggetti pubblici o privati esterni all' Azienda ed alle strutture accreditate, ai quali sono affidati attività o servizi, con esclusivo riferimento alle operazioni di trattamento di dati, viene attribuita la qualità di Responsabile ai sensi dell'art. 29 del D.lgs 196/2003 (allegato 3)

Negli accordi con le strutture accreditate e nei contratti di affidamento di fornitura o di servizi all'esterno dell'Azienda (outsourcing) deve essere inserita apposita clausola di garanzia con la quale il soggetto accreditato o affidatario si impegna, per i trattamenti dei dati affidati in forza del rapporto contrattuale, all'osservanza delle norme di legge sulla protezione dei dati personali e delle disposizioni dell'AUSL di Viterbo in materia. In sede di prima applicazione del presente regolamento, le strutture aziendali competenti per la stipula e la conservazione dei contratti effettuano una costante ricognizione dei contratti in essere, al fine di provvedere, alla eventuale nomina di Responsabile esterno del soggetto a cui è affidata l'attività o il servizio come da allegato A, ovvero all'inserimento

nei contratti medesimi della clausola di garanzia sui trattamenti. Le copie di tali contratti devono essere inviate al Coordinatore del Gruppo Aziendale Privacy. I responsabili esterni operano nel rispetto del presente regolamento in analogia con le competenze e responsabilità affidate ai responsabili interni.

Art. 11 — Criteri per l'esecuzione del trattamento dei dati personali

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto del trattamento devono essere i soli dati essenziali per lo svolgimento delle attività istituzionali. I dati personali devono essere trattati in modo lecito, e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni dei trattamenti in termini compatibili con tali scopi. Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi, anche su richiesta di altri soggetti, così come previsto dall'art. 4 del D.lgs n. 135/99.

I Responsabili del trattamento sono tenuti a verificare periodicamente l'esattezza l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultassero eccedenti o non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I trattamenti di dati effettuati impiegando le banche dati di più titolari diversi dall'AUSL (interconnessione di banche dati), sono utilizzati nelle sole ipotesi previste da espressa disposizione di legge.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente rispetto ai dati anagrafici personali ciò nella ricostanza che i dati non richiedono il loro diretto utilizzo, ovvero devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli incaricati del trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni affidate.

Art. 12 — Informativa all'interessato (consenso informato)

L'informativa è l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.

Acquisire uno specifico consenso informato dell'interessato per utilizzare – attraverso il dossier sanitario – anche le informazioni sanitarie relative a eventi clinici pregressi anche erogate dall'Azienda.

L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso. Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del D.lgs 196/2003 e più specificatamente:

- le le finalità e le modalità con le quali vengono trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a fornire i dati;

- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo successivo;ù
- gli estremi identificativi del Titolare e del Responsabile e dell'incaricato al trattamento;

La predetta informativa può essere resa anche tramite affissione di apposite informative a stampa nei locali di accesso all'utenza, secondo procedure e attraverso modelli concordati con il Gruppo Aziendale per la Privacy.

Art. 13 — Diritti dell'interessato

Secondo quanto disposto dall'art. 7 del D.lgs 196/2003, l'interessato ha diritto di ottenere a cura del Titolare o del Responsabile, senza ritardo:

1) la conferma dell'acquisizione o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;

2) l'indicazione:

a) dell'origine dei dati personali trattati;

b) delle finalità e delle modalità del trattamento;

c) della procedura applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del Titolare;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabil o incaricati

3) di fare richiesta di:

f) aggiornamento, rettifica ovvero, qualora vi abbia interesse, integrazione dei dati;

g)cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione li legge, compresi quelli di cui non è necessaria la conservazione in relazione alle finalità per le quali i dati sono stati raccolti o successivamente trattati;

h) attestazione che le operazioni di cui ai precedenti punti f) ed g) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

4) L'interessato ha inoltre il diritto di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta nonché di poter esprimere la volontà di oscurare nel proprio dossier sanitario anche le informazioni relative ai singoli eventi clinici relativi al pregresso

Nel caso in cui intenda presentare ricorso per fatti inerenti il trattamento dei propri dati personali, l'utente dovrà rivolgere istanza scritta a:

AUSL di Viterbo Gruppo Aziendale per la Privacy Via E. Fermi n. 15 01100 Viterbo

L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Per quanto non riportato agli artt. 12 e 13 si fa riferimento al provvedimento del Garante per la protezione dei dati personali n.610 del 18.12.2014.

Art. 14 — Amministratori di sistema

Il Titolare e i Responsabili del trattamento per i quali si prevede l'utilizzo di apparecchiature informatiche si avvalgono, nella individuazione e applicazione delle misure necessarie a garantire la sicurezza del sistema, di amministratori di sistema formalmente individuati a tale scopo dal Responsabile del Servizio Sistema Informativo Aziendale ai sensi del D.P.R. 318/99, che deve essere nominato con apposito atto deliberativo. In prima applicazione l'amministrazione di sistema è stato individuato con atto 441/2013.

Art. 15 — Documento programmatico della sicurezza

Di prendere atto del Decreto Legge 09 febbraio 2012 n. 5 recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito con modificazioni, dalla legge 4 aprile 2012, n. 35 (Gazzetta Ufficiale n. 82 del 06 aprile 2012).

Art. 16 — Sicurezza degli archivi cartacei

L'accesso agli archivi aziendali deve essere controllato, e devono essere identificati, autorizzati e registrati i soggetti.

Con riferimento agli archivi aziendali la responsabilità della conservazione e sicurezza dei medesimi spetta al responsabile competente per i dati oggetto del trattamento; i /il responsabili/e dovranno essere nominati con apposito atto deliberativo.

Gli archivi delle cartelle cliniche prodotte in ambito ospedaliero sono sotto la responsabilità:

- del Direttore della U.O. (o del modulo dipartimentale) dal momento della formazione della cartella e per tutto il periodo di conservazione della medesima presso il reparto;
- del Direttore del Presidio Ospedaliero al momento in cui la cartella perviene all'archivio centralizzato;
- per le cartelle cliniche e la documentazione equipollente giacente presso strutture non ospedaliere la responsabilità farà capo al Direttore della Struttura ove i medesimi atti sono materialmente conservati;
- nel caso di documentazione archiviata presso ditta convenzionata, il legale rappresentante della medesima è responsabile della conservazione e della sicurezza;
- nel contratto di affidamento del servizio dovrà essere prevista un'apposita clausola di garanzia e la possibilità per l'Azienda di accedere ai locali per verificare il rispetto alle prescrizioni della legge in materia di privacy e del presente regolamento.

MISURE DI SICUREZZA FISICHE

Gli archivi cartacei devono essere situati in locali non esposti a rischi ambientali (quali allagamenti, incendi, deterioramenti di varia natura etc.), anche in ossequio alle disposizioni in materia di sicurezza di cui D.lgs 81/08 e successive modificazioni ed integrazioni.

E' opportuno che venga predisposto un piano periodico aziendale per la conservazione e lo scarto dei documenti, in conformità alle vigente normativa nazionale in tema di conservazione di documenti. A tal fine, partendo dalla rilevazione dei trattamenti di dati ai sensi del D.lgs 196/2003, le singole strutture operative aziendali sono tenute a segnalare al Referente Aziendale per la Privacy la tipologia, l'ubicazione, il metodo di catalogazione e di custodia, la quantità approssimativa e l'anno di riferimento della documentazione custodita ai fini dell'aggiornamento del censimento dei trattamenti di dati personali e/o sensibili.

Per la documentazione riguardante dati personali sensibili e non, è opportuno che ciascun presidio/edificio aziendale si dotasse di un proprio archivio centralizzato munito di misure di sicurezza (meccanismi di chiusura dei locali e dei contenitori, sistemi di allarme a protezione dei locali, etc.. ..) idonee a garantire l'inaccessibilità ai locali stessi da parte di soggetti non autorizzati. Per quanto concerne specificatamente la documentazione sanitaria ed in particolare le cartelle cliniche, per le modalità di tenuta, archiviazione e rilascio copia ogni Azienda dovrà attenersi alla normativa vigente, prestando particolare attenzione a quanto stabilito nell'art. 92 del D.lgs 196/2003.

MISURE DI SICUREZZA LOGICHE

L'Azienda è tenuta ad impartire ai dipendenti che, in ragione delle loro mansioni si trovino ad utilizzare dati personali sensibili e non, adeguate raccomandazioni al fine di una doverosa responsabilizzazione dei soggetti stessi, in particolare per ciò che concerne la conservazione della documentazione cartacea onde evitare accessi non autorizzati perdita smarrimento o distruzione dei dati stessi.

Ricordando che la circolazione infraziendale dei dati, in particolar modo di quelli sensibili, non può eccedere quanto necessario per il puntuale svolgimento dei compiti istituzionali, si raccomanda all'Azienda di adottare modalità e accorgimenti tali da garantire il massimo rispetto della normativa contenuta dal D.lgs 196/2003 soprattutto in relazione ai provvedimenti amministrativi, in particolare delibere e determine dirigenziali, in special modo nella fase di pubblicazione e di rilascio di copie ai sensi della L. 241/90 e s.m.i.

La sicurezza dei dati assicurata con le modalità qui disposte deve essere garantita anche per i dati trattati da personale non dipendente dell'Azienda (tirocinanti, specializzandi...), nonché da personale dipendente che svolge attività libero-professionale intramuraria nei casi in cui questa si svolga presso le strutture aziendali o comunque in locali messi a disposizione dell'Azienda.

MISURE DI SICUREZZA INFORMATICHE

Secondo quanto riportato nel regolamento per la sicurezza informatica, la cui elaborazione è a cura della Responsabile SIIA, si distinguono le seguenti tipologie di trattamento dei dati informatici:

a) **Trattamento dei dati su personal computer**

l'Azienda anche con delega alle UU.OO. incaricate dei trattamenti; è tenuta a predisporre idonee procedure di salvataggio periodico degli archivi e di antivirus, nonché a provvedere alla. registrazione degli accessi con assegnazione ed inserimento di password, tenendo sempre presente le misure minime di sicurezza previste dal D.lgs 196/2003.

b) Trattamento dei dati all'interno di procedure in rete:

- le apparecchiature informatiche devono essere collocate in locali non esposti a rischi ambientali (allagamenti, incendi, deterioramenti di varia natura...), anche in conformità alle disposizioni in materia di sicurezza di cui al D.lgs 81/2008;
- i server devono essere posti sotto gruppo di continuità, onde evitare sbalzi o cadute di tensione che potrebbero danneggiare i dispositivi fisici delle macchine e quindi dei dati;
- deve essere previsto un sistema di salvataggio periodico sul data-base aziendale;
- è opportuno che vengano previste modalità di autenticazione per l'accesso alle varie procedure (password, schede magnetiche, firma digitale, etc...);
- l'Azienda è tenuta a realizzare una propria rete che si interfacci verso l'esterno in maniera controllata e garantita da appositi meccanismi di difesa (proxy-server antivirus e firewall).

c) Accessi ai dati

Gli accessi vengono gestiti dal SIIA aziendale che provvederà tramite la struttura CED ad attivare / annullare i profili utenti e le relative password.

Art. 17 — Gruppo Aziendale per la Privacy

L'Azienda individua un Gruppo Aziendale di studio e di lavoro in materia di privacy e garantisce al medesimo adeguato supporto, anche esterno, per lo svolgimento dei compiti assegnati.

Il Gruppo Aziendale per la Privacy è nominato con disposizione del Direttore Generale. All'interno del Gruppo Privacy ed individuato un Coordinatore con funzioni di coordinamento del gruppo, di tenuta dei rapporti con i Responsabili del trattamento, e di segreteria. Ogni comunicazione al Gruppo Privacy o al Titolare del trattamento andrà indirizzata al Coordinatore.

Il Gruppo Aziendale Privacy svolge i seguenti compiti:

1. garantisce il supporto alla Direzione aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali.
2. assicura la propria collaborazione per la stesura aggiornamento del documento programmatico per la sicurezza dei dati;

3. promuove l'osservanza del regolamento aziendale sulla privacy, fornendo il necessario supporto in ordine alle problematiche in tema di riservatezza;

4. tiene ed aggiorna il censimento dei trattamenti di dati personali e/o sensibili custoditi a livello aziendale sulla base delle indicazioni fornite dai Responsabili del trattamento.

Art. 18 — Il censimento dei trattamenti dei dati personali e/o sensibili

L'Azienda realizza il censimento dei trattamenti dei dati personali e/o sensibili (anagrafe). Il censimento contiene per ogni UU.OO. i trattamenti dei dati di competenza suddivisi per tipologie e per strutture organizzative, come presupposto necessario per adempiere agli obblighi di legge; è tenuto a cura del Gruppo Aziendale per la Privacy, in collaborazione con i Responsabili del trattamento; esso viene aggiornato qualora vengano comunicati da parte del Titolare o dei Responsabili del trattamento casi di attivazione, cessazione o modifica di nuovi trattamenti.

Art. 19 — Rapporti tra diritto di accesso e diritto alla riservatezza

Ai fini dell'accesso alla documentazione amministrativa viene fatto esplicito riferimento al regolamento di accesso alla documentazione amministrativa che disciplina le modalità ed i casi di esclusione dell'accesso ai documenti amministrativi, in conformità all' art. 24 della 17 agosto n. 241.

Ai sensi dell'art. 92 D.lgs 196/2003, eventuali richieste di presa visione o di rilascio di copia della cartella clinica e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dell'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dal richiedente o da organismi giudiziari, ecc.

a) di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Le richieste di accesso alle cartelle cliniche ospedaliere di un terzo sono valutate dal Direttore dello Stabilimento, che ne ha la responsabilità, applicando i criteri enunciati nel capoverso che precede. Ai fini del bilanciamento degli interessi potrà essere chiesto parere al Gruppo Aziendale Privacy.

Le modalità in ordine alle richieste di rilascio di copie della documentazione sanitaria sono oggetto di apposita regolamentazione.

Tutta la documentazione sanitaria (non solo le cartelle cliniche) può essere ritirata anche da persona diversa dal diretto interessato, purchè sulla base di una delega scritta e mediante consegna dei documenti in busta chiusa.

I dati personali idonei a rilevare lo stato di salute possono essere resi noti all'interessato solo attraverso le modalità previste dall'art. 84 del D.lgs 196/2003.

Art. 20 — Videosorveglianza

L'Azienda disciplina l'attività di videosorveglianza finalizzata alla sicurezza degli utilizzatori, utenti o dipendenti, delle strutture aziendali, nonché alla tutela del patrimonio aziendale, con apposito regolamento pur nel pieno rispetto della normativa sulla privacy.

Non rientra nel campo di questa attività l'utilizzo di apparecchiature strumentali per la rilevazione ed il monitoraggio dei parametri vitali dei pazienti né le attività di controllo a distanza dei lavoratori.

L'attivazione di trattamenti di dati con modalità particolari tali da coinvolgere anche informazioni relative al personale dipendente (quali videosorveglianza, monitoraggio della posta elettronica e degli accessi a Internet etc.) l'Azienda adotterà una specifica regolamentazione atta a garantire il rispetto della normativa in tema di riservatezza dei dati personali nonché di tutela del lavoratore dipendente (l.. 300/70).

Simile regolamentazione sarà, altresì adottata per garantire lo scambio di notizie tra l'Azienda ed i mezzi ufficiali di informazione (giornali e televisioni), onde assicurare il massimo rispetto della riservatezza dei dati personali dei soggetti interessati dalle notizie e, contemporaneamente il diritto-dovere di informazione.

Art. 21 — Norma di rinvio

Per quanto non espressamente disciplinato dal presente Regolamento si rimanda al Decreto Legislativo n. 196/2003 e successive modificazioni ed integrazioni.

All.n. 1

MODULO DI DEFINIZIONE PROCEDURE DI TRATTAMENTO DATI

U.O. di : ..... Codice U.O. .....

Responsabile del trattamento: ..... cod: .....

Ufficio incaricato del trattamento: ..... Sede: .....

Descrizione del trattamento / finalità (art. 85 D.Legs 196/2003):

.....

.....

Denominazione Procedura di trattamento dati: .....

Codice U.O. : ..... N. Trattamento: .....

Descrizione dei dati trattati: - .....

- .....
- .....
- .....

Tipologia di dati (art. 4 D.Legs. 196/2003) :

Identificativi Personali (Etnici, Razza, Religione, Politico Sindacali, Sessuali, Stato di salute) ☐,
Giudiziari ☐,
Sensibili ☐,
Altro ☐.

Sede / Luoghi dove vengono trattati i dati: .....

.....

.....

Sede e luoghi dove vengono conservati i dati : .....

.....

.....

Categoria di soggetti a cui i dati si riferiscono:

Utenti / assistiti ☐, clienti ☐, dipendenti ☐, fornitori ☐, altri ☐

Tipologia di procedura utilizzata:

Manuale / Cartacea ☐, Informatizzata ☐, Audio Video – per Immagini ☐, Mista ☐.

Origine dei dati. Raccolti: dall'interessato ☐, da soggetto privato ☐, da soggetto pubblico ☐.

Interconnessione con altri trattamenti:

in carico alla stessa U.O. ☐,
in carico ad altra U.O. ☐ descrizione: ...../ .....

Comunicazione dei dati: verso soggetti pubblici (Regione, Autor. Giudiz., Aziende Sanit., Direz. Provinc. Tesoro, INPS, ecc.) ☐,

Verso soggetti privati ☐ : specificare
.....
.....
.....

Diffusione dei dati : Normativa di riferimento: .....;
Soggetti destinatari (stampa, soc. scientif., università, ecc.) ☐:
.....
.....
.....

TRATTAMENTI CHE UTILIZZANO PROCEDURE INFORMATIZZATE

Sistema di elaborazione utilizzato:
- Non accessibile ad altri operatori ☐
- In rete non accessibile al pubblico ☐
- In rete accessibile al pubblico ☐

Modalità di protezione dei dati: criptaggio ☐, cifratura ☐, altro ☐

Data Base di conservazione / di aggiornamento dati : SI / NO

Funzioni autorizzate :
Inserimento dati ☐
Lettura e stampa ☐
Variazione dati ☐
Cancellazione dati ☐
Estrazione ☐
Alimentazione flussi ☐

Software utilizzati: .....;
.....;
.....

Il responsabile del trattamento

OSSERVAZIONI: .....
.....
.....

MODULO NOMINA INCARICATO AL TRATTAMENTO DEI DATI

U.O.di : ..... Al Sig. ..... Incaricato del trattamento

Il sottoscritto, dirigente dell'U.O. di ..... , responsabile della procedura di trattamento dei dati : ..... Cod. ..... / ....,

in relazione :

- al sistema **manuale** di trattamento dei dati utilizzato ☐
- al sistema **informatizzato** di trattamento dei dati utilizzato ☐
- al sistema **misto** di trattamento dei dati utilizzato ☐

con la presente **nomina, quale incaricato del trattamento,** il Sig. /a .....,

.....matr. .....

segnalando che il/la sunnominato è abilitato ad effettuare gli interventi di seguito elencati:

- ....
- ....
- .....,

utilizzo di procedura informatizzata SI ☐

con abilitazione alle seguenti funzioni:

Inserimento dati ☐
Lettura ☐
Stampa ☐
Variazione dati ☐
Cancellazione dati ☐
Alimentazione flussi ☐
Archiviazione / conservazione di documenti ☐

NO ☐ (senza utilizzo di procedure informatizzate)

Funzioni per la cui esecuzione si richiede la piena osservanza della normativa vigente in tema di privacy, conservazione e sicurezza dei dati .

Per il trattamento di dati informatici, si richiede per il Sig. /a ....., che è responsabile della custodia delle password, l'attribuzione di apposita password di accesso alla procedura sopraindicata.

Data / / Firma del responsabile del trattamento

13

ALLEGATO B

Comunicazione- tipo al Referente Aziendale Privacy per la stipula di convenzione/contratto e nomina del responsabile esterno trattamento dati

Al Direttore U.O.C

_____

Al Referente Aziendale Privacy

OGGETTO: Comunicazione ai sensi del Regolamento aziendale per la protezione dei dati personali

Si comunica che in data _____ questa Azienda ha stipulato un/una contratto/convenzione con cui è stata affidata a terzi l'attività, di seguito indicata, che comporta il trattamento di dati personali:

Si indicano i dati identificativi ed il recapito del soggetto, da nominare responsabile esterno del trattamento, cui è stata affidata l'attività sopra menzionata:

Distinti saluti

Il Responsabile del trattamento dei dati
Direttore/Responsabile UO _____

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

SOMMARIO

PREMESSA

La progressiva diffusione delle nuove tecnologie I.C.T. ed in particolare l'utilizzo della posta elettronica e l'accesso alla rete Internet, espone l'Azienda A.U.S.L. e gli utenti (dipendenti e collaboratori della stessa) a potenziali 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 A.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 A.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.

16

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 A.U.S.L., in possesso o meno di specifiche credenziali di autenticazione per l'utilizzo delle procedure aziendali;
- Per "*I.C.T.*", 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.I.A.*" è l'acronimo di Sistemi Informativi e Informatici Aziendale; è la struttura aziendale preposta al corretto funzionamento delle risorse informatiche aziendali. Per "*Tecnici del S.I.I.A.*" si intende il personale della suddetta articolazione o altra persona da essa temporaneamente delegata (ad es. consulenti, società esterna addetta alla manutenzione, ecc.). Il S.I.I.A. incorpora al suo interno il "*S.I.A.*" (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.

Art.3: Finalità

3.1 Le apparecchiature informatiche, i programmi, e tutte le risorse informatiche che l'Azienda A.U.S.L. di Viterbo 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.

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

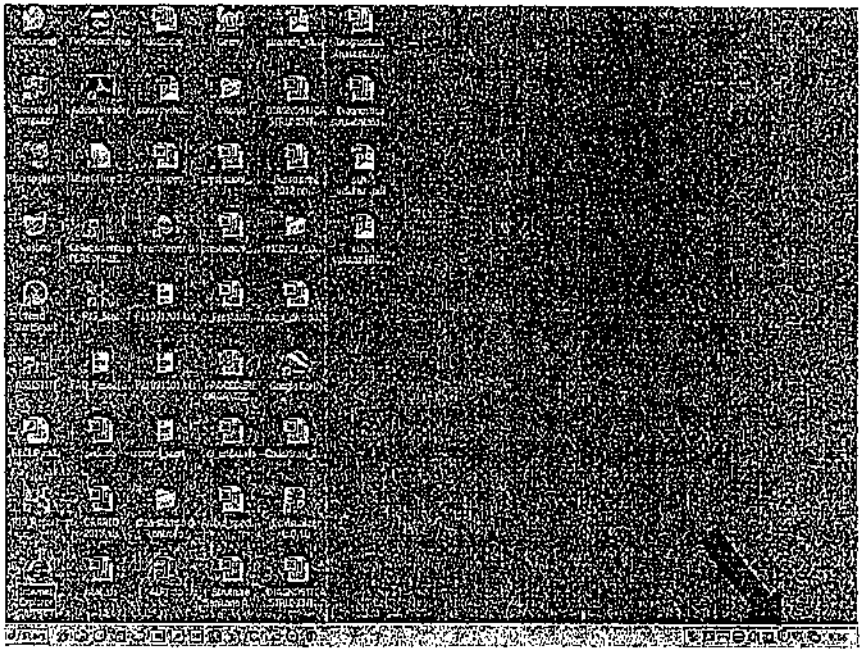
Art.4: Software Installato

4.1 E' vietato provare ad installare arbitrariamente i software, anche free, scaricati da Internet.
Ogni installazione, qualora l'uso fosse collegato ad esigenze lavorative, dovrà essere autorizzata dal S.I.I.A..
4.2 E' facoltà del S.I.I.A. bloccare automaticamente il download, da siti non istituzionali o non affidabili, di programmi o eseguibili potenzialmente infetti. Nel caso in cui sia necessario "scaricare" ulteriori programmi o eseguibili, anche gratuiti, dalla rete, l'utente dovrà formulare una richiesta, preventivamente autorizzata dal Responsabile della propria U.O., al S.I.I.A. che provvederà ad autorizzare il download ovvero ad effettuare direttamente l'installazione del programma.

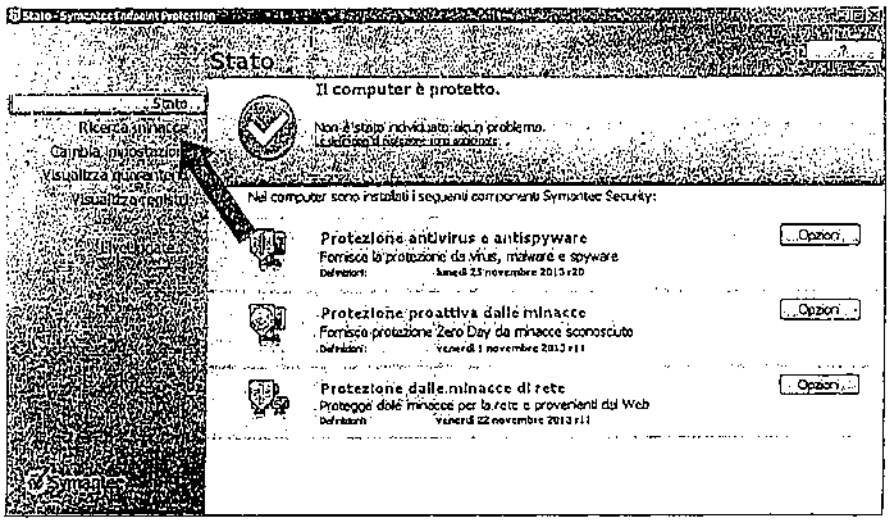
Art.5: Software Anti Virus

5.1 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 presenti nella sezione *MATERIALE INDESIDERATO* e relativi allegati sospetti e non navigare su siti non strettamente collegati ad esigenze professionali. La politica di sicurezza aziendale prevede l'utilizzo presso tutti i PC di uno stesso software antivirus 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.I.I.A. Ogni utente è tenuto comunque a controllare la presenza e il regolare aggiornamento del software antivirus aziendale e della definizione dei virus. Nello specifico, per effettuare la scansione dell'intero sistema per la ricerca di eventuali virus i passi da seguire sono:

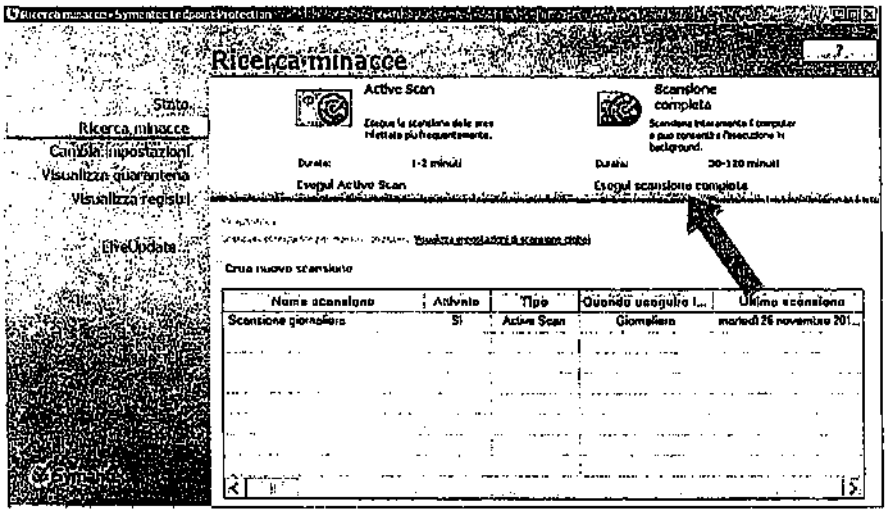
- Fare doppio click con il tasto sinistro del mouse sull'icona del sistema antivirus (l'icona è uno scudo giallo riportato in basso a destra del desktop accanto all'orologio del sistema) come indicato nell'immagine seguente;



- Una volta lanciato il programma antivirus, la cui schermata è riportata di seguito, fare singolo click con il tasto sinistro del mouse sulla dicitura *RICERCA MINACCE* presente nell'elenco a sinistra del software antivirus;



- Lanciare una scansione dell'intero sistema facendo singolo click con il tasto sinistro del mouse sulla dicitura ESEGUI SCANSIONE COMPLETA, come meglio specificato nella successiva immagine.



Nel caso in cui 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.I.I.A./C.E.D.

Nell'eventualità di PC non collegati alla rete aziendale sarà cura dell'utente provvedere al regolare aggiornamento del software.

5.2 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.6: Utilizzo del Personal.Computer

6.1 Il Personal Computer affidato all'utente/servizio è uno strumento di lavoro che 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 A.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.

6.2 I tecnici del S.I.I.A., o le società in out-sourcing alla scopo contrattualizzate, sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la manutenzione, la sicurezza e la salvaguardia del sistema stesso (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Pur rispettando tutti i criteri di riservatezza, anche riportati nel documento programmatico sulla sicurezza dei dati e nel regolamento della privacy (delibera AUSL VT n. 168 del 13/02/2012) 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.I.I.A. possono in qualunque momento procedere alla rimozione di ogni file od applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

6.3 Il personale incaricato del settore S.I.I.A. 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.I.I.A. 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.

6.4 Le stazioni di lavoro vengono predisposte e configurate dai tecnici del S.I.I.A. o dalle ditte esterne allo scopo contrattualizzate, per le esigenze dell'utente finale. Ai fini della manutenzione del sistema viene creato su ogni PC un profilo utente "*administrator*" 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; a tale scopo è facoltà del S.I.I.A. rimuovere/modificare eventuali altri utenti aventi i privilegi di amministratore di sistema. Inoltre, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori o modem) senza il preventivo consenso del S.I.I.A..

6.5 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.

6.6 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici e deve essere bloccato in caso di assenze prolungate dall'ufficio. 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.

6.7 E' consentito agli utenti l'utilizzo di PC personali previa autorizzazione scritta del Responsabile dell'U.O. di appartenenza e comunicazione al S.I.I.A. 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.I.I.A. 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 antivirus adeguato. Sarà cura del proprietario del PC e dell'utilizzatore della postazione tenere aggiornato il software antivirus.

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

6.9 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.7: Utilizzo di PC portatili personali o in dotazione

7.1 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.

7.2 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.

7.3 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.

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

7.5 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.8.

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

7.6 Qualora il portatile sia di proprietà personale si applicano le medesime disposizioni previste al punto 6.7 del presente Regolamento.

Art.8: Internet e Posta Elettronica: Gestione ed assegnazione delle credenziali di autenticazione per l'accesso

8.1 Tutti i dipendenti ed i collaboratori dell'Azienda possono richiedere l'accesso ad Internet e l'attivazione di una casella di posta elettronica compilando e spedendo via fax il modulo di richiesta pubblicato nell'area riservata del sito aziendale (www.asl.vt.it). Tali benefici potranno essere concessi anche a strutture esterne che collaborano con l'Azienda, previa autorizzazione del Dirigente Responsabile di competenza.

8.2 Le credenziali di autenticazione per l'accesso alla rete e per l'utilizzo del servizio di posta elettronica vengono assegnate dal personale del S.I.I.A., previa formale richiesta da effettuare attraverso la compilazione dell'apposito modulo allegato (All. N. 1), 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 dell'apposito modulo allegato (All. N. 1) 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.I.I.A. al fine di evitare un possibile uso illecito dei servizi

forniti e delle credenziali di autenticazione. La medesima modulistica (All. N. 1) 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.I.I.A. senza l'utilizzo dell'apposito modulo (All. N. 1), o eventualmente con compilazione non corretta o incompleta (es. manca firma del Responsabile, manca indicazione della password, etc.) non sarà presa in considerazione.

8.3 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (userid), assegnato dal S.I.I.A. , 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.

8.4 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 (*password forte*).

8.5 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.

8.6 Qualora la parola chiave fosse stata dimenticata, si procederà alla sua sostituzione d'intesa con il personale del S.I.I.A., 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.

8.7 Soggetto preposto alla custodia delle credenziali di autenticazione per l'accesso ad Internet ed alla posta elettronica, è il personale incaricato del S.I.I.A..

8.8 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.9: Programmi Gestionali: Gestione ed assegnazione delle credenziali di autenticazione per l'accesso

9.1 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 A.U.S.L., ovvero da richiedere al S.I.I.A.

9.2 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.I.I.A., anche in caso di trasferimento del dipendente ad altra struttura o eventuale cessazione del rapporto di lavoro con l'Azienda.

Art.10: Registrazione delle attività

10.1 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.I.I.A. Nell'ambito dell'attività autorizzata alla navigazione in internet, con cadenza giornaliera, il S.I.I.A. 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.

10.2 L'Azienda A.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 A.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.11: Utilizzo della rete dell'Azienda A.U.S.L.

11.1 La rete dell'Azienda A.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.
11.2 E' assolutamente vietato connettere alla rete PC personali configurati con indirizzo IP statico, assegnato direttamente dall'utente, senza una preventiva autorizzazione del S.I.I.A.. Introdurre un PC 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 S.I.I.A. che effettuerà la giusta configurazione della macchina.
11.3 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 il S.I.I.A. Analogamente non è ammesso l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub).
11.4 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.
11.5 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.I.I.A. 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.I.I.A. procedere al blocco, se necessario, dell'attività di rete del PC.
11.6 L'utilizzo di reti Wireless(rete senza fili) deve essere autorizzato dal S.I.I.A. 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.
11.7 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.I.I.A.

Art.12: Connessione ad Internet tramite dispositivi Dial-Up

12.1 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.
12.2 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.I.I.A. 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.13: Virtual Private Network

13.1 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.I.I.A. dietro richiesta del Responsabile dell'U.O. interessata che dovrà segnalare tempestivamente eventuali modifiche o cessazione di rapporti con la ditta esterna autorizzata.

Art.14: Navigazione in Internet

14.1 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.

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

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

14.4 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 S.I.I.A. 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 web-mail 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.

14.5 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda A.U.S.L. potrà adottare 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.

14.6 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 A.U.S.L. nominare un'apposita commissione per valutare l'ammissibilità della richiesta.

14.7 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.I.I.A. 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.15: Corsi On-Line

15.1 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.I.I.A. l'abilitazione.

Art.16: Posta Elettronica

16.1 Per lo svolgimento delle mansioni lavorative, viene attribuita 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 modulo allegato (All. N. 1). Si raccomanda di utilizzare l'e-mail esclusivamente per finalità legate all' attività lavorativa. La password assegnata può essere modificata dall'interfaccia Webmail.

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

nome.cognome@asl.vt.it;

Nel caso di messaggi importanti o che devono avere valore legale deve essere utilizzata la posta elettronica certificata (P.E.C.) messo a disposizione dall'Azienda all'indirizzo:

prot.gen.asl.vt.it@legalmail.it.

E' previsto, come standard per ogni casella di posta, un dimensionamento massimo pari a 300 MB; qualora fosse necessario un dimensionamento maggiore bisogna farne richiesta al S.I.I.A.

16.3 L'accesso alla casella di posta elettronica è possibile attraverso la Home Page del sito aziendale (www.asl.vt.it) utilizzando le apposite credenziali di autenticazione fornite come indicato in precedenza; sarà possibile entrare nell'area riservata, da qui cliccando sulla voce *POSTA ELETTRONICA*, 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 *INVIATI, CESTINO*; si raccomanda inoltre di procedere all'eliminazione definitiva dei messaggi che vengono spostati nella cartella *CESTINO*.

16.4 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@asl.vt.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.

16.5 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'U.O., quest'ultimo potrà richiedere l'abilitazione al S.I.I.A., ovvero se esiste al gestore delle password.

16.6 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.

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

16.7 Si raccomanda:

- Di prestare attenzione alla dimensione degli allegati che, di norma, non devono mai superare i 4 MB;
- Di utilizzare, nel caso di invio di allegati pesanti, il formato compresso (.zip);
- 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 non eseguire il download di file eseguibili (.exe) o documenti da siti Web o Ftp non conosciuti o ritenuti non affidabili e di eliminare, senza aprirli, i messaggi di posta presenti nella cartella *MATERIALE INDESIDERATO*.
- Di dare immediata segnalazione al personale del S.I.I.A. 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).

16.8 L'iscrizione, in via eccezionale, a "mailing-list" esterne è concessa solo per motivi professionali.

16.9 E' obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo.

16.10 Si fa presente che il protocollo TCP/IP utilizzato per i sistemi di posta elettronica non usa la crittografia e 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.

16.11 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;

16.12 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, come descritto nel paragrafo 16.2, utilizzare la posta elettronica certificata, o almeno richiedere la conferma di recapito/lettura delle mail inviate.

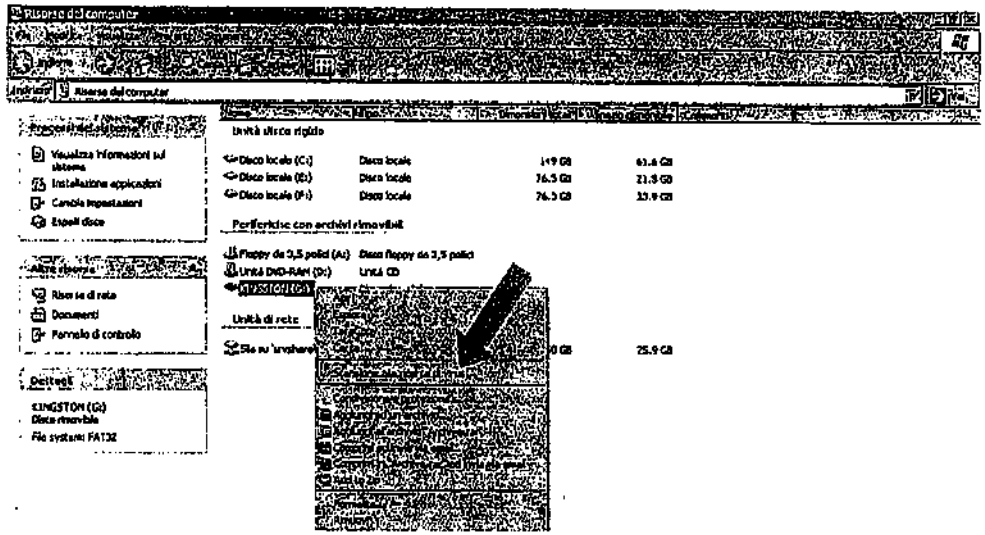
16.13 Trascorsi tre mesi dal giorno della cessazione del rapporto di lavoro con l'A.U.S.L. Viterbo, l'account di posta elettronica e i relativi dati saranno cancellati. Il periodo si riduce ad un mese per il personale con contratto a tempo determinato.

Art.17: Utilizzo di periferiche per l'archiviazione di massa (Chiavette USB)

17.1 Al fine di minimizzare l'importazione sul proprio PC od il trasferimento dal proprio PC verso altri terminali di virus o altro codice malware (worm, trojan, DoS, spyware, ecc.) tramite l'utilizzo delle periferiche di archiviazione di massa (chiavette USB), si richiede a ciascun utente di effettuare sempre una scansione della periferica prima del suo utilizzo. Per effettuare la scansione sono quattro i passi da seguire:

- Inserire la periferica di archiviazione di massa ed accedere, tramite l'apposita icona presente sul desktop, alle *RISORSE DEL COMPUTER*.
- Individuare e selezionare la propria periferica di archiviazione di massa con il mouse;
- Cliccare con il tasto destro del mouse sulla periferica di massa selezionata al passo precedente;

- Selezionare, come riportato nella figura sottostante, la voce *SCANSIONE ALLA RICERCA DI VIRUS* che lancerà la scansione sulla periferica.



Terminata la scansione, qualora non sia stata rilevata la presenza di alcun virus o malware si potrà procedere all'utilizzo della periferica di archiviazione di massa. Nel caso in cui, invece, vengano riscontrati dei virus viene vietato l'utilizzo della periferica di archiviazione di massa.

Art.18: Backup e pulizia del PC

18.1 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, siano essi PC o 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 si gestiscano dati sensibili, per motivi di sicurezza e di privacy è vietato l'uso di supporti di massa esterni (hard disk rimovibili, penne USB) che comunque, se utilizzati, devono essere custoditi in archivi chiusi a chiave.

18.2 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.

DELIBERAZIONE N° 217 del 24 FEB. 2015

composta di n. 4 pagine , frontespizio compresi e retro, e di n. 24 allegati

Pubblicato all'Albo Pretorio dell'Azienda U.S.L. il : 24 FEB. 2015
dove rimarrà affissa per quindici giorni consecutivi.

Viterbo, li 24 FEB. 2015

L' INCARICATO OO.CC. UFFICIO DELIBERE

.....

Trasmessa al Collegio Sindacale il : 24 FEB. 2015

Viterbo, li 24 FEB. 2015

L' INCARICATO OO.CC. UFFICIO DELIBERE

.....

La presente deliberazione diventerà ESECUTIVA il : 24 FEB. 2015

Viterbo, li 24 FEB. 2015

L' INCARICATO OO.CC. UFFICIO DELIBERE

.....

Viterbo, li 24 FEB. 2015

IL DIRETTORE U.O.C. AFFARI GENERALI
Drssa Francesca Gubiotti

.....