REGIONE DEL VENETO

AZIENDA UNITA' LOCALE SOCIO-SANITARIA N. 6 "VICENZA"

DELIBERAZIONE

n. 937 del 30-11-2016

O G G E T T O

Regolamento per l'utilizzo dei sistemi informatici dell'Azienda ULSS n. 6 Vicenza: approvazione.

Proponente: Servizio Affari Legali e Amministrativi Generali
Anno Proposta: 2016
Numero Proposta: 1068

Il Direttore del Servizio Affari Legali e Amministrativi Generali, riferisce:

"" La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone l'U.L.SS. n. 6 e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale connessi ad eventuali violazioni di specifiche disposizioni di legge (tra le altre, legge sul diritto d'autore e legge sulla privacy) e crea evidenti problemi alla sicurezza e alla immagine dell'azienda.

Inoltre, in capo al dipendente pubblico, oltre all'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati, vige l'obbligo di non utilizzare, a fini privati, materiali o attrezzature di cui dispone per fini istituzionali.

In questo contesto tra i poteri del datore di lavoro rientra quello, solitamente riportato nell'ambito del potere direttivo, di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il dipendente usi la prescritta diligenza e osservi le disposizioni impartitegli, anche al fine dell'eventuale esercizio del potere disciplinare.

Tuttavia, proprio in considerazione della delicatezza dell'argomento e con riferimento alla normativa in tema di protezione dei dati personali (D.lgs. 196 del 2003, c.d. "Codice della privacy"), l'attività di controllo deve essere rispettosa dei principi fondamentali di "proporzionalità", "pertinenza" e "non eccedenza" (articoli 4 e 11 del D.lgs. 196/2003) e deve, inoltre, avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato e, soprattutto, di tale attività deve essere fornita adeguata e preventiva informativa.

Come osservato dall'Autorità Garante per la protezione dei dati personali nelle "Linee Guida per posta elettronica e internet" (Deliberazione n. 13 del 01.03.2007), infatti, *"il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali"*.

Inoltre, il Codice Civile, all'articolo 2087 rubricato "Tutela delle condizioni di lavoro", recita quanto segue: *"L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro"*.

A tale riguardo, anche il Codice dell'amministrazione digitale (D.lgs. n. 82 del 07.03.2005), le cui disposizioni si applicano *"nel rispetto della disciplina rilevante in materia di trattamento dei dati personali di cui al D.lgs. 196/2003"*, stabilisce che i cittadini, i lavoratori e le imprese abbiano, in ogni caso, *"il diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie informatiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato"* (articolo 2, comma 5).

Bisogna tenere conto, altresì, delle prescrizioni dettate in materia dalla Direttiva n. 2/2009 del Ministero per la pubblica amministrazione e l'innovazione, ad oggetto *"Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro"*, nonché delle prescrizioni dettate dal *"Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del*

decreto legislativo 165/2001" approvato con il D.P.R. 16 aprile 2013 n. 62 e dal "*Codice di Comportamento dei dipendenti dell'Azienda ULSS n. 6 Vicenza*" approvato con delibera del Direttore Generale n. 337 del 09.05.2014.

Alla luce della vigente normativa sin qui citata, appare evidente come gravi sul datore di lavoro l'onere di indicare chiaramente quali siano le corrette modalità di utilizzo degli strumenti informatici messi a disposizione dei propri lavoratori e in che misura e con quali modalità possano essere effettuati eventuali controlli.

Si rende, pertanto, necessario adottare un regolamento aziendale che disciplini in modo organico la materia, in particolare regolamentando criteri e modalità operative di accesso e utilizzo del servizio internet e di posta elettronica e dei sistemi informatici dell'Azienda ULSS da parte dei dipendenti e di tutti gli altri soggetti che, a vario titolo, prestano servizio o attività per conto e nelle strutture dell'Azienda (a titolo esemplificativo: borsisti, tirocinanti, collaboratori, liberi professionisti, specializzandi, stagisti, ecc..), oltre che da parte dei dipendenti delle società esterne affidatarie di servizi, autorizzati ad accedere alla rete informatica dell'ULSS 6.

Considerato, altresì, che l'Azienda ULSS 6, nell'ottica di uno svolgimento più agevole delle attività, ha da tempo messo a disposizione dei propri collaboratori telefoni e strumenti informatici di ultima generazione *(computer portatili, tablets, telefoni cellulari, smartphone, etc*.), sono state inserite nel regolamento, che si propone di approvare con il presente atto deliberativo, alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di detta strumentazione.

Per quanto concerne la questione dei "controlli", pare opportuno fornire le precisazioni che seguono.

L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 (così detto "*Decreto sulle semplificazioni*" attuativo della Legge delega 10.12.2014 n. 183, anche nota come "*legge di riforma del diritto del lavoro*" o "*Jobs Act*") ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato "*Impianti audiovisivi e altri strumenti di controllo*".

Il testo del nuovo articolo 4 della Legge 300/1970, nel confermare, al primo comma, la precedente disciplina applicabile agli strumenti di controllo a distanza dell'attività dei lavoratori necessari per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (come le telecamere o i rilevatori di posizione Gps), ha introdotto, al comma due, una disciplina diversa per quanto concerne i dispositivi utilizzati dal lavoratore per rendere la prestazione lavorativa (computer, tablet, telefoni, smartphone). Con riferimento a questi ultimi ha stabilito espressamente che le disposizioni dettate in materia di controllo a distanza non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
Ha, inoltre, previsto che le informazioni raccolte in occasione dei controlli sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.lgs. 30 giugno 2003 n. 196 (Codice della privacy).
Alla luce delle disposizioni dettate dal succitato D.lgs. 151/2015, questa Azienda U.L.SS. può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo di detti strumenti e sulle modalità e i casi in cui potranno effettuarsi i controlli.

Si dà atto che l'anzidetta informativa a tutti i lavoratori dell'ULSS n. 6 viene garantita mediante la diffusione del Regolamento, approvato con delibera del Direttore Generale, attraverso la pubblicazione del medesimo nel sito internet aziendale, nell'*intranet* aziendale nonché nell'*Angolo del dipendente* e mediante la sua trasmissione, tramite e-mail, a tutti i dipendenti e collaboratori.

Si dà atto, infine, che la bozza di regolamento, predisposta dal Servizio Affari Legali e Amministrativi Generali in collaborazione con il Servizio per l'Informatica Generale e l'Ingegneria Clinica, è stata previamente esaminata con la Direzione Amministrativa e quindi sottoposta alla visione delle organizzazioni sindacali aziendali sia del comparto che della dirigenza, alle quali è stata fornita apposita informativa durante gli incontri sindacali del 05 agosto 2016 (con i sindacati del "comparto" e con quelli della dirigenza "SPTA") e del 13 settembre 2016 (con i sindacati della dirigenza medica e veterinaria); con successiva nota del 26.10.2016 il Servizio Risorse Umane ha inoltre provveduto a ritrasmettere il testo del nuovo Regolamento in visione alle OO.SS. della dirigenza medica e veterinaria che, sul testo stesso, non hanno formulato alcuna osservazione. ""

Il medesimo Direttore ha attestato l'avvenuta regolare istruttoria della pratica anche in relazione alla sua compatibilità con la vigente legislazione regionale e statale in materia;

I Direttori Amministrativo, Sanitario e dei Servizi Sociali e della Funzione Territoriale hanno espresso il parere favorevole per quanto di rispettiva competenza.

Sulla base di quanto sopra

IL DIRETTORE GENERALE

DELIBERA

1. di approvare il "Regolamento per l'utilizzo dei sistemi informatici dell'Azienda ULSS n. 6 Vicenza", nel testo allegato alla presente deliberazione e di cui costituisce parte integrante e sostanziale;

2. di precisare che, come previsto dal capitolo XIX del Regolamento di cui al punto n. 1, il medesimo entra in vigore dalla data di adozione del presente atto deliberativo di approvazione;

3. di stabilire che venga fornita massima pubblicità e diffusione del Regolamento mediante la sua pubblicazione nel sito internet aziendale, nell'*intranet* aziendale nonché nell'*Angolo del dipendente* e mediante la sua trasmissione, tramite e-mail, a tutti i dipendenti e collaboratori;

4. di stabilire che la presente deliberazione venga pubblicata all'Albo on line dell'Azienda.

*****

Parere favorevole, per quanto di competenza:

Il Direttore Amministrativo
(App.to Dr. Tiziano Zenere)

Il Direttore Sanitario
(App.to Dr.ssa Simona Aurelia Bellometti)

Il Direttore dei Servizi Sociali
e della Funzione Territoriale
(App.to Dr. Salvatore Barra)

IL DIRETTORE GENERALE
(F.to digitalmente Giovanni Pavesi)

Giovanni Pavesi
Digitally signed by Giovanni Pavesi
Date: 2016.11.30 15:13:18 CET

Il presente atto è eseguibile dalla data di adozione.

Il presente atto **è proposto per la pubblicazione** in data 1-12-2016 all'Albo on-line dell'Azienda con le seguenti modalità:

Oggetto e contenuto

Copia del presente atto viene inviato in data 1-12-2016 al Collegio Sindacale (ex art. 10, comma 5, L.R. 14.9.1994, n. 56).

IL RESPONSABILE PER LA GESTIONE ATTI
DEL SERVIZIO AFFARI LEGALI E
AMMINISTRATIVI GENERALI

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 6 "VICENZA"
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050 – COD. U.L.SS. 106 – COD.FISC. E P.IVA 02441500242 – Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@ulssvicenza.it
PEC protocollo.centrale.ulssvicenza@pecveneto.it
www.ulssvicenza.it

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI

dell'Azienda U.L.SS. n. 6 'Vicenza'

A cura del Servizio Affari Legali e Amministrativi Generali
e del Servizio per l'Informatica Generale e l'Ingegneria Clinica
dell'U.L.SS. n. 6 'Vicenza'

SOMMARIO del Regolamento

CAPITOLO I): PREMESSA DI ORDINE NORMATIVO

1.1. La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone l'ULSS n. 6 e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità conseguenti alla violazione di specifiche disposizioni di legge (tra le altre, legge sul diritto d'autore e legge sulla privacy), creando evidenti problemi alla sicurezza e alla immagine dell'azienda.

1.2. Si evidenzia, inoltre, che tra i poteri del "datore di lavoro" rientra quello, solitamente riportato nell'ambito del potere direttivo, di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il dipendente usi la prescritta diligenza e osservi le disposizioni impartitegli, anche al fine dell'eventuale esercizio del potere disciplinare. Al riguardo si ricorda che in capo al dipendente pubblico, oltre all'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati, vige l'obbligo di non utilizzare, a fini privati, materiali o attrezzature di cui dispone per fini istituzionali.

1.3. Tuttavia, proprio in considerazione della delicatezza dell'argomento e con riferimento alla normativa in tema di protezione dei dati personali (D.lgs. 196 del 2003, c.d. "Codice della privacy"), l'attività di controllo deve essere rispettosa dei principi fondamentali di "proporzionalità", "pertinenza" e "non eccedenza" (articoli 4 e 11 del D.lgs. 196/2003) e deve, inoltre, avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato e, soprattutto, di tale attività deve essere fornita adeguata e preventiva informativa.

1.4. Come osservato dall'Autorità Garante per la protezione dei dati personali nelle "Linee Guida per posta elettronica e internet" (Deliberazione n. 13 del 01.03.2007), infatti, *"il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali".*

1.5. Il Codice Civile, all'articolo 2087 rubricato "Tutela delle condizioni di lavoro", recita quanto segue: *"L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro".*

1.6. A tale riguardo, anche il Codice dell'amministrazione digitale (D.lgs. n. 82 del 07.03.2005), le cui disposizioni si applicano *"nel rispetto della disciplina rilevante in materia di trattamento dei dati personali di cui al D.lgs. 196/2003",* stabilisce che i cittadini, i lavoratori e le imprese abbiano, in ogni caso, *"il diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie informatiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato"* (articolo 2, comma 5).

1.7. Ancora in questo senso, il Garante della privacy, nelle succitate "Linee Guida per la posta elettronica e internet", rileva come "*non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro abbiano prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private"*: questa ULSS n. 6 reputa corretto tale *modus operandi* ed intende farlo proprio, al fine di garantire il maggior grado possibile di autonomia ai propri dipendenti e collaboratori, esercitando, al contempo, un'attività di controllo rispettosa del già citato principio fondamentale di "proporzionalità".

1.8. Questa ULSS intende inoltre uniformarsi alle prescrizioni contenute nella Direttiva n. 2/2009 del Ministero per la pubblica amministrazione e l'innovazione, ad oggetto *"Utilizzo di internet e*

della casella di posta elettronica istituzionale sul luogo di lavoro", nonché alle prescrizioni dettate dal *"Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 165/2001*" approvato con il D.P.R. 16 aprile 2013 n. 62 e dal *"Codice di Comportamento dei dipendenti dell'Azienda ULSS n. 6 Vicenza"* approvato con delibera del Direttore Generale n. 337 del 09.05.2014; per quanto non previsto nel presente Regolamento, si fa quindi rinvio alle diposizioni di cui alle succitate norme.

1.9. Assodato 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'ULSS n. 6 adotta il presente regolamento interno al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.
Le prescrizioni, di seguito stabilite, si aggiungono ed integrano le specifiche istruzioni già fornite, nel corso degli anni, a tutti gli incaricati dell'Azienda in attuazione del D.lgs. 30 giugno 2003 n. 196, e del Disciplinare tecnico (Allegato 'B' al citato decreto legislativo) contenente le misure minime di sicurezza.

1.10. I dipendenti e i collaboratori dell'ULSS n. 6 possono, inoltre, prendere visione delle principali normative in materia di privacy e di misure di sicurezza, nonché di alcuni provvedimenti del Garante della privacy, sull'*intranet* aziendale alla voce "privacy".

1.11. Considerato, infine, che l'Azienda ULSS 6, nell'ottica di uno svolgimento più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti *(computer portatili, tablets, telefoni cellulari, smartphone, etc*.), sono state inserite nel regolamento alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di detta strumentazione.

CAPITOLO II): OGGETTO DEL REGOLAMENTO

2.1. Il presente Regolamento, adottato tenendo conto del vigente quadro normativo e delle indicazioni espresse dal Garante della privacy nei provvedimenti citati al capitolo precedente, ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio internet e di posta elettronica e dei sistemi informatici in generale dell'Azienda ULSS da parte dei dipendenti dell'ULSS n. 6 'Vicenza' e di tutti gli altri soggetti che, a vario titolo, prestano servizio o attività per conto e nelle strutture dell'Azienda (a titolo esemplificativo: borsisti, tirocinanti, collaboratori, liberi professionisti, specializzandi, stagisti, ecc..), oltre che da parte dei dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'ULSS 6, nella misura in cui le disposizioni di cui si tratta siano ad essi applicabili.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, specializzando, consulente, ecc.) in possesso di specifiche credenziali di autenticazione.

CAPITOLO III): DEFINIZIONI

Utente è la persona autorizzata ad accedere alla rete aziendale, ad internet e alla posta elettronica.

Incaricato del trattamento è la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Responsabili del trattamento sono le figure formalmente individuate come tali dal Direttore Generale dell'Azienda e preposte al trattamento di dati personali

E-mail indica la funzione di posta elettronica per lo scambio di messaggio e di documenti.

Personal Computer è la postazione di lavoro fissa o mobile.

Download (in italiano scaricamento) è l'azione di ricevere o prelevare dalla rete un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente.

Upload (in italiano, caricamento) è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica.

Freeware è un software che viene distribuito in modo gratuito.

Shareware è un software che può essere liberamente ridistribuito, e può essere utilizzato per un periodo di tempo di prova variabile scaduto il quale per continuare ad utilizzare il software è necessario registrarlo presso la casa produttrice, pagandone l'importo.

Guestbook è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti.

Bacheca elettronica è un'utilità interattiva dove è possibile reperire annunci di vario genere.

Postazione di lavoro è il personal computer collegato alla rete aziendale tramite il quale l'utente accede ai servizi;

Utente internet è la persona autorizzata ad accedere al servizio internet con l'esclusione dei siti previsti nella black-list;

Utente di posta elettronica è la persona autorizzata ad accedere al servizio di posta elettronica;

Black list è l'elenco di siti non accessibili da nessun utente;

Internet provider è l'azienda che fornisce all'ULSS di Vicenza il canale di accesso alla rete internet;

Log è l'archivio delle attività di consultazione in rete.

CAPITOLO IV): UTILIZZO DEL PERSONAL COMPUTER

4.1. Il personal computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività istituzionale è vietato; l'utilizzo improprio, inoltre, può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

4.2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda ULSS 6 solo attraverso specifiche credenziali di autenticazione, come meglio descritto al successivo capitolo quinto del presente Regolamento.

4.3. Il personale incaricato, anche dei servizi esternalizzati, che opera presso il servizio per l'informatica Generale e l'Ingegneria Clinica dell'Azienda, è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso,

nonché per motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 9.2 e 10.1, potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascun operatore, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui 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.

4.4. Il personale incaricato del Servizio per l'informatica Generale e l'Ingegneria Clinica e dei servizi affidati in *outsourcing* ha la facoltà di collegarsi e visualizzare in remoto, previa comunicazione all'interessato, 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. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. 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.

4.5. Non è consentito il collegamento mediante dispositivi non aziendali alla rete aziendale salvo specifica richiesta da parte del responsabile del trattamento e conferma da parte del servizio per l'informatica Generale e l'Ingegneria Clinica. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio medesimo per conto dell'Azienda ULSS 6, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software aziendali esistenti.

4.6. Salvo preventiva espressa autorizzazione del personale del Servizio per l'informatica Generale, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, memory pen, etc.…).

4.7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio per l'informatica nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo capitolo undicesimo del presente Regolamento relativo alle procedure di protezione antivirus.

4.8. II 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, salvo indicazioni contrarie da parte dei responsabili del servizio stesso o del servizio per l'informatica Generale e l'Ingegneria Clinica. Lasciare un elaboratore incustodito e connesso alla rete, può determinare l'utilizzo indebito da parte di soggetti non autorizzati con conseguente trattamento non autorizzato di dati.

4.9. Con regolare periodicità (almeno ogni tre mesi), è opportuno che ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo necessario evitare un'archiviazione ridondante.

CAPITOLO V): GESTIONE e ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

5.1. Le credenziali di autenticazione per l'accesso ai sistemi e alle procedure aziendali vengono assegnate dal personale del Servizio per l'informatica Generale e l'Ingegneria Clinica o da altro personale appositamente incaricato, previa formale richiesta del Responsabile dell'unità operativa nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile della unità

operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico. Lo stesso dicasi nel caso di revoca e/o trasferimento.

5.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal personale del Servizio per l'informatica Generale e l'Ingegneria Clinica o da altro personale appositamente incaricato, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

5.3. 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.

5.4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, ogni tre mesi.

5.5. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il Responsabile dell'unità operativa dovrà richiedere una nuova password di accesso al Servizio per l'informatica Generale e l'Ingegneria Clinica.

5.6. L'utente, preso atto che la conoscenza della password da parte di terzi consente agli stessi l'accesso ai sistemi e alle procedure aziendali, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (ad esempio, visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi) si impegna a:

- ✓ non concedere, una volta superata la fase di autenticazione, l'uso della propria postazione a personale non autorizzato;
- ✓ non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione (ad esempio, attivando il blocco schermo, digitando Ctrl+Alt+Canc, Blocca computer);
- ✓ conservare la password nella massima riservatezza e con la massima diligenza;
- ✓ non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o se pervenute casualmente a conoscenza;
- ✓ mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né istallando ulteriori software non autorizzati;
- ✓ non salvare file audio, video e file non istituzionali di qualsiasi tipo nei sistemi e nelle procedure aziendali su cui viene eseguito giornalmente il back-up
- ✓ eseguire periodicamente i salvataggi e le copie di sicurezza dei dati del proprio p.c.

5.7. La modulistica da utilizzarsi per la richiesta di assegnazione delle credenziali di autenticazione e di utilizzo degli applicativi informatici è disponibile nell'*intranet* aziendale.

CAPITOLO VI): UTILIZZO DELLA RETE DELL'AZIENDA U.L.SS. N. 6

6.1. Per l'accesso alla rete dell'Azienda ULSS 6 ciascun utente deve essere in possesso della specifica credenziale di dominio.

6.2. È proibito entrare nella rete e nei programmi con una credenziale di dominio diversa da quella assegnata.

6.3. Le cartelle utenti presenti nei server dell'Azienda ULSS 6 sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi, in particolare per contenere e condividere dati sensibili.

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 Servizio per l'informatica.

6.4. Il personale del Servizio per l'informatica Generale e l'Ingegneria Clinica può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza delle postazioni di lavoro.

6.5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.6 La rete aziendale di tipo WI-FI è utilizzata esclusivamente con applicazioni aziendali certificate e con dispositivi aziendali appositamente forniti e configurati dall'Azienda.

CAPITOLO VII): UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

7.1. Tutti i supporti magnetici rimovibili forniti dall'Azienda ULSS 6 (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e sensibili nonché informazioni costituenti patrimonio aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili aziendali contenenti dati personali e sensibili, ciascun utente dovrà essere autorizzato dal proprio responsabile di unità operativa e contattare il personale del Servizio per l'informatica Generale e seguire le istruzioni da questo ultimo impartite.

7.3. In ogni caso, i supporti magnetici contenenti dati personali e sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

CAPITOLO VIII): USO DELLA POSTA ELETTRONICA

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

8.2. È fatto divieto di utilizzare le caselle di posta elettronica nome.cognome@ulssvicenza.it per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo capitolo decimo.
In questo senso, a titolo esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, è necessario darne immediata comunicazione al personale del Servizio per

l'informatica Generale. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La conservazione on line è garantita per 24 mesi.

8.4. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di unità operativa, a seconda del loro contenuto e dei destinatari delle stesse. Sono state attivate caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea. L'indirizzo istituzionale per la PEC dell'ULSS n. 6 è il seguente: protocollo.centrale.ulssvicenza@pecveneto.it

8.5. È obbligatorio porre la massima attenzione nell'aprire i *file attachements* di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o Ftp non conosciuti).

8.6. Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura / servizio. In tal caso, la funzionalità deve essere attivata dall'utente.

8.7. Sarà comunque consentito al superiore gerarchico dell'utente accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.6 o assenza non programmata).

8.8. Il personale del Servizio per l'informatica Generale e l'Ingegneria Clinica o altro personale esterno a ciò incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 4.4.

8.9. Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un riferimento alla struttura di appartenenza di colui che invia la comunicazione, nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dell'Azienda ULSS 6 potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nei punti precedenti.

8.10. Non è autorizzato l'utilizzo per fini istituzionali di indirizzi e-mail personali privati al di fuori del dominio aziendale *@ulssvicenza.it*

CAPITOLO IX): NAVIGAZIONE IN INTERNET

9.1. 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 proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa, salvo le indicazioni presenti nel successivo capitolo decimo.

9.2. In questo senso, a titolo puramente esemplificativo, 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 (filmati e musica);
- 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 di unità operativa.

L'accesso, tramite internet, a caselle webmail di posta elettronica personale è consentito solo nel rispetto di quanto riportato al capitolo decimo.

9.3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda ULSS 6 adotta uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una “black list”. L'azienda si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa e compatibili con le finalità non istituzionali di cui al successivo capitolo decimo.

9.4. Gli eventuali controlli, compiuti dal personale incaricato del Servizio per l'informatica Generale e l’Ingegneria Clinica, ai sensi del precedente punto 4.4, potranno avvenire mediante un sistema di controllo dei contenuti (Web Filtering) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

9.5 L’utilizzo e la consultazione di social network sono permessi esclusivamente per finalità istituzionali e previa autorizzazione del Dirigente responsabile della unità operativa.

9.6 I contenuti e la gestione informativa del sito web aziendale (www.ulssvicenza.it) e della relativa intranet aziendale sono di competenza dell’Ufficio per le Relazioni con il Pubblico (URP).

CAPITOLO X): REGOLAMENTAZIONE USO INTERNET PER FINALITÀ NON ISTITUZIONALI

10.1. E’ consentita, previa autorizzazione del Dirigente responsabile della struttura, la consultazione occasionale di siti internet per finalità non istituzionali e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano compatibili con le misure di sicurezza implementate a protezione del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi di servizio che il dipendente ha nei confronti dell'Ente.

CAPITOLO XI): PROTEZIONE ANTIVIRUS

11.1. Il sistema informatico dell'Azienda ULSS n. 6 è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software di tipo malware

11.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio per l'informatica Generale.

11.3. Ogni dispositivo di supporto di memorizzazione elettronico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio per l'Informatica Generale e l’Ingegneria Clinica.

11.4 L’utente utilizzatore del personal computer verifica periodicamente lo stato di aggiornamento dell’antivirus aziendale installato. A fronte di eventuali anomalie contatta il Servizio per l'Informatica Generale e l’Ingegneria Clinica.

CAPITOLO XII): UTILIZZO DI TELEFONI, FAX, SCANNER E FOTOCOPIATRICI

12.1. Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.
Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l'addebito delle chiamate personali.
12.2. È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa autorizzazione da parte del Responsabile dell’unità operativa.
12.3. È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell’unità operativa.
12.4. È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell’unità operativa.
12.5. Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Responsabile della unità operativa a cui detti strumenti sono stati assegnati.
12.6. L’utilizzo del telefono o di altro strumento di comunicazione personale in orario di servizio deve essere limitato ai casi di urgenza ed indifferibilità, che non consentono di effettuare la comunicazione dopo la fine dell’orario di lavoro.

CAPITOLO XIII): UTILIZZO DI SMARTPHONE / TABLET E RELATIVE APPLICAZIONI MOBILI “APP”

13.1. Premesso che i terminali di nuova generazione applicati alla telefonia mobile (smartphone e tablet) e le relative applicazioni mobili software (note comunemente con l'abbreviazione “*App*”), sono in fase di evoluzione costante e consentono, con crescente facilità, di utilizzare, registrare e trasmettere dati sensibili tramite diverse tecnologie di rete, quali *Gprs, Edge o Umts,* comunicando e diffondendo in rete dati e immagini in tempo reale, si fa presente che si tratta di apparecchiature che, per le loro potenzialità, possono essere utilizzate violando, anche involontariamente, i diritti delle persone interessate alla comunicazione, come pure di terzi inconsapevoli.

Premesso ciò si definiscono per i casi seguenti le regole:

CASO 1 - Smartphone/Tablet aziendale in cui è richiesta l’installazione di una applicazione aziendale che gestisce dati sensibili: in questo caso l’autorizzazione per l’installazione è permessa solo se i dispositivi Smartphone/Tablet sono supportati da un apposito sistema di sicurezza aziendale (Sistema MDM - *Mobile Device Management*) .

CASO 2 - Smartphone/Tablet aziendale in cui è richiesta l’installazione di una applicazione mobile App (aziendale) che gestisce dati sensibili: è autorizzata in questo caso l’installazione di App

(aziendali) che gestiscono dati sensibili esclusivamente se tali App sono certificate come Dispositivi Medici secondo le norme e le direttive in vigore sui DM. Inoltre l'autorizzazione di installazione è permessa solo se i dispositivi Smartphone/Tablet sono supportati da un apposito sistema di sicurezza aziendale (Sistema MDM - *Mobile Device Management*) .

CASO 3 - Smartphone/Tablet aziendale non aziendali (personali) in cui è richiesta l'installazione o di una applicazione aziendale o di una applicazione mobile App che gestiscono dati sensibili: in questo caso non sono ammesse installazioni di applicazioni e/o App aziendali di nessun tipo.

CAPITOLO XIV): CONTROLLI

14.1. L'articolo 23 del recente D.lgs. 14 settembre 2015 n. 151 (così detto *"Decreto sulle semplificazioni"* attuativo della Legge delega 10.12.2014 n. 183, anche nota come *"legge di riforma del diritto del lavoro"* o *"Jobs Act"*) ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato *"Impianti audiovisivi e altri strumenti di controllo".*

14.2. Il testo del nuovo articolo 4 della Legge 300/1970, nel confermare, al primo comma, la disciplina applicabile agli strumenti di controllo a distanza dell'attività dei lavoratori necessari per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (come le telecamere o i rilevatori di posizione Gps), che rimangono sottoposti alla stessa disciplina di divieti e di controlli di prima, ha introdotto, al comma due, una disciplina diversa per quanto concerne i dispositivi utilizzati dal lavoratore per rendere la prestazione lavorativa (computer, tablet, telefoni, smartphone) stabilendo espressamente che *"La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte a sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.lgs. 30 giugno 2003 n. 196*

Alla luce delle disposizioni dettate dal succitato D.lgs. 151/2015, questa azienda U.L.SS. può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno effettuarsi i controlli.

14.3. Si dà atto che l'informativa ai lavoratori, di cui al precedente capoverso, viene garantita da questa Azienda U.L.SS. mediante la diffusione del presente Regolamento, approvato con delibera del Direttore Generale, nelle forme previste dal capitolo XIX *("Entrata in vigore e pubblicità")*, e che le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro nel rispetto di quanto previsto dal "Codice della privacy" (D.lgs. 196/2003).

CAPITOLO XV): GRADUAZIONE DEI CONTROLLI

15.1. Premesso che *"il dipendente deve utilizzare il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione"* (art. 11, Codice di comportamento dei dipendenti pubblici e Codice di Comportamento dei dipendenti dell'Azienda ULSS n. 6), come stabilito dal Garante della privacy nelle già citate "Linee guida per posta elettronica e internet" del 01.03.2007, all'articolo 6.1. rubricato "Graduazione", nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

15.2. Come stabilito altresì' dalla già citata Direttiva n. 2/2009 ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", l'eventuale controllo è lecito solo se sono rispettati i principi di proporzionalità, pertinenza e non eccedenza nelle attività di controllo.
Le limitazioni della libertà e dei diritti individuali devono essere proporzionate allo scopo perseguito ed è, in ogni caso, esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati.

15.4. Per quanto possibile deve essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

15.5. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.
L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

CAPITOLO XVI): UTILIZZO DI SOCIAL NETWORKS

16.1. E' vietato l'utilizzo di social networks per la promozione dell'immagine e dell'attività aziendale, salva espressa autorizzazione da parte della Direzione Generale.

16.2. Al fine di assicurare il rispetto del segreto d'ufficio, del segreto professionale e della riservatezza dei dati conosciuti in ambito aziendale, è vietato l'uso, anche privato, dei social networks per lo scambio di informazioni e dati inerenti l'attività istituzionale.

CAPITOLO XVII): CONSERVAZIONE

17.1. I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla.

17.2. Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ✓ ad esigenze tecniche o di sicurezza del tutto particolari;
- ✓ all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede
- ✓ giudiziaria;
- ✓ all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

17.3. In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate e dev'essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

CAPITOLO XVIII): NON OSSERVANZA DEL REGOLAMENTO

18.1. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con azioni civili e penali e fatto salvo in ogni caso il diritto dell'Azienda al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.

CAPITOLO XIX): ENTRATA IN VIGORE E PUBBLICITÀ

19.1. Il presente Regolamento entrerà in vigore dalla data di adozione dell'atto deliberativo di approvazione.

19.2. Del presente Regolamento viene fornita massima pubblicità e diffusione mediante la sua pubblicazione nel sito internet aziendale, nell'I*'intranet* aziendale e nell'A*ngolo del dipendente* e mediante la sua trasmissione, tramite e-mail, a tutti i dipendenti e collaboratori utilizzando il sistema aziendale di comunicazione / avviso a "everyone".

CAPITOLO XX): DISPOSIZIONI FINALI

20.1. E' obbligatorio attenersi alle disposizioni in materia di privacy. Per quanto non espressamente richiamato nel presente regolamento, si rinvia alle disposizioni civili e penali vigenti in materia.

***