ORIGINALE

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 515 del 12/08/2019

Il Direttore Generale dell'Azienda U.L.S.S. n. 9 SCALIGERA, dott. Pietro Girardi, nominato con D.P.G.R.V. n. 196 del 30/12/2015 e confermato con D.P.G.R.V. n. 164 del 30/12/2016, coadiuvato dai Direttori:

- dott. Giuseppe Cenci Direttore Amministrativo
- dott. Roberto Borin Direttore Sanitario f.f.
- dott. Raffaele Grottola Direttore dei Servizi Socio-Sanitari

ha adottato in data odierna la presente deliberazione:

OGGETTO

APPROVAZIONE REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI DELL'ULSS 9 SCALIGERA

Note per la trasparenza:Regolamento Aziendale per l'utilizzo del Sistema Informatico Aziendale

Il Proponente: per il Direttore UOC Servizi Tecnici e Patrimoniali F.TO ing. Fiorenzo Panziera

DELIBERAZIONE DEL DIRETTORE GENERALE N. 515 DEL 12/08/2019

Il Direttore dell'UOC Servizi Tecnici e Patrimoniali ing. Corrado Salfa, sostituito dall'ing. Fiorenzo Panziera (giusta deliberazione n. 529 del 2 agosto 2018), vista la relazione del Direttore U.O.S. Sistemi Informativi ing. Andrea Oliani riferita all'oggetto:

"Premesso che:

- la realtà aziendale dell'ULSS 9 Scaligera si caratterizza per l'elevato uso della tecnologia informatica che, da un lato, ha consentito l'introduzione di innovative tecniche di gestione e, dall'altro, richiede inevitabilmente la gestione di numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda al dipendente per lo svolgimento delle proprie mansioni;
- vi è quindi la necessità di porre in essere adeguati sistemi di gestione e controllo dell'utilizzo di tali strumenti da parte degli utilizzatori autorizzati dall'Azienda, e di prevenire potenziali usi scorretti che, oltre ad esporre l'Azienda a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt.2104 e 2105 del codice civile e dall'Art. 23 del CCNL, oltre che principi del vigente Codice della Privacy (Regolamento Ue 2016/679 o GDPR);
- i controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei Lavoratori e dal D. Lgs 196/03 sulla tutela dei dati personali.

Considerato che:
1. il Regolamento sull'utilizzo del Sistema Informatico Aziendale dell'ULSS 9 Scaligera, allegato come parte integrante del presente provvedimento, viene incontro alle esigenze espresse in premessa, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e telematici da parte dei dipendenti, nel rispetto degli obblighi normativi succitati;

2. i principi applicati nella stesura del presente Regolamento sono tratti dal quadro normativo che segue:

- Costituzione, Art. 15 (Libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione);
- Norme del codice civile: artt. 2087, 2104, 2105 e 2106;
- L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) - artt. 4 e 8;
- Codice in materia di protezione dei dati personali (Regolamento (Ue) 2016/679, D. Lgs. n. 196/2003 e Decreto Legislativo 10 agosto 2018, n. 101);

- Art. 49, D.Lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, "Segretezza della corrispondenza trasmessa per via telematica";
- disposizioni di cui all'art. 47 del D.Lgs. 82/2005 succitato, modificato dal D.L. n.69/2013, convertito con modificazioni con la L. n. 98/2013, che ha definitivamente escluso la trasmissione di documenti a mezzo fax tra le pubbliche amministrazioni;
- "Linee guida del Garante per posta elettronica e Internet", emanate con deliberazione 1 marzo 2007 n. 13.
- Direttiva n. 2 del 25 maggio 2009 della Presidenza del Consiglio dei Ministri - Dipartimento della Funzione Pubblica "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

Precisato che il nuovo Regolamento entrerà in vigore dalla data di adozione del presente provvedimento";

Propone l'adozione del provvedimento sotto riportato.

IL DIRETTORE GENERALE

Vista l'attestazione del Responsabile dell'avvenuta regolare istruttoria della pratica in relazione sia alla sua compatibilità con la vigente legislazione nazionale e regionale, sia alla sua conformità alle direttive e regolamentazione aziendali;

Acquisito agli atti il parere favorevole del Direttore Sanitario, del Direttore Amministrativo e del Direttore dei Servizi Socio-Sanitari per quanto di rispettiva competenza;

DELIBERA

1. di approvare, per le motivazioni indicate in premessa, l'allegato "REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI dell'ULSS 9 Scaligera", che costituisce parte integrante del presente provvedimento;

2. di dare atto che il Regolamento entrerà in vigore dalla data di adozione del presente provvedimento;

3. di dare pubblicità al "Regolamento aziendale per l'utilizzo del Sistema Informatico Aziendale" mediante pubblicazione nell'apposita sezione dell'Amministrazione

DELIBERAZIONE DEL DIRETTORE GENERALE N. 515 DEL 12/08/2019

Trasparente dedicata ai Regolamenti on line raggiungibili anche dalla home page del sito aziendale.

Il Direttore Sanitario f.f.	Il Direttore Amministrativo	Il Direttore dei Servizi Socio Sanitari
F.TO dott. Roberto Borin	F.TO dott. Giuseppe Cenci	F.TO dott. Raffaele Grottola

IL DIRETTORE GENERALE
F.TO dott. Pietro Girardi

Il Proponente: per il Direttore UOC Servizi Tecnici e Patrimoniali F.TO ing. Fiorenzo Panziera

DELIBERAZIONE DEL DIRETTORE GENERALE N. 515 DEL 12/08/2019

ATTESTAZIONE DI PUBBLICAZIONE E DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva dalla data di adozione.

In data odierna copia della presente deliberazione viene:

- Pubblicata per 15 giorni consecutivi nell'Albo on line, ai sensi e per gli effetti dell'art. 32 – comma 1 – della L. 18.06.2009, n. 69 e s.m.i..
- Trasmessa al Collegio Sindacale, ai sensi dell'art. 10 – comma 5 – della L.R. 14.09.1994, n. 56.

Verona, 30/08/2019

P. il Direttore
UOC Affari Generali
F.TO Sig.ra. Margherita Gagliardi

TRASMESSA PER L'ESECUZIONE A:

UOC SERVIZI TECNICI E PATRIMONIALI

TRASMESSA PER CONOSCENZA A:

UOS Sistemi Informativi

Il Proponente: per il Direttore UOC Servizi Tecnici e Patrimoniali F.TO ing. Fiorenzo Panziera

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

INDICE

1. SCOPO.....2

1.1 Elementi costitutivi risorse informatiche.....2

2. CAMPO DI APPLICAZIONE.....2

2.1 Definizione utenti interni e esterni.....2

3. RESPONSABILITA'.....2

4. CONTENUTO.....3

4.1 Utilizzo del personal computer.....3

4.2 Utilizzo della rete dell'Ulss 9 Scaligera.....4

4.3 Modalità di accesso alla rete e ai servizi /programmi utenti interni.....4

4.4 Modalità di accesso alla rete e ai servizi 7 programmi utenti esterni.....5

4.5 Gestione della password.....5

4.6 Utilizzo dei supporti magnetici.....5

4.7 Utilizzo di PC portatili.....6

4.8 Utilizzo delle stampanti e dei materiali di consumo.....6

4.9 Utilizzo della posta elettronica.....6

4.10 Utilizzo della rete internet e dei relativi servizi.....7

4.11 Protezione antivirus.....8

4.12 Teleassistenza.....9

4.13 Controlli.....9

4.14 Non osservanza della normativa aziendale.....10

4.15 Informativa ai sensi dell'art. 13 del D.Lgs. 196/2003.....10

Rev.	Descrizione delle modifiche	Data
01	Prima emissione	01/07/2019

Redatto da: Servizio Sistemi Informativi: Gianfranco Belgiovine	01/07/2019

Verificato da: Servizio Sistemi Informativi: Ing. Andrea Oliani	01/07/2019
Approvata da: Direttore Generale: Dott. Pietro Girardi	

1. SCOPO

Il presente regolamento ha lo scopo di disciplinare le modalità di accesso e di uso della rete Informatica dell'ULSS 9 Scaligera e dei servizi che, tramite la stessa Rete, è possibile ricevere o offrire all'interno e all'esterno dell'Amministrazione.

1.1 Elementi costitutivi Risorse informatiche.

In particolare si specifica che la Rete dell'ULSS 9 Scaligera è costituita dall'insieme delle Risorse informatiche, cioè dalle Risorse infrastrutturali e dal Patrimonio informativo digitale.

- ☐ Le Risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla Rete Informatica aziendale.
- ☐ Il Patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

2. CAMPO DI APPLICAZIONE

Il presente regolamento si applica a tutti gli utenti Interni ed Esterni che sono autorizzati ad accedere alla Rete aziendale.

2.1 Definizione utenti interni e esterni.

- ☐ Per utenti Interni si intendono tutti gli Amministratori, i Dirigenti, i dipendenti a tempo indeterminato e a tempo determinato ed il personale convenzionato.
- ☐ Per utenti Esterni si intendono: le ditte fornitrici di hardware e software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, collaboratori esterni.

3. RESPONSABILITA'

Ogni utente è responsabile civilmente e penalmente del corretto uso delle Risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. L'assegnazione della Risorsa informatica non ne comporta il possesso, in quanto trattasi di strumento di esclusiva proprietà aziendale. L'utente utilizza, per il proprio lavoro, soltanto computer assegnatigli dall'Azienda ULSS 9. L'uso di computer privati deve essere preventivamente autorizzato dal Direttore dell'UOS Servizio Sistemi Informativi. Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella Rete Informatica è sottoposta a registrazione in appositi file e riconducibili ad un account utente e pc client. Detti files possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003 e S.M.I.

E' responsabilità del Dirigente di U.O. verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.

4. CONTENUTO

4.1 Utilizzo del personal computer

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo improprio può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

- ☐ L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen saver .
- ☐ Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Direttore dell'UOS Servizio Sistemi Informativi. Il Direttore dell'UO6 Servizio Sistemi Informativi e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate e tipicamente per attività di manutenzione, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, in relazione agli scopi di volta in volta identificati, garantendo comunque la riservatezza delle informazioni.
- ☐ Non è consentito installare autonomamente programmi provenienti dall'esterno. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree ed i relativi dirigenti, deve essere comunque richiesta per iscritto l'autorizzazione preventiva da parte del Direttore dell'UOS Servizio Sistemi informativi, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.
- ☐ Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'ULSS 9 Scaligera (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).
- ☐ Non è consentito all'utente modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita del Direttore dell'UOS Servizio Sistemi Informativi.
- ☐ Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o almeno una volta a settimana 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. Per tale motivo si richiede all'utente di bloccare la postazione prima di assentarsi (combinazione di tasti WINDOWS+L) mentre sarà abilitato centralmente uno screensaver protetto da password dopo 15 minuti di inattività.
- ☐ Non è consentita l'installazione sul proprio personal computer o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili ed apparati in genere …), se non con l'autorizzazione espressa del Direttore dell'UOS Servizio Sistemi Informativi, previa richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato il personal computer.

- ☐ Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Servizio Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 13 del presente Regolamento relativo alle procedure di protezione antivirus.
- ☐ Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria
- ☐ per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

4.2 Utilizzo della rete dell'Ulss 9 Scaligera

- ☐ Le unità di rete 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, sono svolte regolari attività di controllo, amministrazione da parte del personale dell'UOS Servizio Sistemi Informativi
- ☐ Le condivisioni locali ai pc dovranno essere richieste e approvate dal Direttore dell'UOS Servizio Sistemi Informativi, il quale si occuperà di assegnare le giuste autorizzazione garantendo la riservatezza dei dati.
- ☐ Le password d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' vietato entrare nella rete e nei programmi con nomi utente diversi dal proprio o da quello individuato dal Direttore dell'UOS Servizio Sistemi Informativi .
- ☐ Il personale dell'UOS Servizio Sistemi Informativi può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o non pertinente, sia sui personal computer degli utenti sia sulle unità di rete.
- ☐ Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti da evitare un'archiviazione ridondante.
- ☐ E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio files di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

4.3 Modalità di accesso alla rete e ai servizi/programmi utenti interni.

- ☐ Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che venga presentata al Direttore dell'UOS Servizio Sistemi Informativi, da parte del responsabile della propria Unità Organizzativa una richiesta scritta, con firma anche dell'interessato, per l'utilizzo della Rete Informatica aziendale, per l'uso della posta elettronica e di internet e per l'uso di servizi/programmi specifici.
- ☐ Il Direttore dell'UOS Servizio Sistemi Informativi provvede ad assegnare ad ogni utente un account di rete e un account per ogni servizio/programma autorizzato. Ogni account è costituito dall'accoppiamento di un Codice personale o Username/Smartcard con una Parola chiave o Password. Per ogni servizio/programma vengono abilitate all'utente solo le funzioni per le quali è stato autorizzato. Non sono previsti account anonimi, nel caso di

creazione di profili generici (per es. nome dell'unità) in assenza di diversa indicazione la responsabilità è attribuita al Direttore dell'unità.

- ☐ Non è prevista la creazione di account per le borse di studio o per altro personale non definito al punto 2.1.

4.4 Modalità di accesso alla rete e ai servizi/programmi utenti esterni.

- ☐ Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti Esterni presentino richiesta scritta e motivata, preventivamente autorizzata dal Direttore dell'Unità Organizzativa presso cui devono svolgere il servizio, al Direttore dell'UOS Servizio Sistemi Informativi.
- ☐ Il Direttore dell'UOS Servizio Sistemi Informativi provvede alla creazione di un account per l'accesso alla rete con i privilegi minimi necessari per l'attività che deve essere svolta.

4.5 Gestione della password

- ☐ L'accesso alla Rete Informatica dell'ente, nonché l'accesso ai programmi è protetto da password. Username e Password sono strettamente personali; la loro tutela è a carico dell'utente. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico. Ai fini dell'assistenza sistemistica, la password di accesso può venire comunicata agli operatori tecnici chiamati ad intervenire i quali ne assicurano la riservatezza e la tutela, indicando all'utente di provvedere immediatamente, dopo l'intervento, alla sua sostituzione.
- ☐ La password deve essere lunga almeno 8 caratteri, non deve avere riferimenti diretti con dati personali dell'utente (data di nascita, nome, cognome, nome dei figli, ecc.) o ad esso facilmente riconducibili, deve essere alfanumerica e contenere almeno 2 numeri.
- ☐ Le password utilizzate hanno una durata massima di tre mesi, trascorsi i quali le password devono essere sostituite.
- ☐ La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
- ☐ Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'interessato al fine che quest'ultimo provveda alla sostituzione.
- ☐ E' dato incarico ai Dirigenti di comunicare tempestivamente per iscritto al Direttore dell'UOS Servizio Sistemi Informativi eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

4.6 Utilizzo dei supporti magnetici

- ☐ Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, cd-rom, dvd, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
- ☐ I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

- ☐ I supporti magnetici utilizzati e non più fruibili per qualsiasi motivo, devono essere distrutti fisicamente.
- ☐ Non è consentito importare sulla stazione di lavoro aziendale, o su risorse dell'Azienda, files non aventi alcuna attinenza con la propria prestazione lavorativa.
- ☐ Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo da parte del personale dell'UOS Servizio Sistemi Informativi.

4.7 Utilizzo di PC portatili

- ☐ L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nella UO di lavoro.
- ☐ Se i PC portatili sono condivisi da più persone, sarà compito del responsabile dell'UO vigilare che il PC sia usato in modo appropriato.
- ☐ Ai PC portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
- ☐ I PC portatili utilizzati all'esterno (convegni, corsi etc.), in caso di allontanamento, devono essere custoditi in un posto protetto.

4.8 Utilizzo delle stampanti e dei materiali di consumo

- ☐ L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come cd-rom e dvd) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
- ☐ Non è consentito lasciare incustoditi presso le stampanti documenti cartacei contenenti dati sensibili o riservati.

4.9 Utilizzo della posta elettronica

- ☐ Sono attivati indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse (es.: ufficio.informatico@aulss9.veneto.it). Al singolo utente interno può essere assegnato un indirizzo e-mail personale del tipo: nome.cognome@aulss9.veneto.it. La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.
- ☐ 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. Si rammenta che i normali sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, gli utenti non devono inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.
- ☐ Non deve essere trasmesso a mezzo Posta Elettronica materiale pedofilo/pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno. Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.

- ☐ Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) dovrà essere accluso il seguente testo: " Qualora questo messaggio fosse da Voi ricevuto per errore, vogliate cortesemente darcene notizia a mezzo fax (od e-mail) e distruggere il messaggio ricevuto erroneamente. Si invita ad astenersi dall'effettuare inoltri, copie, distruzioni e divulgazioni non autorizzate del presente messaggio e degli eventuali allegati. Quanto precede ai fini del rispetto della Legge 196/2003 sulla tutela dei dati personali!".
- ☐ Non si devono utilizzare le caselle di posta elettronica ……@aulss9.veneto.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente. Viene ammesso invece l'utilizzo, al di fuori dell'orario di servizio, della mail aziendale per attività inerenti alle relazioni sindacali e all'attività legate ai circoli aziendali che rimangano nell'ambito dell'ULSS 9.
- ☐ La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.
- ☐ Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'ULSS 9 Scaligera ovvero contenga documenti da considerarsi riservati, deve essere visionata ed autorizzata dal Dirigente cui si riferisce l'attività ed indirizzata ad una casella di posta certificata.
- ☐ E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi della posta elettronica certificata.
- ☐ Per la trasmissione di file all'interno dell'ULSS 9 Scaligera è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
- ☐ Non aprire od eseguire files allegati alla posta elettronica se non si è certi del mittente e del loro contenuto.
- ☐ Non si devono inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Direttore dell'UOS Servizio Sistemi Informativi. Non si deve in alcun caso attivare gli allegati di tali messaggi.
- ☐ E' severamente vietato eseguire o favorire pratiche di spamming.
- ☐ Ciascun operatore può, anche da postazioni esterne all'azienda, utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e funzioni di inoltro automatico dei messaggi ricevuti verso indirizzi di altro personale dipendente.
- ☐ Nel caso in cui un dipendente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, un fiduciario, da lui preventivamente nominato, o, in sua assenza, il Direttore della U.O., potrà accedere alla casella di posta al fine di garantire la continuità dell'attività lavorativa. La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e consegnata al responsabile dell'U.O..
- ☐ Per la gestione della password della posta elettronica si rimanda al punto 4.5

4.10 Utilizzo della rete internet e dei relativi servizi

- ☐ Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' consentito l'uso

dell'accesso ad internet anche per motivi personali purché tale utilizzo sia occasionale, limitato nel tempo, confinato all'esterno dell'orario di lavoro, non pregiudizievole dell'uso dei sistemi da parte degli altri utenti né della efficienza ed efficacia della prestazione lavorativa, né della sicurezza del sistema informativo aziendale e comunque per finalità lecite.

- ☐ Data la vasta gamma di attività aziendali, non è definito a priori un elenco di siti aziendali autorizzati; potranno comunque essere utilizzati appositi strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie e/o singoli siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività aziendali. Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.
- ☐ Non è consentito all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet.
- ☐ Non è permessa, all'interno dell'orario di lavoro, l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
- ☐ Non è permessa, tramite la rete aziendale, la registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- ☐ Non è permessa, tramite la rete aziendale, 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 attinenti l'attività lavorativa svolta.
- ☐ Il Direttore dell'UOS Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
- ☐ Non è consentito visitare siti e/o memorizzare documenti informatici dai contenuti di natura pedofilo/pornografica, fraudolenta/illegale, riguardante il gioco d'azzardo, blasfema e/o molesta/oscena, oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i P.C. aziendali hanno visitato. L'accesso a questi dati è effettuato dal personale della UOS Servizio Sistemi Informativi ed eventualmente da personale tecnico esterno autorizzato dalla direzione della UOS Servizio Sistemi Informativi.
I sistemi software sono programmati e configurati in modo da cancellare semestralmente i dati relativi agli accessi ad Internet ed al traffico telematico.
L'eventuale prolungamento dei suddetti tempi di conservazione é eccezionale e può avere solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

4.11 Protezione antivirus

- ☐ Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
- ☐ Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
  - ☐ sospendere ogni elaborazione in corso senza spegnere il computer;
  - ☐ segnalare l'accaduto al personale dell'UOS Servizio Sistemi Informativi.
- ☐ Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, dvd, nastri magnetici e ogni altro supporto di memorizzazione di provenienza ignota.
- ☐ Ogni dispositivo di memorizzazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al personale dell'UOS Servizio Sistemi Informativi.

4.12 Teleassistenza

- ☐ Relativamente alle attività di manutenzione remota su personal computer connessi alla rete aziendale, il personale tecnico dell'UOS Servizio Sistemi Informativi potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene previo avviso all'utente interessato che può rifiutare tale tipo di assistenza allungando però in questa maniera i tempi d'intervento. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al personal computer.
- ☐ Viene fornita, su richiesta, una comunicazione informativa sullo strumento utilizzato, nonché le modalità del suo utilizzo per tutti gli utenti aziendali interessati.

4.13 Controlli

- ☐ Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:
  - ☐ analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (e-mail, fileaudio, accesso a risorse estranee alle mansioni);
  - ☐ emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
  - ☐ in caso di successivo permanere di una situazione non conforme, é possibile effettuare controlli circoscritti su singole postazioni di lavoro.
- ☐ Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:
  - ☐ analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
  - ☐ emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti

assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;

- ☐ in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

4.14 Non osservanza della normativa aziendale

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni che possono essere comminate e ulteriori conseguenze di natura penale, civile e amministrativa.

4.15 Informativa ai sensi dell'art. 13 del D.Lgs. 196/2003

Il Titolare del trattamento dei dati personali della presente direttiva è l'Azienda ULSS 9 Scaligera.

I Responsabili del trattamento dei dati personali sono stati nominati dal Direttore Generale AULSS 9, e pubblicati sul portale Aziendale.

I diritti previsti dall'art. 7 D.Lgs. 196/2003 e in particolare il diritto di conoscere i dati che riguardano l'utente, il diritto di aggiornarli e il diritto di cancellare i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi al Responsabile dei trattamenti, oppure al Titolare.