Azienda U L S S n. 2
Marca trevigiana
Sede Legale via Sant'Ambrogio di Fiera, 37 31100 Treviso

DELIBERAZIONE DEL DIRETTORE GENERALE

28/06/2018, n. 1119

Il Direttore generale di questa Azienda U.L.S.S. dott. Francesco Benazzi, nominato con D.P.G.R. 30 dicembre 2015 n. 191, integrato con D.P.G.R. 30 dicembre 2016 n. 157, coadiuvato da:

Direttore amministrativo	- Dott.ssa Annamaria Tomasella
Direttore sanitario F.F.	- Dott. Stefano Formentini
Direttore dei servizi socio-sanitari F.F.	- Dott. Gerardo Favaretto

ha adottato la seguente deliberazione:

OGGETTO

REGOLAMENTO CONCERNENTE L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI: APPROVAZIONE.

OGGETTO: REGOLAMENTO CONCERNENTE L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI: APPROVAZIONE.

Il Dirigente incaricato dell'U.O.C. Affari Generali, responsabile del procedimento, di concerto con il Responsabile incaricato dell'U.O.S.D. Sistemi Informativi, verificata la compatibilità con le norme nazionali, regionali e regolamenti vigenti in materia, relaziona al Direttore Generale quanto di seguito riportato:

RITENUTO e considerato in fatto e in diritto quanto segue:

La diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi rendono fondamentale, per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati.

È dovere dell'Azienda individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.

L'elevato uso delle tecnologie informatiche (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) come strumento di lavoro dell'Azienda impone la necessità di regolamentarne l'utilizzo attraverso specifiche disposizioni; ciò al fine di fornire agli utenti dei predetti sistemi informatici un'adeguata informazione circa le modalità da seguire per il corretto uso nello svolgimento dei compiti istituzionali, in modo che possano, contestualmente, collaborare alle politiche di sicurezza messe in atto.

È inoltre necessario porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo interferire nella sfera personale del lavoratore e nel diritto alla riservatezza e alla dignità come sanciti dallo Statuto dei Lavoratori (legge 20.5.1970, n. 300) e dalla normativa in materia di protezione dei dati personali (Codice della privacy – D.Lgs. 30.6.2003, n. 196 e Regolamento (CE) 27.4.2016, n. 2016/679/UE del Parlamento Europeo).

Nella materia in esame il Garante per la protezione dei dati personali è intervenuto con appositi atti, a cui si fa espresso rinvio, tra i quali si richiamano le "Linee guida del Garante per la posta elettronica e Internet" (deliberazione n. 13 del 1.3.2007);

A tal fine la proposta di Regolamento in oggetto:
- si conforma alle indicazioni fornite dal Garante per la protezione dei dati personali in materia di utilizzo di strumenti informatici e telematici, nonché della posta elettronica e della rete Internet, nel rapporto di lavoro, nonché alle altre disposizioni normative in materia;
- si configura come strumento a tutela dei diritti patrimoniali dell'Azienda ed a garanzia della sicurezza ed integrità del proprio patrimonio informativo;
- si caratterizza come strumento di garanzia a favore di tutti coloro che svolgono un rapporto di lavoro o di servizio a beneficio dell'Azienda, nella misura in cui costituisce un'informativa preventiva, fornita a tutti questi soggetti, circa termini, casi e modalità di verifica del corretto utilizzo degli strumenti informatici e telematici messi a loro disposizione per le attività di lavoro o di servizio;

SI PROPONE sulla base dei presupposti di fatto e delle ragioni giuridiche risultanti dalla relativa istruttoria di approvare il Regolamento concernente l'utilizzo dei sistemi informatici aziendali, nel testo allegato al presente provvedimento per farne parte integrante e sostanziale;

VISTE le Leggi Regionali n. 55 e n. 56 del 14 settembre 1994;

VISTO l'art. 3, comma 6, del D.Lgs. n. 502/1992 e successive modificazioni ed integrazioni;

IL DIRETTORE GENERALE

VISTA la suesposta relazione;

CONDIVISE le motivazioni in essa indicate e fatta propria la proposta del succitato Dirigente proponente;

ACQUISITO il parere favorevole del Direttore Amministrativo, del Direttore Sanitario e del Direttore dei Servizi Socio-Sanitari, per le parti di rispettiva competenza;

DELIBERA

1) di approvare il "Regolamento concernente l'utilizzo dei sistemi informatici aziendali", nel testo allegato al presente provvedimento per farne parte integrante e sostanziale;

2) di dare atto che il Regolamento entra in vigore nel quindicesimo giorno successivo a quello della pubblicazione della presente deliberazione di approvazione nell'Albo on-line istituzionale.

3) di rendere noto a tutti gli utenti dei sistemi informatici aziendali il contenuto del presente Regolamento mediante comunicazione personalizzata nella cosiddetta "Bacheca on-line" inserita nell'Angolo del dipendente – procedura del personale, nonché a mezzo di pubblicazione nell'apposita sezione dell'Amministrazione Trasparente;

4) di dare atto che nessun onere deriva dall'assunzione del presente provvedimento;

5) di dichiarare il presente provvedimento esecutivo dalla data di pubblicazione.

Deliberazione 28/06/2018, n. 1119

Documento firmato elettronicamente secondo la normativa vigente.

Per il parere di competenza:

Il Direttore amministrativo n.ro certificato: 2585B80B2A04F471 Firmatario: Dott.ssa Annamaria Tomasella

Il Direttore sanitario F.F. n.ro certificato: 7E8E16D2DFC6445D Firmatario: Dott. Stefano Formentini

Il Direttore dei servizi socio-sanitari F.F.
n.ro certificato: 7E22F653A4D06F6C Firmatario: Dott. Gerardo Favaretto

Il Direttore Generale
Dott. Francesco Benazzi
n.ro certificato: 0A374A2C08064C79

La presente deliberazione viene:

- affissa all'albo Aziendale per quindici giorni consecutivi da oggi

- inviata in data odierna al Collegio Sindacale

Treviso, 17/07/2018 SERVIZIO AFFARI GENERALI – Il Funzionario

n.ro certificato: 718820ECD3AB7259 Firmatario: Roberta Tallon

---

La presente deliberazione è divenuta esecutiva il 17/07/2018

Treviso, 17/07/2018 SERVIZIO AFFARI GENERALI – Il Funzionario

n.ro certificato: 718820ECD3AB7259 Firmatario: Roberta Tallon

---

La presente deliberazione viene inviata a:

Uffici/Servizi:

U.O.C. Affari Generali
U.O.S.D. Sistemi Informativi

REGIONE DEL VENETO

ULSS2 MARCA TREVIGIANA

REGOLAMENTO CONCERNENTE L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

approvato con deliberazione n. __ del _____

in vigore dal _____

CAPO I – DISPOSIZIONI GENERALI

CAPO II – DISPOSIZIONI PER L'UTILIZZO DEI SISTEMI INFORMATICI

CAPO III – NORME FINALI

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto e principi generali

Le disposizioni del presente Regolamento disciplinano l'utilizzo delle risorse informatiche e telematiche dell'Azienda ULSS n. 2 Marca trevigiana da parti del personale dipendente e degli altri operatori abilitati, tenuto conto delle seguenti finalità e principi:

- l'uso delle tecnologie informatiche e telefoniche, che ha consentito l'introduzione di innovative tecniche di gestione delle attività, ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici e telefonici forniti dall'Azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati;
- le implicazione in termini di sicurezza, disponibilità ed integrità dei sistemi informatici dell'ente;
- prevenire comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei sistemi aziendali e nel trattamento dei dati.
- 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;
- è fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte degli operatori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 1.3.2007) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'Azienda stessa 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;
- i controlli sull'uso degli strumenti informatici e telefonici devono garantire sia il diritto dell'Ente di proteggere la propria organizzazione, essendo i computer, gli applicativi per la gestione delle diverse attività, i telefoni aziendali e gli altri mezzi strumenti di lavoro, la cui utilizzazione personale è preclusa, sia il diritto del lavoratore a non vedere invasa la propria sfera personale, il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003) nonché dal Regolamento europeo in materia (Reg. (CE) 27.4.2016, n. 2016/679/UE);
- informare gli interessati sulle finalità dell'utilizzo degli strumenti informatici, del controllo e sulle specifiche metodologie adottate per effettuarlo;
- sensibilizzare gli interessati al rispetto della normativa sulla tutela legale del software;
- l'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al rispetto da parte degli operatori delle norme civili, penali e amministrative applicabili.

Art. 2 – Campo di applicazione

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 (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, specializzandi, personale universitario, altro) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda.

Art. 3 – Definizioni

Ai fini del presente regolamento si intende per:

a) *Utente*: è la persona autorizzata ad accedere alla rete informatica aziendale, ad internet e alla posta elettronica, agli applicativi aziendali e alle altre risorse informatiche e telematiche a ciò autorizzato;
b) *Autorizzato al trattamento*: è la persona fisica autorizzata a compiere operazioni di trattamento dal titolare;
c) *E-mail*: indica la funzione di posta elettronica per lo scambio di messaggio e di documenti;
d) *Download* (in italiano scaricamento): è l'azione di ricevere o prelevare dalla rete informatica un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente;
e) *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;
f) *Freeware*: è un software che viene distribuito in modo gratuito;
g) S*hareware*: 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;

h) *Ransomware*: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.

Art. 4 – Gestione ed assegnazione delle credenziali di autenticazione

L'abilitazione attraverso le credenziali di autenticazione per l'accesso alla rete informatica viene eseguita dal personale del servizio di assistenza ai Sistemi Informativi e deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente, attraverso il "modulo o procedura informatizzata (se attivata) di abilitazione utente". Lo stesso responsabile è tenuto a dare repentina comunicazione nel caso di revoca e/o trasferimento degli utenti della propria funzione/unità organizzativa.

Nel caso di collaboratori la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile del servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal servizio di assistenza ai Sistemi Informativi, associato ad una parola chiave (password) riservata, che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione, senza preventiva autorizzazione da parte del servizio di assistenza ai Sistemi Informativi.

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

Al primo utilizzo della rete informatica aziendale verrà chiesto obbligatoriamente di sostituire la parola chiave rilasciata dal servizio per l'informatica, sarà poi il sistema a chiedere la sostituzione della stessa ogni tre mesi.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il responsabile di funzione/unità operativa dovrà richiedere una nuova password di accesso ai Sistemi Informativi.

Soggetto preposto alla custodia delle credenziali di autenticazione alla rete informatica è il personale incaricato del servizio di assistenza ai Sistemi Informativi dell'Azienda.

CAPO II – DISPOSIZIONI PER L'UTILIZZO DEI SISTEMI INFORMATICI

Art. 5 – Utilizzo della rete informatica aziendale

Per l'accesso alla rete informatica dell'Azienda ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È proibito entrare nella rete informatica e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete informatica ed ai programmi sono personali e vanno tenute segrete.

Le cartelle utenti 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 temporaneamente, in queste unità. Sulle predette cartelle vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del servizio di assistenza ai Sistemi Informativi.

Il personale del servizio di assistenza ai Sistemi Informativi è autorizzato in qualunque momento a procedere alla rimozione di ogni file o applicazione pericolosi per la sicurezza del sistema sia nei personal computer degli incaricati sia nelle unità di rete.

È vietata l'installazione non autorizzata di modem o altri dispositivi o servizi atti a trasmettere o ricevere dati che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'Azienda.

È compito di ciascun utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati, le notizie e le informazioni aziendali che circolano nella rete informatica dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia.

I sistemi di teleassistenza remota sono permessi solo tramite VPN, preventivamente autorizzata dai Sistemi Informativi. Altre modalità potranno essere valutate per i singoli casi.

È vietato monitorare ciò che transita nella rete informatica dell'Azienda.

Art. 6 – Utilizzo del personal computer

Il personal computer affidato all'utente è uno strumento di lavoro.

Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza aziendale.

Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. È vietato ogni utilizzo a fini privati.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete informatica dell'Azienda solo attraverso specifiche credenziali di autenticazione come descritto negli articoli successivi.

L'Azienda si riserva di eliminare qualsiasi elemento hardware e software la cui installazione sia avvenuta senza formale richiesta da parte del responsabile di funzione/unità operativa e autorizzazione esplicita da parte dei Sistemi Informativi.

Costituisce buona regola la pulizia periodica (almeno una volta all'anno) delle cartelle, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati evitando l'archiviazione ridondante, specialmente sulle unità o cartelle di rete condivise.

L'archiviazione nei dischi locali del personal computer di dati personali e sensibili dell'assistito non è permessa. Tali dati dovranno essere archiviati nelle unità di rete aziendali NAS, previa abilitazione attraverso il "modulo o procedura informatizzata (se attivata) di abilitazione utente" richiedibile per singolo utente.

Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nel personal computer o in rete.

Il personale incaricato, anche dei servizi esternalizzati, che opera presso i Sistemi Informativi è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, alto). Detti interventi potranno comportare l'accesso in qualunque momento ai dati trattati da ciascun utente, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. Analogamente, sempre ai fini di sicurezza del sistema e per garantire la corretta operatività delle attività istituzionali, si procede in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato del servizio di assistenza ai Sistemi Informativi e dei servizi affidati in outsourcing è autorizzato a collegarsi e visualizzare in remoto, previa comunicazione all'utente, il desktop delle singole postazioni di personal computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, e simili. 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, fatta salva l'urgenza di procedere per non pregiudicare l'efficacia dell'intervento, verrà data comunicazione della necessità

dell'intervento stesso.

Non è consentito il collegamento mediante dispositivi non aziendali alla rete informatica aziendale salvo specifica richiesta da parte del responsabile di funzione/unità operativa e conferma dei Sistemi Informativi. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal servizio di assistenza ai Sistemi Informativi per conto dell'Azienda, né è consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, a fronte del grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della precedente disposizione espone sia l'Azienda sia l'utente a gravi responsabilità civili; inoltre le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e non protetto dal diritto d'autore, sono sanzionate penalmente.

Salvo preventiva espressa autorizzazione del personale del servizio di assistenza ai Sistemi Informativi, non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (a titolo esemplificativo masterizzatori, modem, dispositivi di memorizzazione, altro).

È autorizzato il solo uso di dispositivi esterni forniti dall'Azienda. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del servizio di assistenza ai Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dai successivi articoli del presente Regolamento relativamente alle procedure di protezione antivirus.

Il personal computer deve essere spento: ogni sera prima di lasciare gli uffici, 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 di assistenza ai Sistemi Informativi.

Il Personal Computer connesso alla rete informatica non va lasciato incustodito e per evitare l'utilizzo improprio da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso, è necessario attivare il blocco con la richiesta password**.**

Non sono consentiti spostamenti di postazioni di lavoro, salvo formale richiesta da parte del responsabile di funzione/unità operativa e autorizzazione esplicita da parte dei Sistemi Informativi.

Relativamente alle installazioni di personal computer da parte di terzi fornitori, devono essere autorizzate per iscritto dai Sistemi Informativi e devono rispettare pedissequamente il protocollo fornito a corredo dell'autorizzazione.

Nel personal computer non devono essere presenti file personali, quali ad esempio fotografie, file musicali, file video, file di attività extra lavorative. L'Azienda può monitorare la tipologia di file presenti e procede, senza nessun preavviso, alla rimozione degli stessi. Durante le operazioni di cambio / sostituzione del personal computer (ammodernamento del parco macchine), il tecnico addetto alla sostituzione rimuoverà, se presenti, tutti i file non inerenti all'attività lavorativa.

Art. 7 – Utilizzo di personal computer portatili

L'utente è responsabile del personal computer portatile assegnatogli dal servizio di assistenza ai Sistemi informativi e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai personal computer portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

II portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.

L'utente assegnatario di personal computer portatile è tenuto a collegarsi periodicamente, almeno una volta ogni 15 giorni, alla rete informatica interna per consentire il caricamento dell'aggiornamento

dell'antivirus.

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

I personal computer portatili devono essere restituiti al servizio di assistenza ai Sistemi Informativi al termine del rapporto.

Le disposizioni del presente articolo si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, altro.

Art. 8 – Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili forniti dall'Azienda (dischetti, CD e DVD riscrivibili, supporti USB, UNS Key, SSD ecc.), contenenti dati 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.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici e digitali rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio di assistenza ai Sistemi Informativi e seguire le istruzioni da questo impartite.

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

È vietato l'utilizzo di supporti rimovibili personali, salvo i casi espressamente autorizzati dal responsabile del servizio.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Art. 9 – Utilizzo degli applicativi informatici

Gli applicativi informatici per la gestione informatizzata delle attività istituzionali sono strumenti di lavoro.

Il loro utilizzo è consentito previa autenticazione personalizzata e profilazione per le funzioni allo specifico applicativo aziendale.

È vietato ogni utilizzo non inerente all'attività lavorativa con la correlata responsabilità dell'utente in ogni caso di uso illecito.

Art. 10 – Utilizzo della posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.

L'utente assegnatario è responsabile del corretto utilizzo della propria casella di posta elettronica.

Eventuali controlli a campione sui contenuti delle e-mail potranno essere effettuate dall'Azienda, adottando il principio di liceità e necessità come stabilito dal Garante per la protezione dei dati personali (deliberazione del n.13 del 1.3.2007).

L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa attraverso il "modulo o procedura informatizzata (se attivata) di abilitazione utente". Lo stesso responsabile è tenuto a dare tempestiva comunicazione nel caso di revoca e/o trasferimento degli utenti della propria funzione/unità organizzativa.

È fatto divieto di utilizzare le caselle di posta elettronica *nome.cognome@aulss2.veneto.it* per motivi diversi da quelli strettamente legati all'attività lavorativa. A titolo esemplificativo l'utente non può utilizzare la posta elettronica per:

- invio e/o il ricevimento di allegati contenenti filmati o brani musicali (mp3) non legati all'attività lavorativa;
- invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve dare comunicazione immediatamente al personale del servizio di assistenza ai Sistemi Informativi; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e in particolare gli allegati ingombranti.

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, conseguentemente, non deve essere utilizzata per inviare documenti o dati di lavoro contenenti dati sensibili.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus o ransomware, è obbligatorio cancellare i messaggi senza aprirli.

È obbligatorio controllare e porre la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica prima del loro utilizzo. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .cab, .exe, .scr, .pif, .bat, .cmd, altro) o collegamenti a siti web o ftp per lo scarico di file, questi ultimi non devono essere aperti e i messaggi devono essere cancellati.

Per la trasmissione di file è opportuno utilizzare le cartelle condivise; è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 15 MB, anche facendo ricorso ai più comuni formati compressi (*.zip *.rar *.jpg).

È fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti e collaboratori in ottemperanza agli obblighi di fedeltà e correttezza. È obbligatorio mantenere il seguente schema tipo per la firma in calce, inclusa la clausola di riservatezza delle informazioni:

Cognome Nome
Ruolo (opzionale)
Servizio …….. Distretto di ……...
Azienda ULSS 2 Marca trevigiana
tel. .....

CLAUSOLA DI RISERVATEZZA: Il contenuto della presente comunicazione è strettamente riservato, essendo indirizzato esclusivamente al destinatario sopra individuato e potendo contenere informazioni strettamente personali e/o confidenziali. Qualora fosse pervenuto a soggetto diverso dal destinatario questi deve intendersi sin d'ora avvisato che qualsiasi forma di diffusione dei dati, dei fatti e delle notizie apprese è assolutamente vietata. Si chiede cortesemente di cancellare il messaggio erroneamente ricevuto dal proprio sistema, dopo aver notificato al mittente l'errore commesso.

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 (ferie, permessi, 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. In tal caso, la funzionalità deve essere attivata dall'utente.

Sarà comunque consentito al responsabile della funzione/unità organizzativa dell'utente, preventivamente

sentito quest'ultimo, o comunque a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

Il personale del servizio di assistenza ai Sistemi Informativi 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 nel presente Regolamento o dalla legge.

Art. 11 – Utilizzo della rete Internet

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

L'utente è direttamente e pienamente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine Internet ai quali abbia stabilito un collegamento tramite link.

L'abilitazione ad Internet deve essere preceduta da regolare richiesta attraverso il "modulo o procedura informatizzata (se attivata) di abilitazione utente".

A titolo 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);
- 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 responsabile della funzione/unità organizzativa e/o dei Sistemi Informativi 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 o Social Network 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 della funzione/unità organizzativa.

L'accesso, tramite Internet, a caselle webmail di posta elettronica personale è consentito solo nel rispetto di quanto riportato nel presente Regolamento.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda adotta uno specifico sistema di blocco o filtro automatico per prevenire 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 articolo.

I controlli effettuati dall'Azienda a mezzo del personale incaricato dei Sistemi Informativi, ai sensi del precedente art. 3, 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 non oltre 6 mesi, e comunque per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

Art. 12 – Utilizzo di telefoni, fax, scanner e fotocopiatrici aziendali

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 comprovata necessità ed urgenza, mediante il telefono aziendale a disposizione.

Qualora venisse assegnato un telefono cellulare aziendale all'utente, previa autorizzazione rilasciata dalla Direzione, l'utente stesso sarà responsabile del suo utilizzo e della sua custodia.

Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso 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 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.

È vietato l'utilizzo dei fax aziendali per fini personali sia per spedire sia per ricevere documentazione, salva diversa esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile della funzione/unità organizzativa.

Art. 13 – Protezione antivirus

Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque verificare la presenza dell'antivirus nei propri dispositivi e tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, spegnere il personal computer e segnalare prontamente, attraverso gli opportuni canali, l'accaduto al personale del servizio di assistenza ai Sistemi Informativi.

Ogni dispositivo magnetico e digitale 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 di assistenza ai Sistemi Informativi.

Art. 14 – Osservanza delle disposizioni in materia di privacy

Tutti i soggetti a cui si applica il presente Regolamento devono osservare le disposizioni in materia di protezione dei dati personali e le misure minime per la sicurezza ai sensi del Codice della Privacy (D.Lgs. 30.6.2003, n. 196) e del Regolamento (CE) 27.4.2016 n. 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

Art. 15 – Accesso ai dati trattati dall'utente

È facoltà dell'Azienda – tramite il personale del servizio di assistenza ai Sistemi Informativi o addetti alla manutenzione – accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico sia per motivi di sicurezza del sistema informatico sia per motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, altro) o per finalità di controllo e programmazione dei costi aziendali (quali verifica dei costi di connessione ad Internet, traffico telefonico, altro), comunque estranei a qualsiasi forma di controllo dell'attività lavorativa.

Art. 16 – Sistema di controlli graduali

In caso di anomalie il personale incaricato del servizio di assistenza ai Sistemi Informativi effettuerà controlli anonimi, che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia e nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali con invito agli interessati di attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e per i

casi di particolare gravità previa autorizzazione della Direzione.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 17 – Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni del presente Regolamento.

Il mancato rispetto o la violazione delle disposizioni regolamentari è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dalla contrattazione collettiva e dalla legge, nonché con tutte le azioni civili e penali consentite (a titolo esemplificativo codice penale: art. 595, artt. 600-ter e segg., art. 615-ter, art. 615-quarter, art. 615-quinques, art. 617-quarter, art. 617-quinquies, art. 617-sexies, art. 635-bis, art. 635-ter, art. 635- quarter, art. 635-quinquies, art. 640 ed art. 640 ter).

CAPO III – NORME FINALI

Art. 18 – Norma di rinvio

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa statale e regionale di riferimento.

Art. 19 – Abrogazione di norme

Dalla data di entrata in vigore del presente Regolamento sono abrogate tutte le precedenti disposizioni in materia emanate dalle ex aziende sanitarie n. 7 di Pieve di Soligo, n. 8 di Asolo, n. 9 di Treviso e dall'Azienda ULSS n. 2 Marca trevigiana.

Art. 20 – Entrata in vigore

Il presente Regolamento entra in vigore nel quindicesimo giorno successivo a quello della pubblicazione della relativa deliberazione di approvazione nell'Albo on-line istituzionale.