REGOLAMENTO
PER L'UTILIZZO DEL SISTEMA INFORMATICO PROVINCIALE

CAPO I

INFORMAZIONI E NORME GENERALI

Art.1

Le informazioni formate, gestite e conservate dalla Provincia e i sistemi informatici a tale scopo utilizzati formano nel loro insieme il Sistema Informativo Provinciale. Tale Sistema è un patrimonio dell'Amministrazione. E' compito di ogni collaboratore operare preservando e valorizzando questo patrimonio.

Art. 2

Il Sistema Informatico Provinciale è costituito dall'insieme degli strumenti tecnologici di cui la Provincia dispone per il trattamento delle informazioni, come hardware (personal computers, server di rete, stampanti e periferiche varie) e software (programmi informatici di base e applicativi, database, ecc.) e reti telematiche.

Art.3

Tutti coloro che, per qualsiasi motivo, accedono al Sistema Informatico Provinciale, sono tenuti ad osservare le vigenti Leggi ed i regolamenti in materia.

Art.4

Il Sistema Informatico Provinciale può essere utilizzato dal dipendente unicamente per lo svolgimento di attività legate alla propria mansione ed ai propri incarichi.

Art.5

Gli strumenti informatici - personal computer, stampanti, programmi, supporti magnetici, materiale di consumo, ecc. - che la Provincia mette a disposizione degli utenti per lo svolgimento del proprio lavoro sono di esclusiva proprietà dell'Amministrazione e devono essere utilizzati unicamente per gli scopi della

stessa. E' quindi vietato l'utilizzo di attrezzature informatiche per scopi personali.

Art.6

L'Amministrazione si riserva la facoltà di ricorrere contro comportamenti da parte degli utenti in contrasto con le leggi vigenti o il presente Regolamento.

CAPO II

MISURE GENERALI DI SICUREZZA

Art.7

In linea generale tutte le attività e gli utilizzi dei sistemi informatici che non sono previsti e specificamente definiti non sono autorizzati.

Art.8

Le componenti del sistema informatico provinciale (hardware, software, reti) sono gestite unicamente dall' Ufficio Sistemi informativi in forma diretta o tramite soggetti (imprese, consulenti, ecc.) che operano su incarico e per conto dell'Ufficio medesimo. Nessun altro soggetto è autorizzato ad operare sul sistema informatico provinciale.

Art.9

Qualsiasi richiesta di intervento tecnico di qualsiasi natura a carico del sistema informatico provinciale deve essere gestita dal Ufficio Sistemi informativi. Non è permesso intervenire autonomamente o ricorrere in modo autonomo a prestazioni tecniche fornite da soggetti esterni.

Art.10

Ogni utente del Sistema Informatico Provinciale è tenuto ad osservare i comportamenti previsti dal presente Regolamento per garantire la massima sicurezza delle informazioni e l'integrità funzionale degli strumenti utilizzati.

Art.11

E' vietata l'installazione di programmi di qualsiasi genere o specie, se non dietro esplicita autorizzazione del Responsabile dell' Ufficio Sistemi informativi.

Art. 12

Ogni utente è tenuto a segnalare all'Ufficio Sistemi informativi qualsiasi malfunzionamento degli strumenti informatici in uso.

Non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti dei sistemi informatici, se non dietro esplicita autorizzazione e supervisione del personale appositamente preposto.

Art.13

La configurazione dei personal computer dell'Amministrazione è realizzata su un modello standard studiato per garantire la semplicità di gestione del parco macchine e la condivisione delle risorse informatiche tra tutti gli utenti del sistema informatico provinciale. Di conseguenza non è permesso modificare la configurazione hardware del proprio posto di lavoro. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax, e installare o disinstallare dispositivi hardware (banchi di memoria, schede, mouse, stampanti, ecc.).

Art. 14

Non è permesso modificare la configurazione software dei personal computer. In particolare sono tassativamente vietate l'alterazione dei parametri di configurazione del sistema operativo e qualsiasi variazione alla configurazione originale standard prevista ed implementata su tutti i personal computer dell'Amministrazione.

Art.15

Gli utenti che in seguito alla volontaria manomissione della propria postazione di lavoro provocheranno la perdita di dati o comunque malfunzionamenti a carico delle apparecchiature, saranno ritenuti responsabili degli eventuali danni subiti dall'Amministrazione.

CAPO III

L'ACCESSO AL SISTEMA INFORMATICO PROVINCIALE

Art.16

L'accesso al sistema informatico provinciale è consentito unicamente ai dipendenti

in possesso di credenziali di autenticazione rilasciate dall' Ufficio Sistemi Informativi. Per credenziale di autenticazione si intende l'insieme di identificativo utente e di parola chiave (password). Di norma l'identificativo utente è composto dal cognome dell'utente e dal nome uniti dal simbolo "_". Esempio: l'identificativo utente di Mario Rossi è "rossi_mario).

Art.17

Le credenziali di autenticazione sono personali e devono essere esclusivamente utilizzate dal titolare, il quale provvederà a custodire e a garantire la segretezza della parola chiave e a sostituirla almeno ogni tre mesi.

Art.18

L'identificativo utente è indispensabile per poter accedere al Sistema Informatico Provinciale. L'identificativo dell'utente deve infatti essere fornito all'avvio della sessione di lavoro. Esso permette al Sistema Informatico di riconoscere l'utente e di consentirne l'accesso alle risorse informatiche per le quali è autorizzato (cartelle su server di rete, accesso ad archivi, accesso a programmi, internet, posta elettronica, ecc.)

Art.19

Ciascun Dirigente è responsabile della gestione delle credenziali di autenticazione dei dipendenti della propria struttura, in particolare della richiesta di nuova credenziale e di revoca di credenziale esistente. Le richieste di rilascio o di revoca di credenziali di autenticazione devono essere inoltrate via e-mail al Dirigente dei Sistemi Informativi. Nella richiesta il Dirigente dovrà precisare a quali risorse informatiche l'utente è abilitato ad accedere, come ad esempio archivi (database), programmi, cartelle residenti su server di rete, internet, posta elettronica, ecc.).

Art.20

Non saranno prese in considerazioni richieste di credenziali di autenticazione formulate da soggetti diversi dal Dirigente o suo delegato.

Art.21

In caso di cessazione dal servizio o di trasferimento ad altra struttura di un dipendente in possesso di credenziali di autenticazione, il Dirigente responsabile

deve chiedere all'Ufficio Sistemi Informativi la revoca delle credenziali stesse. Il Dirigente è quindi responsabile di danni arrecati all'Amministrazione derivanti dall'accesso indebito ad archivi provinciali effettuato con credenziali di dipendenti non più in servizio e non revocate (Art. 169 L.196/03 "Codice in materia di protezione dei dati personali")

CAPO IV

UTILIZZO DELL'HARDWARE

Art.22

L' Ufficio Sistemi informativi provvede, direttamente o tramite gli uffici dell'Amministrazione preposti alle forniture, all'acquisto delle apparecchiature informatiche necessarie per l'informatizzazione degli Uffici Provinciali. La tipologia, la dotazione e la configurazione delle apparecchiature informatiche e dei posti di lavoro in generale sono definiti dall' Ufficio Sistemi informativi sulla base delle esigenze degli utenti e della integrazione e compatibilità col Sistema Informatico Provinciale.

Art.23

L'installazione, configurazione e manutenzione di tutte le componenti del Sistema Informatico Provinciale sono gestite dall'ufficio Sistemi Informativi.

Art.24

E' tassativamente vietato il collegamento al Sistema Informatico Provinciale di apparecchiature non di proprietà dell'Amministrazione o la connessione ad altre reti telematiche salvo specifica autorizzazione dell' Ufficio Sistemi informativi.

Art.25

Tutti i dispositivi utilizzati dagli utenti devono essere trattati con cura e deve essere segnalato qualsiasi malfunzionamento.

Art.26

Non è autorizzato lo spostamento di alcun strumento od accessorio fuori delle sedi provinciali, o tra sedi diverse, se non dopo esplicita autorizzazione da parte del

Dirigente di Settore competente sentito il parere del Responsabile dell' Ufficio Sistemi informativi.

Art. 27

Ogni utente deve procedere allo spegnimento dei dispositivi che ha in uso alla fine dell'orario lavorativo ed in tutti i casi di assenza prolungata dal proprio posto di lavoro, con esclusione delle postazioni che per ragioni di servizio devono rimanere sempre accese (es: server di rete).

Art.28

Imballi, confezioni dei dispositivi in uso, manuali d'uso e altri materiali di corredo dei dispositivi devono essere conservati o consegnati al personale dell' Ufficio Sistemi informativi, salvo diverse disposizioni dell'ufficio medesimo.

Licenze e documentazione di acquisto devono essere consegnate al personale dell' Ufficio Sistemi informativi che ne cura la conservazione ai fini amministrativi e di controllo.

Art.29

Non si deve procedere ad operare sulle connessioni elettriche o di rete, se non dietro specifica autorizzazione. In nessun caso si deve operare sulle connessioni elettriche o di rete quando i dispositivi sono in tensione.

Art.30

Gli utenti non sono autorizzati ad operare su dispositivi di rete, quali server, stampanti condivise, dispositivi di connessione (hub, armadi di rete, router, stampanti di rete).

CAPO V

UTILIZZO DEI PROGRAMMI APPLICATIVI (SOFTWARE)

Art.31

L'Ufficio Sistemi Informativi provvede all’acquisto delle licenze d’uso dei pacchetti applicativi necessari all’informatizzazione degli Uffici Provinciali.

Le caratteristiche del software applicativo acquistato sono definite dall'Ufficio Sistemi Informativi sulla base delle esigenze degli utenti e della integrazione e

compatibilità col Sistema Informatico Provinciale.

Art.32

Le licenze d'uso dei pacchetti applicativi installati dall'Ufficio Sistemi Informativi su ogni singolo computer sono di proprietà dell'Amministrazione. L'Amministrazione può sottoporre a mappatura le risorse informatiche in modo da aggiornarne periodicamente la dotazione . Ciò servirà in seguito e periodicamente a verificare l'esistenza di programmi in più o in meno rispetto a quelli forniti in partenza al ciascun dipendente.

Art. 33

Il datore di lavoro o il responsabile informatico, per tutelarsi contro la responsabilità di omissione di controllo dovrà sensibilizzare gli utilizzatori finali dei programmi, (i propri dipendenti, colleghi o collaboratori), attraverso la diffusione di indicazioni e policy aziendali sulla gestione dei programmi installati e sui rischi penali connessi all'uso indebito del mezzo informatico o alla riproduzione non autorizzata di software.

Art.34

I programmi applicativi sviluppati in proprio dall'Amministrazione attraverso i propri dipendenti o da terzi appositamente incaricati, al fine di soddisfare esigenze di informatizzazione delle attività degli uffici, sono di esclusiva proprietà dell'Amministrazione.

L'utilizzo di tutti i programmi applicativi è limitato ai casi ed agli scopi previsti dall'Amministrazione. Non è comunque consentito l'utilizzo di programmi applicativi per scopi personali.

Art.35

Non è consentito l'accesso a programmi od a parti di programmi applicativi cui non si è autorizzati, anche se non esistono misure tecniche a protezione delle stesse.

Art.36

Non è consentita l'esecuzione di alcuna modifica ai programmi applicativi se non,

in casi particolari, dopo esplicita autorizzazione del Responsabile dell'Ufficio Sistemi Informativi. In particolare non è consentito il cambio di versioni o di lingua, lo spostamento di dischi o cartella di installazione.

Art.37

E' vietata la duplicazione o copia parziale del software installato nel Sistema Informatico Provinciale, con esclusione delle copie di salvataggio effettuate dal personale dell'Ufficio Sistemi Informativi.

Art. 38

L'utente deve segnalare attraverso l'apposito software disponibile nella intranet interna, qualsiasi malfunzionamento od errore dei programmi applicativi in uso, agli addetti del Sistema Informatico; la segnalazione deve essere tempestiva e completa e, se possibile, deve evidenziare le condizioni in cui si è verificato l'errore.

CAPO VI

GESTIONE DEGLI ARCHIVI

Art. 39

Le informazioni prodotte dagli utenti (documenti, archivi, dati in generale) devono essere memorizzate unicamente sul dispositivo di rete (file server) appositamente configurato dall'Ufficio Sistemi Informativi, salvo specifiche diverse autorizzazioni scritte o per motivi legati alla conformazione della struttura della rete informatica.

Art. 40

L'Ufficio Sistemi informativi coordina le attività volte a garantire la sicurezza delle informazioni memorizzate sui server di rete attraverso periodiche copie di salvataggio degli archivi su dispositivi di backup secondari: memorie di massa, dischi e nastri, dedicati alla funzionalità di ripristino dati erroneamente cancellati o alterati e disaster recovery. Tale attività viene svolta direttamente dal personale dell'Ufficio medesimo.

Art.41

Sul File Server, nell'area identificata fra le risorse del computer con la mappatura di rete**“P:”,** vengono definiti per ciascun Settore/Ufficio una o più specifiche cartelle. Il Dirigente responsabile di ciascun settore indicherà, attraverso richiesta scritta via e-mail, al Dirigente dell'Ufficio Sistemi Informativi gli utenti che avranno il permesso di accedere e i relativi permessi (lettura e/o scrittura) a ciascuna delle cartelle appartenenti al suo Settore.

A disposizione dei singoli utenti vi è poi un'area sul File Server, identificata fra le risorse del computer con la lettera “H”: Homes., dove è possibile la gestione di documenti riservati.

Art.42

I singoli utenti sono responsabili della integrità e riservatezza delle informazioni memorizzate sui server di rete nelle cartelle alle quali hanno accesso.

Art. 43

Le informazioni eventualmente memorizzate sui dischi locali dei computer non sono protette e non vengono copiate durante l’esecuzione delle copie di salvataggio effettuate dall'Ufficio Sistemi Informativi. Gli utenti saranno responsabili della perdita dei dati eventualmente memorizzati su dispositivi locali rispondendo degli eventuali danni subiti dall’Amministrazione.

Art. 44

Gli utenti non sono autorizzati alla cancellazione di files o gruppi di files dei quali non conoscono scopo e/o contenuto. Gli utenti hanno la facoltà unicamente di cancellare dai dispositivi in loro uso i files che hanno personalmente creato rispondendo degli eventuali danni subiti dall’Amministrazione.

Art. 45

Non è consentita la copia di archivi contenenti dati dell’Amministrazione di qualsiasi genere o specie su dispositivi asportabili (floppy disk, CD/DVD, USB pen drive, nastri e simili) né su dispositivi di memorizzazione esterni all’azienda (ad esempio in server accessibili mediante Internet) se non per attività istituzionali e dietro esplicita autorizzazione dell’Amministrazione.

Art. 46

L'Ufficio Sistemi Informativi, nell'ambito delle proprie attività di gestione e manutenzione del parco macchine, effettua controlli periodici sui personal computer in uso agli utenti e in particolare sui dispositivi di memorizzazione locale. Gli archivi, i programmi installati e le modifiche alla configurazione del PC non precedentemente autorizzati saranno cancellati .

CAPO VI

RISERVATEZZA DELLE INFORMAZIONI

Art. 47

Il sistema informatico provinciale gestisce dati personali così come definiti dalla Legge 196/03 sulla tutela dei dati personali. Ogni comportamento da parte degli utilizzatori del Sistema informatico deve essere quindi conforme a quanto previsto dalla Legge e dai regolamenti.

Art. 48

Ogni utente ha accesso unicamente ai dati per i quali è stato autorizzato al trattamento. Questo si riferisce in generale a tutte le informazioni trattate dal Sistema Informativo Provinciale, ed in particolare ai dati personali, per i quali l'Amministrazione assicura l'osservanza delle normative di legge.

Art. 49

Tutte le informazioni dell'Amministrazione sono riservate all'utilizzo ed alla circolazione unicamente all'interno della Provincia, tranne nei casi diversi esplicitamente previsti.

Art. 50

Nessuna informazione deve essere trattata, comunicata e diffusa all'esterno della Provincia se non nei casi previsti dalla Legge o dai Regolamenti.

Art.51

L'utente può autonomamente modificare in qualsiasi momento la propria parola

chiave di accesso al sistema provinciale. Egli è comunque obbligato dalle leggi vigenti a cambiarla almeno una volta ogni tre mesi e in caso di violazione della sua segretezza.
L'utente che desidera modificare la parola chiave in uso deve seguire le procedure indicate dall'Ufficio Sistemi Informativi.

Art.52

I documenti riservati devono essere di norma custoditi su cartelle riservate dei server di rete.

Art. 53

E' vietata la cifratura di documenti effettuata autonomamente dal dipendente se non in casi particolari e con l'autorizzazione del Dirigente responsabile al quale deve comunque essere consegnata copia della chiave di cifratura.

Art.54

Ai sensi dell'Art.10 del Disciplinare tecnico allegato alla L.196/03, il Titolare e il Responsabile del Trattamento dati possono richiedere agli Amministratori dell'Ufficio Sistemi Informativi la disponibilità di dati o strumenti elettronici assegnati ad un dipendente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password del dipendente effettuata dall'Amministratore dei Sistemi Informatici che la comunica al Titolare/Responsabile. L'Amministratore che ha provveduto alla sostituzione della password comunica tempestivamente via e-mail al dipendente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

Art. 55

L'utilizzo improprio della parola chiave, ad esempio per occultare documenti od errori commessi è considerato illecito dall'Amministrazione, che è eventualmente autorizzata a procedere nei confronti dell'utente ai sensi del C.C.N.L. e delle leggi vigenti.

CAPO VII

UTILIZZO DI INTERNET

Art. 56

L'Amministrazione Provinciale mette a disposizione dei propri dipendenti l'utilizzo della navigazione Internet sulla base delle esigenze di ufficio e delle disposizioni emanate in materia dagli Organi competenti.

Art.57

L'abilitazione per il dipendente all'utilizzo della navigazione Internet deve essere richiesta per iscritto all'Ufficio Sistemi Informativi dal Dirigente responsabile via e-mail.

Art. 58

L'accesso alla navigazione internet avviene, per gli utenti abilitati, attraverso autenticazione su Proxy mediante lo stesso identificativo (nome utente e password) usato per l'accesso alle risorse informatiche dell'Amministrazione.

Art. 59

Non è consentito l'utilizzo dell'accesso ad internet per motivi personali.

Art. 60

L'Amministrazione non è responsabile di eventuali dati personali, anche di tipo sensibile, che potrebbero risultare automaticamente memorizzati all'interno di postazioni di lavoro assegnate ad utenti che, contravvenendo alla precedente disposizione, abbiano consultato per uso personale siti a carattere politico, sindacale o religioso.

Art.61

Non è consentito comunicare informazioni personali - anche se non riguardano l'Amministrazione - nei siti visitati durante la navigazione, eccetto che per motivi strettamente legati alla propria attività.

Art.62

E' tassativamente vietato il download (memorizzazione sul disco del proprio

computer o su altri dispositivi di memorizzazione, anche rimovibili) di files od archivi di qualsiasi genere trovati durante la navigazione su Internet, se non per motivi strettamente legati alla propria attività. In particolare è vietato il download di contenuti protetti dalle leggi sul diritto d'autore (software, brani musicali, films, fotografie, ecc.).

Art. 63

Non è ammessa la comunicazione di dati dell'Amministrazione in siti o sistemi di posta elettronica, se non dietro autorizzazione e per motivi direttamente collegati alla propria attività.

Art.64

L'Amministrazione adotta sistemi automatici di filtraggio degli indirizzi Internet (URL filtering) per impedire l'accesso da parte degli utenti a siti non di carattere istituzionale. Gli stessi sistemi regolamentano l'accesso ad Internet in base all'orario ed al giorno della settimana impedendo, di norma, l'accesso alla rete al di fuori dell'orario di servizio. Le modalità di filtraggio degli indirizzi internet possono essere diversificate in base a eventuali esigenze di servizio, che sono segnalate dai Dirigenti interessati al Responsabile dell'Ufficio Sistemi Informativi via e-mail.

Art. 65

L'Amministrazione può avvalersi dei medesimi sistemi di cui al punto precedente anche ai fini di documentare il traffico internet generato dalla stazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet che abbiano causato danni all'Amministrazione, o per controlli difensivi, oppure nell'ambito di indagini condotte dall'Autorità Giudiziaria.
La raccolta e la custodia sono effettuate nelle modalità previste dalla normativa vigente e la garanzia e tutela delle informazioni trattate saranno assicurate in osservanza delle disposizioni di Legge in materia di Privacy e degli atti emanati dal Garante.

Art. 66

Le informazioni di cui al punto precedente sono custodite per la durata massima indicata dalle leggi vigenti e poi sono distrutte. L'accesso ai dati è consentito

unicamente al Responsabile del trattamento dati e si effettuerà unicamente nei modi previsti dall'Art. 11 del D.Lgs. 196/03 ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

Art. 67

I sistemi informatici di cui sopra non sono in alcun modo abilitati al "controllo a distanza del lavoratore" e quindi non sono in contrasto con le norme contenute nello "Statuto dei Lavoratori"

CAPO VIII

UTILIZZO DELLA POSTA ELETTRONICA

Art. 68

L'Amministrazione Provinciale mette a disposizione dei propri dipendenti l'utilizzo di un sistema informatico di posta elettronica sulla base delle esigenze di ufficio e delle disposizioni emanate in materia dagli Organi centrali competenti .

Art.69

Non è permesso l'utilizzo delle caselle di posta fornite dall'Amministrazione per motivi personali.

Art. 70

Le caselle di posta elettronica sono di esclusiva proprietà dell'Amministrazione. Non è prevista la creazione di caselle e-mail per uso personale del dipendente.

Art. 71

Le caselle possono essere intestate a Settori, Servizi, UC, singole unità operative e singoli dipendenti. Alle caselle dei Settori, Servizi, UC, singole unità operative potranno accedere singoli dipendenti o gruppi di dipendenti a seconda delle esigenze organizzative. In caso di accesso alle caselle di ufficio consentito a gruppi di utenti, i singoli utenti che ne fanno parte saranno individuati dal dirigente responsabile.

Art. 72

Le caselle possono essere intestate a singoli utenti. L'assegnazione di una casella

di posta elettronica con un indirizzo riportante il nome del dipendente non sottintende un uso personale della stessa come evidenziato dal nome del dominio (provincia.vicenza.it) e quindi la “personalità” dell’indirizzo non implica “privatezza” dello stesso.

Art. 73

La creazione di un nuovo indirizzo di posta elettronica deve essere richiesto dal Dirigente responsabile per iscritto all'Ufficio Sistemi Informativi via mail, specificando il nominativo del dipendente cui è assegnato (referente) o il gruppo di nominativi che dovranno accedervi, specificando anche in questo caso un referente principale.

Art.74

Il Dirigente responsabile dovrà tempestivamente richiedere per iscritto o via mail all'Ufficio Sistemi Informativi la chiusura di caselle personali per cessazione dal servizio o trasferimento del dipendente oltreché la chiusura di indirizzi di ufficio non più utilizzati. Dovrà altresì fare richiesta nel caso vi siano variazioni nella composizione del gruppo di utenti che accedono alle caselle di ufficio.
Le caselle chiuse, vengono definitivamente cancellate dall'Ufficio Sistemi Informativa dopo 30 gg. dalla richiesta di chiusura

Art.75

Il contenuto delle caselle di posta elettronica viene conservato sul server, al fine di consentire il regolare backup della posta, quindi l'accesso avverrà esclusivamente via protocollo IMAP o mediante l'utilizzo del web client in uso all'Amministrazione. L'accesso attraverso protocollo POP3 e il conseguente scaricamento della posta sul PC in locale è bloccato.

Art. 76

I referenti devono provvedere a eliminare periodicamente i messaggi più vecchi, ovvero a salvare su server di rete gli allegati per evitare la saturazione dello spazio della casella.

Art. 77

L'invio di messaggi che configurano impegni per la Provincia (come ad esempio ordini a fornitori, ecc.) deve sempre seguire la procedura di approvazione prevista

ed in particolare l’apposizione della segnatura di protocollo; non è permesso utilizzare il sistema di posta elettronica per modificare le procedure esistenti, neanche nei casi di particolare urgenza.

Art. 78

Per motivi di sicurezza informatica è vietato l'utilizzo di caselle personali di posta elettronica esistenti presso domini esterni ed accessibili via browser utilizzando i sistemi dell’Amministrazione .

Art. 79

Non è ammessa la comunicazione di dati aziendali in siti o sistemi di posta elettronica, se non dietro autorizzazione e per motivi direttamente collegati alla propria attività.

CAPO IX

PROTEZIONE ANTIVIRUS

Art. 80

Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico provinciale da parte di virus o di ogni altro software che operi con lo scopo di superare le difese di sicurezza del sistema stesso.

Art.81

Ogni utente è tenuto a controllare il regolare funzionamento ed aggiornamento del software antivirus installato, secondo le procedure definite dal Servizio Informatica.
Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto all'Ufficio Sistemi Informativi.

Art.82

E' consentito l'utilizzo di dispositivi asportabili (floppy disk, CD/DVD, USB pen drive, nastri e simili) anche non provenienti dall’Amministrazione solo per finalità di

servizio. Ogni dispositivo magnetico dovrà essere verificato mediante il programma antivirus prima del suo utilizzo, e, nel caso in cui venissero rilevati virus, dovrà essere segnalato all'Ufficio Sistemi Informativi per la sua verifica/pulizia.

Art. 83

Si consiglia di evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile. Si consiglia inoltre di non aprire files allegati ad e-mail provenienti da utenti sconosciuti.

CAPO X

ACCESSO AD ARCHIVI CONTENENTI DATI PERSONALI (D.LGS. 196/03 "CODICE SULLA PRIVACY")

Art.84

La Provincia di Vicenza, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di Privacy. A tal proposito la Giunta Provinciale ha nominato Responsabili del Trattamento dei dati i Dirigenti di Settore ognuno per gli archivi di propria competenza.

Art.85

L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli utenti autorizzati, detti anche Incaricati del Trattamento dati.
L'accesso viene consentito attraverso specifiche abilitazioni dell'Identificativo e della password dell'utente.

Art.86

Gli Incaricati del trattamento dei dati sono individuati e nominati direttamente dal Responsabile del trattamento sulla base dell'analisi delle esigenze di servizio del Settore.

All'atto della nomina, gli Incaricati del trattamento riceveranno precise indicazioni sul tipo di trattamento dei dati che sarà loro consentito (lettura, modifica, cancellazione, stampa, esportazione, importazione).

Art.87

Nella gestione di archivi tutelati dalla normativa sulla Privacy gli Incaricati dovranno attenersi a quanto previsto dal proprio Responsabile del trattamento. In particolare l'accesso ad archivi contenenti dati personali deve essere tassativamente circoscritto alle sole informazioni strettamente necessarie per adempiere ai compiti loro assegnati.

Art.88

L'incaricato del trattamento di dati personali non può allontanarsi dal proprio posto di lavoro anche per brevi periodi senza aver prima chiuso la propria sessione di lavoro ("logoff" o "chiudi sessione").

CAPO XI

TUTELA DEL PATRIMONIO DELL'ENTE E RISPETTO DELLA RISERVATEZZA E DELLA DIGNITA' DEL LAVORATORE

Art.89

La politiche dell'Amministrazione in materia di tutela del patrimonio dell'Ente e di rispetto della riservatezza e della dignità del lavoratore applicano la normativa italiana e comunitaria.

L'Amministrazione, nella gestione del sistema informatico provinciale, opera ricercando un bilanciamento tra il diritto alla riservatezza dei lavoratori e gli interessi legittimi dell'Ente e tra questi ultimi il diritto di tutelarsi contro le responsabilità e i danni cui possono dare origine gli atti dei lavoratori. Tale bilanciamento è attuato in base a principi di proporzionalità e di trasparenza delle azioni e delle misure adottate nei confronti dei lavoratori. Altro principio guida è quello della prevenzione di atti o comportamenti illeciti o cioè riguarda quelle azioni messe in atto dall'Ente orientate a prevenire comportamenti illeciti che possono avere conseguenze dannose evitando così il ricorso a restrizioni drastiche nell'uso degli strumenti informatici o alla sorveglianza individuale e continuativa.

Art.90

I sistemi informatici provinciali ed in particolare quelli preposti al trattamento dei dati personali o delle informazioni pubblicate su Internet (server web), raccolgono informazioni tecniche (log monitoraggio) riguardanti l'utilizzo delle apparecchiature. Tali informazioni sono utilizzate per la tutela del sistema informatico provinciale al fine di identificare accessi e utilizzi illeciti ai sistemi ed alle informazioni e consentire l'adozione di adeguate misure di sicurezza informatica. L'implementazione di questi sistemi di monitoraggio è attuata in osservanza all'Art.33 del D.Lgs. 196/03 ed alle specifiche tecniche internazionali in materia di sicurezza informatica (ISO 27000).

Art.91

I controlli effettuati dall'Amministrazione utilizzando le informazioni di cui all'articolo precedente saranno attuati solamente ex-post, per soddisfare innanzitutto esigenze statistiche di controllo di sicurezza del funzionamento del sistema informatico e ai fini del controllo della spesa per servizi telematici. Potranno essere inoltre utilizzati per la individuazione di accessi non autorizzati a sistemi ed informazioni o di comportamenti illeciti evidenziati dalla presenza nei sistemi informatici di virus, programmi software o altro materiale protetto da diritti d'autore (brani musicali, films, ecc.) privi di licenza d'uso. Tali verifiche sono effettuate "ex post" ai fini del cosiddetto controllo difensivo escludendo qualsiasi forma di controllo continuativo a distanza del lavoratore.

Le fattispecie oggetto di controllo difensivo sono quelle disciplinate dal Codice Penale in materia di reati informatici ed in particolare: Art. 420 C.P. "Attentato ad impianti di pubblica utilità", Art. 615 ter "Accesso abusivo ad un sistema informatico", Art. 615 quinquies "Diffusione di programmi diretti ad interrompere o a danneggiare un sistema informatico", Art. 635 bis "Danneggiamento di sistemi informatici e telematici"

Art. 92

L'esercizio dei controlli difensivi sono attuati secondo i citati principi di gradualità e proporzionalità e prendono il via da controlli di tipo statistico su informazioni di tipo anonimo (es: numero e durata delle connessioni per settore, per ufficio, ecc.) e solo in caso di accertata violazione di legge o di danno per l'Amministrazione

possono riguardare altre informazioni che sono sempre trattate secondo i principi di pertinenza e non eccedenza.

La custodia delle informazioni tecniche (log monitoraggio) riguardanti l'utilizzo dei sistemi è assicurato dal Responsabile del Trattamento dati e cioè dal Responsabile dell'Ufficio Sistemi Informativi, che previene qualsiasi accesso illecito a tali dati. A tal proposito sono adottate adeguate misure di sicurezza informatica.