

AZIENDA SANITARIA LOCALE TO 1
REGIONE PIEMONTE
Via San Secondo, 29 – 10128 Torino

DELIBERAZIONE DEL DIRETTORE GENERALE
(Nominato con DGR n. 65-7819 del 17/12/2007)

N. 126/300/2010 DEL 31 DIC. 2010

GRUPPO DI PROGETTO DEI SERVIZI INTEGRATI E DELLA GESTIONE AZIENDALE DELLA
PROTEZIONE DEI DATI PERSONALI

**OGGETTO: REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE
INFORMATICHE, DI INTERNET E DI POSTA ELETTRONICA DA
PARTE DEI LAVORATORI DELL'ASL TO1.**

AZIENDA SANITARIA LOCALE TO1

L'anno duemiladieci il giorno 31 del mese di dicembre in Torino, presso la sede dell'A.S.L. TO1 di Torino, Via S. Secondo, 29

IL DIRETTORE GENERALE

Esaminata la seguente proposta del Direttore del Gruppo di Progetto dei Servizi Integrati e della Gestione Aziendale della Protezione dei Dati Personali;

- *“richiamato il Decreto Legislativo 30 giugno 2003, n. 196 denominato “Codice in materia di protezione dei dati personali”;*
- *preso atto che tale decreto detta una serie di regole volte alla tutela della riservatezza dei cittadini, al fine di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, disciplinando anche, le modalità per l'adempimento degli obblighi di rispetto e di tutela dei diritti e delle libertà da parte dei titolari del trattamento;*
- *considerato che, in tale ambito, anche i datori di lavoro, in quanto titolari del trattamento, devono conformare il loro operato alle disposizioni vigenti e richiamata la deliberazione del 1° marzo 2007 n. 13 con la quale il Garante della Privacy ha fornito le linee guida per l'utilizzo nei luoghi di lavoro della posta elettronica e di internet e definito le regole alle quali il datore di lavoro deve attenersi nel trattare i dati personali raccolti in occasione delle attività di verifica del corretto utilizzo della rete Internet e del sistema di posta elettronica da parte dei lavoratori;*
- *richiamata la direttiva N. 02/09 del 26/05/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica la quale, riferendosi anche al provvedimento del Garante della Privacy, rileva che l'utilizzo delle tecnologie informatiche costituisce ormai il principale strumento di lavoro a disposizione dei dipendenti delle pubbliche amministrazioni e pertanto riconosce da un lato alle Amministrazioni, in quanto datori di lavoro, l'obbligo di assicurare la funzionalità ed il corretto utilizzo degli strumenti informatici da parte dei lavoratori, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici; dall'altra riconosce all'Amministrazione il potere di controllo sul corretto utilizzo di tali mezzi, nel rispetto di alcune regole e principi generali quali il principio di proporzionalità cioè di pertinenza e non eccedenza delle attività di controllo; di rispetto delle procedure di informazione/consultazione delle rappresentanze dei lavoratori; della preventiva informazione ai lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere dati personali;*
- *considerato ancora che tale circolare chiarisce come esista in capo ai dipendenti l'obbligo sancito da norme di legge e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa e pertanto, anche l'utilizzo delle risorse informatiche da parte dei dipendenti oltre a non dover compromettere la sicurezza e la riservatezza del Sistema Informatico Aziendale, non deve essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici, atteso che, come la giurisprudenza amministrativa ha già statuito, l'indebito utilizzo del dipendente di suddette risorse (quali ad esempio l'indebita connessione ad internet) configura responsabilità a carico del lavoratore per il danno patrimoniale cagionato all'Amministrazione, consistente nel mancato svolgimento dell'attività lavorativa durante le ore di connessione;*
- *verificato, alla luce della normativa sopra richiamata, che grava sul datore di lavoro l'onere di indicare chiaramente quali siano le modalità di utilizzo ritenute corrette, degli strumenti*

informatici messi a disposizione dei propri lavoratori e in che misura e con quali modalità vengano effettuati controlli;

- *dato atto quindi della necessità di adottare a cura dell'ASL TO1 un regolamento aziendale che disciplini in modo organico la materia in particolare informando i lavoratori rispetto al trattamento dei dati effettuato dall'Azienda, nell'ambito dell'uso di Internet e posta elettronica;*
- precisato che, la bozza di tale regolamento, è stata sottoposta all'esame delle Organizzazioni Sindacali Aziendali sia del Comparto che della Dirigenza;
- ritenuto di condividere la suddetta proposta;
- assunta la correttezza del processo istruttorio correlato la cui responsabilità è riconducibile al Dirigente proponente;
- preso atto del concordante parere favorevole espresso dal Direttore Amministrativo e dal Direttore Sanitario, ex art. 3, 1° comma quinquies, D.Lgs. 30/12/92 n. 502 e successive integrazioni e modificazioni;

DELIBERA

1. di approvare il "Regolamento aziendale per l'utilizzo delle risorse informatiche, di Internet e di Posta Elettronica da parte dei lavoratori dell'ASL TO1, che costituisce parte integrante e sostanziale del presente provvedimento;
2. di trasmettere il presente provvedimento al Collegio Sindacale, per gli adempimenti di competenza, ai sensi dell'art. 3 ter D.Lvo 229/99 e dell'art. 14, comma 2, lettera b) della L.R. 24.1.1995 n. 10;
3. di dare atto che il presente provvedimento non comporta, ex se, alcun onere di spesa;
4. di dichiarare la presente deliberazione immediatamente esecutiva, ai sensi dell'art. 28 della L.R. 24.1.1995 n. 10.

IL DIRETTORE GENERALE
(Dott. Ferruccio MASSA)

AZIENDA SANITARIA LOCALE TO 1
REGIONE PIEMONTE
Via San Secondo, 29 – 10128 Torino

**REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE, DI
INTERNET E DI POSTA ELETTRONICA DA PARTE DEI LAVORATORI DELL'ASLTO1.**

INDICE

Premessa

Art. 1 – OGGETTO

Art. 2 – DEFINIZIONI

Art. 3 – UTILIZZO DEL PERSONAL COMPUTER

Art. 4 – MODALITA' DI ACCESSO E DI UTILIZZO

Art. 5 – UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Art. 6 – UTILIZZO DI PC PORTATILI

Art. 7 – UTILIZZO DI INTERNET

Art. 8 – UTILIZZO DELLA POSTA ELETTRONICA

Art. 9 - UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI AZIENDALI

Art. 10 – MONITORAGGIO E CONTROLLI

Art. 11- INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO INTERNET

Art. 12- NON OSSERVANZA DEL REGOLAMENTO

Art. 13- INFORMATIVA

Art. 14 ENTRATA IN VIGORE E PUBBLICITA'

Art. 15 – DISPOSIZIONI FINALI

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'ASL TO1 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 TO1 adotta il presente Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.

Le prescrizioni di seguito stabilite si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003, n. 196, e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza.

Considerato, inoltre, che l'ASL TO1, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha deciso di mettere a disposizione dei propri dipendenti e collaboratori, che ne necessitino per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri da osservare circa l'utilizzo di tale strumentazione.

Art. 1 – OGGETTO

1. Il disciplinare, adottato sulla base e secondo le indicazioni contenute nella deliberazione 1° marzo 2007, n. 13, del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e Internet", ha per oggetto i criteri e le modalità operative di accesso e utilizzo del servizio Internet e di posta elettronica da parte dei dipendenti dell'ASL TO1 e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Azienda (a titolo esemplificativo e non esaustivo: lavoratori interinali, collaboratori, liberi professionisti, specializzandi, tirocinanti/stagisti).

Art. 2 – DEFINIZIONI

1. Nel presente documento, i termini di seguito elencati hanno le correlate definizioni:
 - **POSTAZIONE DI LAVORO:** personal computer collegato alla rete aziendale tramite il quale l'utente accede ai servizi;
 - **UTENTE INTERNET:** persona autorizzata ad accedere al servizio internet con l'esclusione dei siti previsti nella black-list;
 - **UTENTE DI POSTA ELETTRONICA:** persona autorizzata ad accedere al servizio di posta elettronica;
 - **BLACK LIST:** elenco di siti non accessibili da nessun utente;
 - **INTERNET PROVIDER:** azienda che fornisce all'ASL TO1 il canale di accesso alla rete internet;
 - **LOG:** archivio delle attività di consultazione in rete.

Art. 3 – UTILIZZO DEL PERSONAL COMPUTER.

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.
2. Il Personal Computer deve essere custodito con cura prevenendo ogni possibile forma di danneggiamento.
3. Il personale incaricato dalla Struttura Complessa Sistema Informatico 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 esempio aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware)
4. Il personale incaricato dalla Struttura Complessa Sistema Informatico ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni di lavoro PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito di 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.

5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'Azienda tramite la Struttura Complessa Sistema Informatico, né è 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.
6. L'inosservanza della presente disposizione espone l'Azienda a gravi responsabilità civili; si evidenzia inoltre che la violazione 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, sono sanzionate anche penalmente.
7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna e avvertire immediatamente il personale della Struttura Complessa Sistema informatico nel caso in cui siano rilevati virus.
8. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaborato incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Art. 4 – MODALITA' DI ACCESSO E DI UTILIZZO

1. Per accedere al Personal Computer l'utente deve utilizzare un codice identificativo (id utente) ed una parola chiave segreta (password). Le medesime credenziali di autenticazione consentono l'accesso anche ai servizi informatici.
2. Superato il sistema di autenticazione l'utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.
3. Le postazioni di lavoro sono preventivamente individuate ed assegnate personalmente a ciascun utente, ove possibile, o condivise tra più utenti.
4. L'utente, preso atto che la conoscenza della password da parte di terzi consente agli stessi l'accesso alla rete aziendale, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato, con possibilità di gestione degli stessi (ad esempio, visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi) si impegna a:
 1. non concedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato;
 2. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione (ad esempio, attivando il blocco schermo, digitando Ctrl+Alt+Canc, Blocca computer);
 3. conservare la password nella massima riservatezza e con la massima diligenza;
 4. non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o se pervenute casualmente a conoscenza;
 5. mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati;
 6. non salvare file audio, video e file non istituzionali di qualsiasi tipo nelle connessioni di rete su cui viene eseguito giornalmente il back-up.
5. L'installazione di software o la modifica delle configurazioni, la configurazione dei servizi di accesso ad internet e di posta elettronica sono eseguite esclusivamente da personale specializzato incaricato dall'ASL TO1. Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati.
6. Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.
7. L'utente è civilmente responsabile di qualsiasi danno arrecato all'ASL TO1 e all'Internet provider e/o terzi in dipendenza della mancata osservazione di quanto previsto dal presente disciplinare.
8. L'utente può essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della Corte di Cassazione.

9. La violazione delle presenti disposizioni può comportare responsabilità disciplinare, rimanendo ferma ogni ulteriore forma di responsabilità penale.

Art. 5 – UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, 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.
2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati sensibili, ciascun utente potrà contattare il personale della Struttura Complessa Sistema Informatico e seguire le istruzioni impartite.
3. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
4. E' vietato l'utilizzo di supporti rimovibili personali.
5. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi custoditi.

Art. 6 – UTILIZZO DI PC PORTATILI

1. **Il PC portatile assegnato costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.**
2. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
3. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
4. I PC 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 e sottrazioni.

Art. 7 – UTILIZZO DI INTERNET

1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.**
2. Tutti gli utenti cui è assegnata dall'Azienda ASL TO1 una postazione di lavoro possono utilizzare Internet, previa identificazione con le modalità precedentemente illustrate (ID UTENTE/PASSWORD). Su richiesta, adeguatamente motivata, dei direttori di struttura è possibile revocare l'accesso ad Internet a determinate utenze.
3. Al fine di prevenire il rischio di utilizzi impropri della rete, l'ASL TO1 utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno natura istituzionale (BLACK LIST).
4. Le modalità di individuazione e di applicazione dei filtri sono decise dalla Struttura Complessa Sistema Informatico.
5. L'utente è direttamente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che ivi vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
6. E' vietato scaricare immagini, file audio o musicali, file video e in ogni caso di grandi quantità di dati in grado di degradare le prestazioni offerte dal servizio agli altri utenti.
7. All'utente non è consentito:
 - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
 - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting, messaging o similari, così come connettersi ai siti che trasmettono programmi streaming (come radio o TV via WEB);

- scaricare software dalla rete; eventuali necessità devono essere appositamente richieste alla Struttura Complessa Sistema Informatico;
- utilizzare Internet provider diversi da quello ufficiale dell'ASL TO1 e la connessione di stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi (ad esempio, modem) da quello centralizzato;
- usare la rete in modo difforme da quanto previsto dal presente disciplinare e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

Art. 8 – UTILIZZO DELLA POSTA ELETTRONICA

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.
2. L'utilizzo del servizio di posta elettronica è consentito ai lavoratori ai quali l'ASL TO1 assegna indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, affari.general@aslto1.it) affiancati a quelli individuali (ad esempio mario.rossi@aslto1.it).
3. L'eventuale casella del Servizio/Ufficio è accessibile solo in modalità di delega, previa richiesta e autorizzazione del Responsabile della Struttura.
4. In caso di assenza l'utente delega altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al diretto superiore quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà comunque consentito al responsabile della struttura di appartenenza dell'utente accedere alla casella di posta elettronica dell'utente, in caso di assenza, qualora si renda necessario. Di tale operazione deve essere redatto apposito verbale.
5. Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominativa) verrà accluso il seguente testo: "Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente".
6. All'utente non è consentito:
 - utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione o azioni equivalenti;
 - utilizzare il servizio di posta elettronica per inoltrare "catene di Sant'Antonio", appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, messaggi augurali e altre e-mail che non siano di lavoro;
 - allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad esempio, programmi, script, macro), così come file di dimensioni eccessive.

ART. 9 UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI AZIENDALI.

1. Per quanto riguarda l'utilizzo di telefoni sia fissi che cellulari si rimanda alla specifica disciplina di cui all'atto deliberativo n. 31/D.04/10 del 22/01/2010 avente ad oggetto "Regolamenti aziendali di assegnazione e gestione degli apparecchi di telefonia fissa e di telefonia mobile".
2. E' vietato l'uso di fotocopiatrici aziendali per fini personali.

Art. 10 – MONITORAGGIO E CONTROLLI

1. L'ASL TO1 può avvalersi di sistemi di controllo del corretto utilizzo degli strumenti di lavoro che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori nel rispetto di quanto previsto dal Provvedimento del garante della Privacy del 1° marzo 2007 n. 13.
2. Le comunicazioni effettuate attraverso il servizio di posta elettronica interno sono riservate. Il contenuto di tali comunicazioni non può essere in nessun caso oggetto di alcuna forma di verifica, controllo o censura da parte dell'ASL TO1, dell'Internet provider o da parte di altri soggetti.
3. Le attività sull'uso del servizio di accesso ad Internet sono automaticamente registrate in forma elettronica attraverso i LOG di sistema.
4. Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima e/o aggregata, in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.
5. I dati anonimi e/o aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Direttore Amministrativo per le valutazioni di competenza e riguardano:

h

- per ciascun sito/dominio visitato le seguenti informazioni: il numero di indirizzi IP che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
 - per ciascun indirizzo IP le seguenti informazioni: il numero di siti visitati, la quantità totale di dati scaricati e le postazioni di lavoro utilizzate per la navigazione.
6. I dati personali contenuti nei log possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:
- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
 - su richiesta della Direzione Aziendale quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
 - su richiesta della Direzione Aziendale limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area.
- In particolare i controlli si svolgeranno in forma graduata:
1. In via preliminare l'azienda provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.
 2. In assenza di successive anomalie non si effettueranno controlli su base individuale.
 3. Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazione di lavoro e in caso di abusi singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati – anche per verifiche sulla funzionalità e sicurezza del sistema – inoltrando preventivi avvisi collettivi o individuali).
 4. Nel caso in cui la posta elettronica e la rete Internet siano utilizzate indebitamente o di riscontro e reiterato uso non conforme delle risorse informatiche, la Struttura Complessa Sistema Informatico, che effettua i controlli, segnalerà il comportamento al responsabile della struttura di appartenenza del dipendente il quale si attiverà per il procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L. del comparto sanità e dal regolamento aziendale. Tale segnalazione dovrà essere trasmessa anche alla Direzione Aziendale.
 5. Per il personale dirigente il comportamento andrà segnalato alla Direzione Aziendale per l'adozione degli atti di rispettiva competenza.
 6. Anche per il personale non dipendente il comportamento andrà segnalato al responsabile della struttura in cui svolge la propria attività tale personale per l'adozione degli atti di competenza, nonché alla Direzione Aziendale.
7. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 12 mesi, e sono periodicamente cancellati automaticamente dal sistema.
8. I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

Art. 11 – INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO INTERNET

1. Eventuali interruzioni del servizio sono comunicate agli utenti dalla Struttura Complessa Sistema Informatico.
2. Ai sensi del presente regolamento, l'utilizzo del servizio di accesso ad internet cessa d'ufficio nei seguenti casi:
 - se non sussiste più la condizione di lavoratore autorizzato o non è confermata l'autorizzazione all'uso o se la medesima è sospesa per un periodo uguale o superiore a sei mesi;
 - se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
 - se sono sospettate manomissioni e/o interventi su hardware e/o software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
 - in caso di diffusione o di comunicazione imputabili direttamente o indirettamente all'utente di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
 - in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
 - in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti;
 - in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

Art. 12 – NON OSSERVANZA DEL REGOLAMENTO

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

Art. 13 – INFORMATIVA (ai sensi dell'art. 13 D.L.vo 196/03)

1. L'ASL TO1 è Titolare del trattamento dei dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori.

FINALITA' del trattamento è la verifica del corretto utilizzo delle risorse informatiche, della posta elettronica e della rete internet nel rapporto di lavoro.

MODALITA' del trattamento: gli operatori della Struttura Complessa Sistema Informatico o personale tecnico esterno autorizzato dal Direttore della struttura medesima effettueranno il trattamento dei dati con strumenti informatici.

COMUNICAZIONE DEI DATI; il trattamento di verifica è effettuato con gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo lavoratore, la comunicazione, nel caso si accerti un uso indebito della singola postazione, sarà data al Direttore della Struttura alla quale appartiene il dipendente per la valutazione del caso sotto il profilo disciplinare.

DIRITTI DELL'INTERESSATO: il dipendente potrà far valere i diritti di cui all'art. 7 del D.L.vo 196/2003 con richiesta scritta.

Art. 14 – ENTRATA IN VIGORE E PUBBLICITA'

1. Il presente Regolamento entrerà in vigore dalla data di adozione dell'atto deliberativo di approvazione.
2. Copia del Regolamento oltre ad essere pubblicato sul sito Aziendale Intranet, verrà trasmesso alle Strutture Aziendali.

Art. 16 – DISPOSIZIONI FINALI

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