ASL di Brescia – Sede Legale: viale Duca degli Abruzzi, 15 – 25124 Brescia
Tel. 030.38381 Fax 030.3838233 - www.aslbrescia.it - informa@aslbrescia.it
Posta certificata: servizioprotocollo@pec.aslbrescia.it
Codice Fiscale e Partita IVA: 03436310175

DECRETO n. 179 del 05/04/2013

Cl. 01.07

OGGETTO: Approvazione del Regolamento per l'utilizzo dei sistemi informatici aziendali.

Il DIRETTORE GENERALE - Dr. Carmelo Scarcella
nominato con D.G.R. IX/001088 del 23.12.2010

Acquisiti i ***pareri di competenza*** del DIRETTORE SANITARIO	Dr. Francesco Vassallo
e del DIRETTORE SOCIALE	Dott.ssa Anna Calvi
Acquisito il ***parere di legittimità*** del DIRETTORE AMMINISTRATIVO	Dott. Pier Mario Azzoni

Regione Lombardia

ASL Brescia

IL DIRETTORE GENERALE

Premesso che:
- 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'Ente 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;

Rilevato che 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, (dipendenti, amministratori e collaboratori) adeguata informazione circa le modalità da seguire per un corretto uso degli strumenti e delle risorse informatiche e telematiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che possano, contestualmente, collaborare alle politiche di sicurezza messe in atto;

Ritenuto inoltre di 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 invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori (legge n. 300/1970) e dal D.Lgs. 196/03;

Richiamata la deliberazione dell'autorità Garante per la protezione dei dati personali (G.U. del 10.03.2007) con la quale sono state definite le "Linee guida del Garante per la posta elettronica ed Internet" (n. 13 del 01 marzo 2007);

Vista la proposta di "Regolamento aziendale sull'utilizzo dei sistemi informatici" predisposta dal Responsabile del Servizio Sistema Informativo Aziendale e Controllo di Gestione e ritenuto di approvarla nel testo che si allega al presente decreto per farne parte integrante e sostanziale (Allegato "A" di pagine n. 23);

Dato atto che la proposta di Regolamento è stata oggetto di informativa alle Organizzazioni Sindacali;

Precisato e ribadito che tale Regolamento:
- si conforma alle indicazioni fornite dal Garante per la Protezione dei dati personali che, con deliberazione n. 13 del 01 marzo 2007, ha emanato le linee guida 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'Ente 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'Ente, 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;

Regione Lombardia

ASL Brescia

Vista la proposta del Direttore del Servizio Informativo Aziendale e Controllo di Gestione, Dott. Gianfranco Tortella;
Dato atto che il Responsabile dell'U.O. Innovazione e Sviluppo Tecnologico attesta, in qualità di Responsabile del procedimento, la regolarità tecnica del presente provvedimento;
Preso atto che dal presente provvedimento non discendono oneri per l'Azienda;
Acquisiti i pareri di competenza del Direttore Sanitario, Dr. Francesco Vassallo e del Direttore Sociale, Dott.ssa Anna Calvi;
Acquisito il parere di legittimità del Direttore Amministrativo, Dott. Pier Mario Azzoni;

D E C R E T A

a) di approvare il "Regolamento aziendale sull'utilizzo dei sistemi informatici" (posta elettronica – rete intra/internet – postazioni di lavoro) di cui all'allegato "A", parte integrante del presente provvedimento (composto di n. 23 pagine);
b) di incaricare il Responsabile dell'U.O. Innovazione e Sviluppo Tecnologico, Ing. Ivan Campa, di rendere noto a tutti gli utenti il contenuto del presente Regolamento con le forme più efficaci ed immediate e di supervisionare in ordine alla sua corretta attuazione;
c) di disporre che i Responsabili dei differenti assetti aziendali prestino la necessaria collaborazione affinché vengano attuate tutte le disposizioni contenute nel Regolamento;
d) di demandare al Direttore del Servizio Risorse Umane l'integrazione dei modelli di contratto per il conferimento degli incarichi di lavoro autonomo con la previsione dell'obbligo, per i lavoratori autonomi (tra i quali titolari di incarichi libero professionali e di collaborazione coordinata e continuativa), del rispetto del Regolamento che si approva con il presente provvedimento;
e) di dare atto che nessun onere deriva dall'assunzione del presente provvedimento;
f) di dare atto che il presente provvedimento è sottoposto al controllo del Collegio Sindacale in conformità ai contenuti dell'art. 3-ter del D.Lgs. n. 502/1992 e s.m.i. e dell'art. 12, comma 12, della L.R. n. 33/2009;
g) di disporre, a cura del Servizio Affari Generali, la pubblicazione all'Albo on-line ai sensi dell'art. 18 della L.R. n. 33/2009 e dell'art. 32 della L. n. 69/2009.

Firmato digitalmente dal Direttore Generale
Dr. Carmelo Scarcella

Regione Lombardia

ASL Brescia

Allegato A

REGOLAMENTO AZIENDALE SULL'UTILIZZO DEI SISTEMI INFORMATICI

(*POSTA ELETTRONICA – RETE INTRA/INTERNET – POSTAZIONI DI LAVORO*)

INDICE

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'ASL della provincia di Brescia ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Considerato inoltre che l'ASL della provincia di Brescia, nell'ottica di uno svolgimento proficuo e 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, postazioni di lavoro, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), viene adottato il presente regolamento relativo alle modalità ed all'utilizzo di tale strumentazione.

2. SCENARIO

Le realtà aziendali sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche e telefoniche, che se da un lato hanno consentito l'introduzione di innovative tecniche di gestione, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici/telefonici forniti dall'Azienda ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati.

In questo senso, viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 01/03/07) 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/telefonici tuttavia, devono garantire tanto il diritto dell'Ente di proteggere la propria organizzazione, essendo i computer ed i telefoni aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, 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 (legge n. 300/1970) e dal Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003).

Alla luce delle considerazioni sopra espresse e tenuto opportunamente conto delle Linee guida emanate dall'Autorità garante per la protezione dei dati personali, con propria deliberazione n. 13 del 1 marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, è stato elaborato il presente regolamento, al fine di disciplinare le condizioni e le modalità per il corretto utilizzo degli strumenti informatici/telefonici da parte dei dipendenti e/o collaboratori. Il regolamento, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto tenendo opportunamente conto altresì delle disposizioni contenute nella Legge. n. 300/1970 in tema di provvedimenti disciplinari (art. 7).

Con riferimento alle normativa in tema di protezione dei dati personali, si ricorda come il Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003) stabilisca che l'attività di controllo debba essere rispettosa dei principi fondamentali di "proporzionalità" (art. 3), debba avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (art. 2) e soprattutto, che di tale attività, debba essere fornita adeguata e preventiva informativa (art. 13).

Il regolamento ha lo scopo di informare gli interessati sulle finalità dell'utilizzo degli strumenti informatici, del controllo e sulle specifiche metodologie adottate per effettuarlo. Particolare attenzione dovrà comunque esser prestata all'attività di controllo della navigazione internet qualora, mediante l'individuazione dei contenuti dei siti visitati, si determini un trattamento di dati sensibili per i quali deve sempre essere rispettato il principio dell'indispensabilità (art. 26, 4°comma lett. c) del Codice sul trattamento dei dati personali (D.Lgs. n. 196/2003).

Il regolamento, inoltre, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici/telefonici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela della attività aziendale, quando queste importanti informazioni di proprietà dell'Azienda sono custodite nel sistema informatico.

Il presente Regolamento disciplina le modalità di accesso e fornitura dei servizi informatici e di rete dell'ASL, sia all'interno sia all'esterno delle sedi di lavoro.
L'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al rispetto da parte degli utenti del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.
Il Regolamento si applica a tutte le tipologie di servizi e dati, nelle modalità operative descritte nelle di seguito indicate
Le Norme Attuative sono modificate/aggiornate dal Servizio SIA come da successivo art. 5.

3. DEFINIZIONI

Per gli scopi del presente regolamento si definiscono:

Account istituzionale	Account fornito dall'ASL a ciascun Utente per accedere ai servizi informatici e di rete in accordo con il relativo Profilo Utente
ASL	Azienda Sanitaria Locale della provincia di Brescia
BIOS	Basic Input-Output System
Internet	Rete di accesso pubblico alla quale la Rete Interna accede e si presenta con i propri servizi
LOG	Registrazione cronologica delle operazioni e il file su cui tali registrazioni sono memorizzate
NAS	Network Attached Storage
PdL	Postazione di Lavoro che si basa su strumenti informatici (PC, *smartphone*, ecc.) tramite i quali l'Utente accede ai servizi informatici e di rete dell'ASL, sia dalla Rete Interna sia da Internet
Profilo utente	Tipologia di Utente con accesso ad un numero predefinito di servizi informatici e di rete
Responsabile di Struttura	Direttore di Dipartimento o responsabile di UOC o UOS
Rete Interna	insieme delle risorse di rete che consentono il collegamento informatico e telematico tra le diverse sedi dell'ASL
SIA	Sistema Informativo Aziendale
Sistema	Dispositivo in grado di erogare servizi informatici o di rete (*server*, *access point*, *router*, *switch*, ecc.)
Struttura	Unità operativa (semplice o Complessa) dell'Azienda
UOC	Unità Operativa Complessa
UOS	Unità Operativa Semplice
Utente	Soggetto con diritto di accesso ai servizi informatici e di rete, in accordo con il proprio profilo di appartenenza e il presente Regolamento
VPN	Virtual Private Network

4. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento, sarà disponibile sulla intranet aziendale.

4.1. CAMPO DI APPLICAZIONE DEL REGOLAMENTO.

4.1.1. Il nuovo 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 (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

4.1.2. 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, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

5. ATTUAZIONE DEL REGOLAMENTO

Spettano al Servizio SIA i compiti di coordinamento e controllo dell'attuazione tecnica del Regolamento secondo le modalità descritte nelle Norme Attuative.
Il responsabile del Servizio SIA può modificare le Norme Attuative, purché rimangano conformi al Regolamento.
Tali modifiche vengono elaborate in accordo o su indicazione del Delegato del Direttore Generale per l'Innovazione e lo sviluppo Tecnologico dei Sistemi Informativi, sulla base dell'evoluzione tecnologica nel settore o di variazioni apportate al Regolamento o comunque ogni qualvolta si riscontrino evidenti e documentabili esigenze tecniche o funzionali.
Nell'espletamento di queste funzioni il responsabile del Servizio SIA si avvale della collaborazione del personale del Servizio stesso ed in particolare di tutti i Responsabili delle UOC., ognuno secondo le rispettive competenze.
Il responsabile del Servizio SIA, ove necessario, può ricorrere anche a consulenti esterni o interni all'ASL, esperti di comprovata competenza nell'erogazione dei servizi informatici e di rete.

6. UTILIZZO DEL PERSONAL COMPUTER

6.1. LA POSTAZIONE DI LAVORO.

6.1.1. 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, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

6.1.2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'ASL della provincia di Brescia solo attraverso specifiche credenziali di autenticazione, come meglio descritto nei paragrafi successivi del presente Regolamento.

6.1.3. Il personale incaricato, che opera presso il Servizio SIA, 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 (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.).

6.1.4. Il personale incaricato del Servizio SIA ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, etc. 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.

6.1.5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio SIA per conto dell'ASL, 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 esistenti. L'inosservanza della presente disposizione espone la stessa ASL a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

6.1.6. Salvo preventiva espressa autorizzazione del personale del SIA, non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori. Modem, modem USB, dispositivi di memorizzazione USB ecc…).

6.1.7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio SIA nel caso in cui siano rilevati virus.

6.1.8. 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. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

6.1.9. Sul personal computer non devono essere presenti file personali, quali ad esempio: fotografie, file musicali, file video, file di attività extra lavorative. Il servizio SIA monitora con strumenti automatizzati 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".

7. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

7.1. CREDENZIALI DI AUTENTICAZIONE.

7.1.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del servizio SIA, previa formale richiesta del responsabile del servizio 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 del servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

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

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

7.1.4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi e comunque nel rispetto della vigente normativa in tema di privacy.

8. UTILIZZO DELLA RETE LOCALE

8.1. RETE LOCALE ASL.

8.1.1. Per l'accesso alla rete locale dell'ASL ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

8.1.2. Le credenziali costituiscono l'Account Istituzionale dell'Utente presso l'ASL.

8.1.3. Le credenziali vengono revocate alla chiusura del rapporto tra Utente ed ASL.

8.1.4. L'Utente, preso atto che la conoscenza della password da parte di terzi può consentire agli stessi l'accesso ai servizi in nome dell'Utente titolare e l'accesso ai dati cui il medesimo è abilitato (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, uso indebito di servizi, ecc.), si impegna a:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria Postazione di Lavoro (PdL) a persone non autorizzate;
- non lasciare incustodita ed accessibile la propria PdL una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password nella massima riservatezza e con la massima diligenza avvisare prontamente l'ufficio competente al riguardo nell'ipotesi di smarrimento dei dati di accesso, non utilizzare credenziali di altri utenti nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.

8.1.5. Le cartelle utenti presenti nei server dell'ASL (NAS) 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. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio SIA. Tutti i documenti per qui si renda necessaria la garanzia della conservazione devono essere posizioni sui server NAS o copiati sugli stessi periodicamente..

8.1.6. Il personale del Servizio SIA può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

8.1.7. 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.

8.1.8. E' fatto divieto di collegare alla rete aziendale computer personali o computer non assegnati dal competente servizio aziendale, salvo motivata richiesta da parte del Dirigente responsabile del richiedente ed autorizzazione da parte del Servizio SIA.

8.2. REGOLE DI UTILIZZO

8.2.1. Servizi informatici e di rete potranno essere utilizzati dagli Utenti previa autenticazione e nel rispetto del Profilo Utente di appartenenza.

8.2.2. A ciascun Profilo Utente è associato un insieme di servizi informatici e di rete predefiniti. Ciascun Utente può accedere ed utilizzare unicamente i servizi disponibili per il proprio profilo Utente.

8.2.3. L'Utente è autorizzato all'utilizzo dei servizi unicamente nell'ambito delle proprie funzioni istituzionali dell'ASL.

8.2.4. Per ciascun Utente, in fase di utilizzo dei servizi, è vietato:

- violare la privacy di altri Utenti o dell'integrità di dati personali;
- compromettere l'integrità dei sistemi o dei servizi;
- consumare risorse in misura tale da compromettere l'efficienza di altri servizi di rete;
- compiere atti di criminalità informatica;
- accedere alla Rete Interna per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'ASL;
- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete Interna;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi;
- violare gli obblighi contrattualmente assunti dall'ASL per la realizzazione e la gestione della Rete Interna, particolarmente in materia di copyright, licenze d'uso di software e regolamenti dei fornitori di connettività di rete;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (persone, capacità, elaboratori), danneggino o restringano l'utilizzabilità o le prestazioni della Rete Interna;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete Interna, dei quali non si è destinatari specifici;
- compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del software;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare o accedere o tentare di

accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi;

- creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
- utilizzare la Rete dell'ASL e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale, tranne nei casi specificatamente autorizzati dal Direttore Generale.

9. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

9.1. SUPPORTI RIMOVIBILI.

9.1.1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, dischi esterni, memorie a stato solido, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how 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.

9.1.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio SIA e seguire le istruzioni da questo impartite.

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

9.1.4. E' vietato l'utilizzo di supporti rimovibili personali.

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

10. UTILIZZO DI PERSONAL COMPUTER PORTATILI

10.1. PERSONAL COMPUTER PORTATILI

10.1.1.L'utente è responsabile del Personal Computer portatile assegnatogli dal Servizio SIA e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

10.1.2.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.

10.1.3.I Personal Computer portatili, se non dotati di connessione VPN, per garantire il corretto aggiornamento degli applicativi installati, devono essere connessi alla rete aziendale, almeno ogni due settimane, per un periodo non inferiore alle 2 ore.

10.1.4.Tali disposizioni si applicano anche nei confronti di incaricati esterni.

11. USO DELLA POSTA ELETTRONICA

11.1. POSTA ELETTRONICA.

11.1.1.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.

11.1.2.È fatto divieto di utilizzare le caselle di posta elettronica nome.cognome@aslbrescia.it per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti fotografie, 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, catene telematiche, ecc. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi, questo per evitare l'infezione da virus informatici.

11.1.3.La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di dimensioni rilevanti.

11.1.4.Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile cancellare tutto, messaggio ed allegato, onde evitare infezioni da virus, ecc.

11.1.5.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 del Servizio di appartenenza. Tale funzionalità deve essere attivata dall'utente, in subordine sarà attivata dal Servizio SIA su richiesta del Dirigente Responsabile.

12. ACCESSO AD INTERNET

12.1. RETE INTERNET.

L'accesso ad internet è consentito da tutte le postazioni di lavoro Aziendali.
L'accesso alla Rete Interna da parte dell'Utente da Internet è consentito unicamente mediante i servizi di accesso remoto erogati dal servizio SIA.
Il personale del Servizio SIA periodicamente effettua controlli a campione sugli accessi internet effettuati dai dipendenti stessi.
Si ribadisce che i controlli rispettano i principi di pertinenza e di non eccedenza.

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

12.1.2.In questo senso l'utente non potrà utilizzare internet per:

- *l'upload o il download di software, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio SIA);*
- *ogni forma di registrazione e accesso 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 (è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti) anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile del Servizio;*

12.1.3.Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, è stato attivato uno specifico sistema di filtro automatico che impedisce determinate operazioni quali lo scarico di programmi o l'accesso a determinati siti inseriti in una black-list.

12.1.4.Il personale del Servizio SIA è autorizzato al trattamento in forma anonima, tale da precludere l'immediata identificazione degli utenti, dei dati relativi al "traffico" internet. I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

12.1.5.Il controllo anonimo potrebbe concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito, da parte del Responsabile del Servizio SIA, ad attenersi scrupolosamente a

compiti assegnati e istruzioni impartite dal Responsabile del Servizio di appartenenza dell'utente individuato. L'avviso sarà circoscritto ai dipendenti afferenti al Servizio a cui l'utente individuato appartiene e in cui è stata rilevata l'anomalia. In assenza di successive anomalie non verranno in ogni caso effettuati controlli su base individuale.

12.1.6.E' esclusa la possibilità e l'ammissibilità di controlli prolungati, costanti e indiscriminati.

12.1.7.Il Sistema informatico di questa ASL è programmato e configurato per cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

12.1.8.Verranno prolungati i tempi di conservazione (limitatamente comunque alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

- *Esigenze tecniche o di sicurezza del tutto particolari;*
- *Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;*
- *Obbligo di custodire o conservare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria*

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

13. PROTEZIONE ANTIVIRUS

13.1. ANTIVIRUS.

13.1.1. Il sistema informatico dell'ASL 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 aggressivo.

13.1.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto al personale del Servizio SIA.

13.1.3. Ogni supporto di memoria 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 SIA.

14. UTILIZZO DEI TELEFONI FAX E FOTOCOPIATRICI

14.1. TELEFONI.

14.1.1. 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 consentito solo nel caso di comprovata necessità ed urgenza.

14.1.2. 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 dal personale del Servizio SIA.

14.2. FAX

14.2.1. È vietato l'utilizzo dei fax aziendali per fini personali.

14.3. FOTOCOPIATRICI

14.3.1. È' vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

15. SISTEMI DI CONTROLLO GRADUALI

15.1. CONTROLLI GRADUALI

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

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

16. SANZIONI

È fatto obbligo a tutti gli utenti (art. 4.1) di osservare le disposizioni portate a conoscenza con il presente regolamento.
Il mancato rispetto o la violazione delle regole sopra indicate comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare. Sono, inoltre, fatte salve le azioni civili e /o penali qualora ne ricorrano i presupposti.