AZIENDA
ULSS 9
TREVISO

Regolamento per l'utilizzo dei sistemi informatici

ACCREDITATION CANADA
Accredited by ISQua
Accreditamento di eccellenza 2007-2010

INDICE

Premessa

Negli ultimi anni l'utilizzo di risorse informatiche (computer, periferiche, software, internet e interconnessioni con altri soggetti) da parte dell'Azienda Unita' Locale Socio Sanitaria n. 9 (d'ora in avanti Azienda ULSS9) è notevolmente aumentato sia in termini quantitativi che di complessità di tali strumenti messi a disposizione dei propri collaboratori. Tutto ciò ha avuto un'importante implicazione in termini di sicurezza, disponibilità ed integrità dei sistemi informativi dell'ente ed è pertanto necessario stabilire una serie di regole di comportamento che, nel rispetto della normativa in materia di protezione dei dati personali, garantiscano l'efficienza ed il corretto utilizzo delle risorse informatiche e aziendali.

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

Tuttavia proprio in considerazione della delicatezza dell'argomento e con riferimento alla normativa in tema di protezione dei dati personali l'attività di controllo deve essere rispettosa dei principi fondamentali di "proporzionalità" (art. 3), inoltre deve 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).

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'Azienda ULSS 9 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 Azienda ULSS 9, 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, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

Definizioni

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

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

Responsabili del trattamento sono le figure formalmente individuate dal titolare e preposte al trattamento di dati personali

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

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

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

Freeware è un software che viene distribuito in modo gratuito

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

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

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

1. Entrata in vigore del regolamento e pubblicità

1.1 Il nuovo regolamento entra in vigore il 1° aprile 2010.. 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. Pertanto si intende abrogato il precedente regolamento adottato con delibera n.1862 del 16 luglio 1998.

1.2 Copia del regolamento, oltre ad essere pubblicato nella intranet aziendale, verrà consegnato a ciascun dipendente che dovrà sottoscriverlo al momento dell'instaurazione del rapporto contrattuale o al momento della richiesta delle credenziali di autenticazione per l'accesso ai vari strumenti informatici.

2. Campo di applicazione del regolamento

2.1 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 (lavoratori somministrati, collaboratore a progetto, in stage, specializzandi, universitari, ecc.) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'ULSS 9.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, specializzando, consulente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

3. Utilizzo del Personal Computer

3.1 **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. Inoltre per i dipendenti pubblici, così come previsto dalla normativa di settore, è vietato un utilizzo a fini privati di materiali o attrezzature di cui dispone per ragioni di ufficio

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda ULSS 9 solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 L'Azienda ULSS 9 rende noto che il personale incaricato, anche dei servizi esternalizzati, che opera presso il servizio per l'informatica della stessa l'Azienda ULSS 9 è stato 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.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

3.4 Il personale incaricato del Servizio per l'informatica e dei servizi affidati in outsourcing ha la facoltà di collegarsi e visualizzare in remoto, previa comunicazione all'interessato, il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito il collegamento mediante dispositivi non aziendali alla rete aziendale salvo specifica richiesta da parte del responsabile del trattamento e conferma da parte del servizio per l'informatica. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio per l'informatica per conto dell'Azienda ULSS 9 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 Azienda ULSS 9 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.

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

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio per l'informatica nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 11 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 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, salvo indicazioni contrarie da parte dei responsabili del servizio stesso o del servizio per l'informatica. 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**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio per l'informatica, 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. Lo stesso dicasi nel caso di revoca e/o trasferimento.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio per l'informatica, 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, senza preventiva autorizzazione da parte del Servizio per l'informatica.

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

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

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

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione alla rete informatica è il personale incaricato del Servizio per l'informatica dell'Azienda ULSS 9.

5. Utilizzo della rete dell'Azienda ULSS 9

5.1 Per l'accesso alla rete dell'Azienda ULSS 9 ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

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

5.3 Le cartelle utenti presenti nei server dell'Azienda ULSS 9 sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio per l'informatica.

5.4 Il personale del Servizio per l'informatica può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve

essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili forniti dall'Azienda ULSS 9 (dischetti, CD e DVD riscrivibili, supporti USB, 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.

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

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

6.4 E' vietato l'utilizzo di supporti rimovibili personali, salvo i casi espressamente autorizzati dal Responsabile del servizio.

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

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dal Servizio per l'informatica e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 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.

7.3 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 o sottrazioni.

7.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, ecc.

7.5 I PC portatili vanno restituiti al Servizio per l'informatica al termine del rapporto.

8. Uso della posta elettronica

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

8.2 È fatto divieto di utilizzare le caselle di posta elettronica ***ncognome@ulss.tv.it*** [1] per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo punto 10.
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 filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio per l'informatica. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La conservazione on line è garantita per 6 mesi.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ULSS 9 ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse. Sono state attivate delle caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea.

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

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

8.8 Sarà comunque consentito al superiore gerarchico dell'utente preventivamente sentito l'utente, o comunque a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7 o assenza non programmata).

8.9 Il personale del Servizio per l'informatica o altro personale esterno a ciò incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.4.

[1] Ovvero potrà essere realizzato un sistema di indirizzi di posta elettronica condivisi tra più utenti (ad es. segdipalgot@ulss.tv.it al posto di un sistema basato sull'identità personale).

8.10 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dell'Azienda ULSS 9 potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate aziendale nei punti precedenti.

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo punto 10.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica);
- 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 d'ufficio e/o del Servizio per l'informatica 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 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 d'ufficio.

L'accesso, tramite internet, a caselle webmail di posta elettronica personale è consentito solo nel rispetto di quanto riportato al punto 10.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda ULSS 9 rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.L'azienda si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa e compatibili con le finalità non istituzionali di cui al successivo punto 10.

9.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio per l'informatica ai sensi del precedente punto 3.4, 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, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

10. Regolamentazione uso internet per finalità non istituzionali

10.1. L'Azienda USLL 9 , potrà consentire la consultazione di determinati siti internet e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano compatibili con le misure di sicurezza implementata a protezione del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi che l'utente ha nei confronti dell'ente. Al fine di contemperare le rispettive esigenze l'uso di internet per tali finalità è consentito da postazioni dedicate, individuate dalle Direzioni di Area con la collaborazione del Servizio per l'Informatica.

11. Protezione antivirus

11.1 Il sistema informatico dell'Azienda ULSS 9 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.

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

11.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio per l'informatica.

12. Utilizzo dei telefoni, fax, scanner e fotocopiatrici aziendali

12.1 **Il telefono aziendale affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.

Qualora venisse assegnato un cellulare aziendale all'utente,(la concessione dell'utilizzo del cellulare viene rilasciata dalla Direzione Generale) quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l'addebito delle chiamate personali.

12.2 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

12.3 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

12.4 È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

13. Osservanza delle disposizioni in materia di Privacy

13.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Disciplinare tecnico allegato al D.Lgs. n. 196/2003.

14. Accesso ai dati trattati dall'utente

14.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio per l'informatica 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.

15. Sistemi di controlli graduali

15.1 In caso di anomalie, il personale incaricato del servizio per l'informatica 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. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie e per i casi di particolare gravità solo su autorizzazione della Direzione.

15.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale.

17.2 Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data 1 aprile 2010

REVISIONI

Data	Revisione	Descrizione della Revisione
