PROVINCIA DI AREZZO
Decorata di Medaglia d'Oro al V.M. per attività partigiana

Disciplina aziendale per l'utilizzo dei sistemi informatici (Rev. 1.0)

APPROVATO CON DELIBERAZIONE . GP 26 DEL 17.1.2005

Sommario

PROVINCIA DI AREZZO
Decorata di Medaglia d'Oro al V.M. per attività partigiana

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone la Provincia di Arezzo a rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza ed all'immagine dell'Amministrazione stessa.

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

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 196/03 sulla privacy e del relativo disciplinare sulle misure minime di sicurezza.

Termini utili ed abbreviazioni

Account: Una registrazione tenuta su reti locali e con sistemi operativi multiutente, di ciascun utente autorizzato dal sistema a scopi identificativi, gestionali e di sicurezza.
Amministratore di Sistema: Responsabile della U.O. Informatica o un suo delegato.
Amministrazione: Amministrazione Provinciale di Arezzo
Autorizzazione esplicita: Richiesta scritta indirizzata al Responsabile della U.O. Informatica
Chiave PGP: Acronimo di Pretty Good Privacy. Programma per la crittografia a chiave pubblica
Criptazione: Utilizzo di codici per convertire dati in modo che possano essere letti solo da uno specifico destinatario, usando una chiave
Dischi flash: Tipo di memoria non volatile
Firewall: Sistema di sicurezza volto a proteggere la rete di un'organizzazione dalle minacce esterne, per esempio gli hacker, provenienti da un'altra rete, per esempio Internet
Freeware: Programma per computer fornito gratuitamente
Log: Archivio elettronico (file) dove vengono registrate dal sistema le attività compiute
Newsgroup: Forum in Internet per discussioni concatenate riguardo una specifica varietà di argomenti
PC: Personal Computer
Shareware: Software coperto da copyright, distribuito sulla base di "una prova prima dell'acquisto"
Spamming: Attività di invio di materiale pubblicitario non richiesto a numerose caselle di posta elettronica
Spyware: un piccolo programma in esecuzione nel vostro computer, in grado di raccogliere a vostra insaputa svariate informazioni personali come il vostro nome utente, la vostra Email, quali file prelevate dal Web oppure che tipo di pagamenti avete effettuato con la carta di credito
Virus: Programma che "infetta" i file di un calcolatore inserendovi copie di se stesso

1.FINALITA' DELLA DISCIPLINA

1.1 Il presente disciplinare viene adottato dall'Amministrazione Provinciale per salvaguardare il buon funzionamento di un fondamentale strumento di lavoro quale è la rete aziendale nonché per la tutela da possibili responsabilità derivanti dall'utilizzo degli strumenti informatici di sua proprietà.

1.2 Nel rispetto della privacy degli utenti l'Amministrazione rinuncia all'impiego di programmi che rilevano sistematicamente e continuativamente (software di sniffing) tutte le attività in rete dei computer, registrando unicamente i log di connessione.

1.3 Solo in casi di malfunzionamento della rete verificabile attraverso i log di connessione, l'Amministratore di Sistema potrà attivare la consultazione dei log di dettaglio delle connessioni effettuate da parte degli utenti, al fine di garantire la salvaguardia dell'intero sistema informativo nonché la tutela per responsabilità indiretta derivante da eventuali illeciti. Ciò nel pieno rispetto dei diritti dei dipendenti e, in particolare, delle disposizioni contenute negli artt. 4 e 8 dello Statuto dei Lavoratori (L. 20/5/70, n. 300).

1.4 I dati raccolti saranno conservati in una banca dati elettronica, collocata nei locali della U.O. Informatica, visionabile solo da parte dell' Amministratore di Sistema

.

2 . Utilizzo del Personal Computer (fisso o mobile)

2.1 Il datore di lavoro deve fornire ad ogni dipendente, secondo quanto stabilito dalla Direttiva del 27 novembre 2003 della Presidenza del Consiglio dei Ministri, Dipartimento per l'innovazione e le tecnologie, una casella di posta elettronica personale. Inoltre deve dotare il dipendente degli strumenti informatici necessari allo svolgimento dei compiti assegnatigli sulla base della valutazione del Dirigente del Servizio presso cui il Dipendente presta la propria attività.

2.2 Non è consentito installare autonomamente software non standard, se non previa autorizzazione esplicita dell'Amministratore di Sistema, perché sussiste il grave pericolo di introdurre Virus informatici o similari e di alterare la stabilità delle applicazioni dell'elaboratore.

2.3 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dalla Provincia di Arezzo (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore). L'elenco del software di base distribuito viene approvato periodicamente dal Servizio Informatica con determinazione dirigenziale.

2.4 Non è consentito all'utente modificare le caratteristiche e configurazioni impostate sul proprio PC, se non previa autorizzazione esplicita dell'Amministratore di Sistema, nonché svolgere qualsiasi attività che produca: spreco di risorse di rete o del personale addetto al suo funzionamento, interferenza nel lavoro di altri utenti, usi che impediscano l'utilizzo del servizio da parte di altri utenti, altri usi impropri quali la diffusione di "Virus".

2.5 Il PC deve essere spento ogni sera prima di lasciare i locali di lavoro o in caso di assenze prolungate. Lasciare un PC acceso e 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

2.6 Non è consentita l'installazione sul PC affidato di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, dischi flash o comunque estraibili), se non con l'autorizzazione espressa dell'Amministratore di Sistema.

2.7 Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC (art. 5 del DPR 318/99).

2.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo Art. 8 del presente regolamento relativo alle procedure di protezione antivirus.

2.9 Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

2.10 Non è consentito sui PC dotati di scheda audio e/o di lettore CD/DVD l'ascolto di programmi, files audio o musicali e la visione di filmati non a fini prettamente lavorativi.

2.11 Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

2.12 Non è consentito installare prodotti di sicurezza attiva e passiva quali firewall, compressori con chiavi PGP, utilità per la criptazione di dati o similare se non espressamente autorizzati dall'Amministratore di sistema.

2.13 L'Amministratore di Sistema può in qualunque momento, dando opportuno preavviso, laddove possibile, 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 effettuando un sintetico report sull'attività svolta.

2.14 Non è consentito lo spostamento di componenti informatiche senza l'autorizzazione dell'Amministratore di Sistema.

3. Utilizzo della rete aziendale

3.1 Le unità di rete 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 da parte dell'Amministratore di Sistema.

3.2 Non e' consentita la creazione e condivisione di cartelle salvo che queste siano in sola lettura protetta da password per il solo scambio di file tra computer.

3.3 Non è consentita la condivisione di archivi (basi di dati) se non espressamente autorizzate dall'Amministratore di Sistema.

3.4 Le password d'ingresso alla rete, ai programmi ed alle risorse condivise sono segrete e vanno comunicate e gestite secondo le procedure impartite nell'art. 5. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

3.5 Costituisce buona regola la periodica (almeno ogni tre mesi) pulizia degli archivi, ovvero la cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

3.6 E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3.7 Non è consentito utilizzare software per controllo remoto di altre risorse collegate alla rete. In particolare è vietato l'utilizzo di prodotti quali VNC, PC-anyware, Net-Meeting o similare senza espressa autorizzazione da parte dell'Amministratore di Sistema.

3.8 Non è consentito operare per attività di tele assistenza tramite connessioni modem (analogico e digitale) su dispositivi collegati alla rete aziendale. Per le modalità e le regole legate alla tele assistenza prendere direttamente contatto con l'Amministratore di Sistema.

3.9 Non è consentita nessuna forma di predisposizione del PC per servizi di accesso remoto, ovvero non deve esistere possibilità di accesso dall'esterno alla rete aziendale, che si potrebbe trovare, altrimenti, a consentire manipolazioni dei dati a personale non autorizzato.

4. Procedure di controllo

4.1 Il PC affidato al dipendente è uno strumento di lavoro che il dipendente è tenuto ad utilizzare correttamente avendo cura e custodia delle componenti hardware, software e dati ivi memorizzati. Non è consentito l'utilizzo degli strumenti informatici forniti dall'Ente per scopi non inerenti all'attività lavorativa e pertanto qualunque documento memorizzato in qualsiasi formato non è da considerarsi riservato personale.

4.2 L'Amministratore di Sistema è deputato al controllo della funzionalità del sistema informativo. Le verifiche di routine o dietro segnalazione di malfunzionamento prevedono il controllo dei log di connessione al fine di evidenziare siti che notoriamente inviano spyware sui pc o che comunque provocano un elevato traffico. In caso di riscontro positivo è necessario individuare il/i pc destinatari di tali software al fine di rimuovere il virus.

4.3 L'Amministratore di Sistema per l'espletamento delle sue funzioni, ha la facoltà, ogni qualvolta se ne presenti la necessità, di attivare i log di dettaglio, ivi compresi gli archivi di posta elettronica interna ed esterna o i log di accesso ad Internet, al fine di individuare le cause che provocano rallentamenti, malfunzionamenti o difficoltà di accesso a Internet. Questi controlli verranno effettuati per assicurare la perfetta funzionalità del sistema. In tali occasioni potrà essere rilevato quanto segue:

- accessi a siti che potrebbero essere visitati per scopi non istituzionali. Tale rilevazione verrà effettuata esclusivamente perché l'accesso ha causato elevato traffico, ha provocato lo scarico di spyware o per tutela dell'Amministrazione per responsabilità indiretta per eventuali illeciti. Nel caso di accesso a questi siti apparentemente non istituzionali, verranno individuati gli utenti che vi hanno acceduto e ne verrà data comunicazione al Dirigente del Servizio presso quale il dipendente presta la propria attività lavorativa affinchè assuma le informazioni del caso e adotti – eventualmente – opportuni provvedimenti.
- accessi a siti istituzionali che hanno provocato elevato traffico. In questo caso, l'Amministratore di Sistema prenderà i necessari accordi direttamente con l'utente dopo averlo individuato, per concordare con esso le necessarie procedure per evitare che tali accessi possano provocare rallentamenti o quant'altro.

4.4 L'attività di controllo, oltre quanto detto al punto 2.2, prevede due fasi: la prima in cui verrà effettuata la lettura del file di log dove sono memorizzati i dati relativi agli accessi ai singoli siti (nome sito, indirizzo, data, durata totale e traffico effettuato in bytes). In base a questa analisi, se si verificano le situazioni sopra previste, si analizza il log di dettaglio, dove vi sono le informazioni relative all'indirizzo di chi ha effettuato tali visite, la durata, la data e l'ora. L'attività di controllo nel caso in cui abbia comportato la necessità di accedere ai log di dettaglio verrà conclusa con la redazione di un verbale

in cui verranno riportate oltre alla data e l'ora del controllo, anche eventuali situazioni anomale riscontrate. Tale verbale verrà inviato al Direttore Generale.

4.5 I log memorizzati solo su supporto magnetico/ottico, verranno conservati per almeno 18 mesi – come attualmente auspicato dalla Comunità Europea – o per il periodo temporale previsto da normative nazionali o comunitarie successivamente approvate, in apposita cassaforte.

5 Gestione delle Password

5.1 Le password di ingresso alla rete, di accesso ai programmi, di condivisione, dello screen saver e di accensione del PC, devono essere utilizzate. È consentita l'autonoma gestione da parte degli utenti che le devono mettere a disposizione del Dirigente del Servizio come stabilito dal DPS approvato con provvedimento del Segretario Generale n.331 del 30/06/2004

5.2 Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema.

5.3 Regole minime di sicurezza prevedono l'utilizzo delle password per un massimo di 3 mesi, trascorsi i quali le stesse devono essere sostituite.

5.4 La password deve essere immediatamente sostituita, dando comunicazione all'Amministratore di Sistema, nel caso si sospetti che la stessa abbia perso la segretezza.

5.5 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all' Amministratore di Sistema.

6 Utilizzo dei supporti magnetici e telematici

6.1 Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (art. 7 del DPR 318/99). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

6.2 I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

6.3 Non è consentito scaricare (download) archivi, programmi o dati contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria attività lavorativa.

6.4 Non è consentito salvare (upload) archivi, programmi o dati su supporti magnetici/ottici e trasportati all'esterno delle strutture (edifici) aziendali. Qualora esista la necessità di portare all'esterno dati di proprietà dell'Amministrazione, l'attività deve essere autorizzata dal Dirigente del Servizio interessato.

6.5 Esistono situazioni di periodico invio di dati da e per altri Enti/Aziende. Tali flussi di dati devono avere autorizzazione amministrativa (come ad esempio le leggi regionali che regolano i flussi DOC) o scaturire da obblighi normativi vigenti (come ad esempio i rapporti con Ministeri, Agenzia delle Entrate, Enti Previdenziali) e devono avere modalità tecnologiche note all'Amministratore di Sistema. Qualsiasi modifica strutturale nella gestione tecnologica di detti flussi deve essere comunicata tempestivamente all'Amministratore di Sistema.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dall'Amministrazione 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 per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno (convegni, visite ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.

7.4 Non è consentito l'utilizzo di risorse di rete o di software aziendali con PC portatili personali o con altre apparecchiature non di proprietà della Provincia di Arezzo se non espressamente autorizzate dall'Amministratore di Sistema.

7.5 I PC portatili aziendali non possono essere utilizzati con configurazioni di rete già assegnate ad altro dispositivo. L'Amministratore di Sistema provvederà ad assegnare specifiche configurazioni.

8. Uso della posta elettronica

8.1 La casella di posta, assegnata dall'Amministrazione all'utente, è uno strumento di lavoro per cui la posta ivi ricevuta non è da considerarsi corrispondenza privata. Ogni messaggio di posta elettronica in quanto attinente all'attività lavorativa, può essere reso pubblico in ogni momento. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 E' fatto divieto di utilizzare le caselle di posta elettronica aziendale del dominio provincia.arezzo.it (……@provincia.arezzo.it) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione dell'Amministratore di Sistema.

8.3 E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Ad ogni connessione, l'utente è tenuto a scaricare la posta dal server aziendale, in modo da non occupare inutilmente lo spazio disco del server stesso.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti per la Provincia di Arezzo, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dall'Amministratore di Sistema. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

8.5 E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta). La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati" o che contengano dati soggetti alla normativa sulla privacy.

8.6 Per la trasmissione di file all'interno dell'Amministrazione è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. L'invio di file di grosse dimensioni allegati ai messaggi, deve essere utilizzata con parsimonia; inoltre avendo uno spazio limitato sul server (5Mb per utente), inviare un numero cospicuo di allegati potrebbe saturare tale spazio non permettendo di ricevere ulteriori messaggi. L'Amministratore di Sistema può autorizzare il superamento dei limiti di dimensione e di capienza.

8.7 E' obbligatorio controllare gli allegati di posta elettronica prima del loro utilizzo (non eseguire download di files eseguibili o documenti da siti Web o Ftp non conosciuti). Tale comportamento previene l'introduzione di virus o similari nel proprio PC e nella rete aziendale.

8.8 E' vietato partecipare a catene telematiche (cosiddette di Sant'Antonio). Se si dovessero ricevere messaggi di tale natura, si deve dare comunicazione immediatamente all'Amministratore di Sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi.

8.9 E' buona norma inviare messaggi sintetici; indicare sempre l'oggetto (subject) chiaramente in modo tale che il destinatario possa immediatamente individuare l'argomento della mail ricevuta. In caso di utilizzo di firma nella e-mail, questa deve essere breve e significativa riportando gli estremi del mittente (nominativo, indirizzo, telefono, fax ecc.). In caso di richiesta di ricevuta confermare l'avvenuta lettura.

8.10 E' vietato l'invio di posta elettronica con contenuti diffamatori, scandalosi, o con informazioni che violino la privacy di soggetti senza la loro autorizzazione; l'invio di posta elettronica con l'intenzione di procurare stress emotivo al destinatario o a terze persone; qualunque forma di violazione di diritti d'autore, di marchio registrato o, in generale, violazione dei diritti della proprietà intellettuale.

8.11 E' vietato utilizzare messaggi di posta elettronica privi del proprio indirizzo per mandare a terzi pubblicità; produrre attività di spamming, ovvero mandare materiale pubblicitario non richiesto a numerose caselle di posta elettronica o a newsgroups, creando in generale un elevato volume di posta in uscita.

8.12 E' vietato mandare messaggi oltraggiosi e/o offensivi per provocare numerose riposte; iscrivere, senza autorizzazione, terzi ad una o più mailing list.

8.13 E' vietata la configurazione sul PC di account di posta elettronica che non facciano riferimento al dominio aziendale (provincia.arezzo.it).

8.14 E' vietata la configurazione del client di posta elettronica per l'accesso a newsgroup esterni. Qualora, per esigenze di servizio, fosse necessario l'accesso a determinati newsgroup, deve esistere un'autorizzazione dell'Amministratore di Sistema.

8.15 Potranno essere effettuati controlli dei log del server di posta qualora si verifichino segnalazioni di invii di posta non conforme a quanto sopra elencato, finalizzati all'individuazione dell'utente e della stessa posta inviata. Tutto ciò verrà segnalato al Dirigente del Servizio presso quale il dipendente presta la propria attività lavorativa affinchè assuma le informazioni del caso e adotti – eventualmente – opportuni provvedimenti.

9. Uso della rete Internet/Intranet e dei servizi correlati

9.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Per tale motivo il firewall della Provincia provvede a verificare e bloccare gli accessi a siti con contenuti ritenuti inappropriati. In caso di necessità il Dirigente del Servizio potrà richiedere la rimozione di tali blocchi per le postazioni che ne hanno bisogno.

9.2 Le eventuali violazioni rilevate in seguito ai controlli sulla funzionalità del sistema effettuati secondo le modalità descritte ai punti 3.2, 3.3 e 3.4 saranno comunicate al Dirigente del Servizio competente, per gli opportuni provvedimenti.

9.3 E' fatto divieto all'utente di scaricare software, anche se gratuito (freeware e/o shareware), prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema. Sono fatti salvi gli aggiornamenti di software gestionali in uso presso l'Amministrazione e per i quali esiste una autorizzazione preventiva.

9.4 E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dall'Amministratore di Sistema e con il rispetto delle normali procedure di acquisto.

9.5 E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

9.6 E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche, canali IRC, software peer to peer e le registrazioni in guest books anche utilizzando pseudonimi (nicknames).

9.7 E' vietata ogni forma di utilizzo finalizzata alla distribuzione o copiatura di software coperto da diritto d'autore senza autorizzazione; arrecare molestie, o frodare o pubblicare e diffondere materiale osceno o pornografico, o promuovere l'uso di droghe o del gioco d'azzardo e ogni altra forma di attività illecita.

9.8 E' vietato ogni tentativo di intrusione verso risorse protette o accedere ad informazioni riservate senza autorizzazione.

9.9 E' obbligatorio che il software di navigazione (browser) installato nel PC abbia come pagina predefinita di ingresso la pagina iniziale della Intranet aziendale, vista la presenza nella pagina stessa di news e comunicazioni importanti per l'utenza, nonchè degli aggiornamenti antivirus.

10. Protezione antivirus

10.1 Ogni utente deve tenere comportamenti tali da ridurre al minimo il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

10.2 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato, secondo le procedure previste.

10.3 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer; scollegare il computer dalla rete aziendale; procedere alla rimozione del virus stesso; informare dell'accaduto l'Amministratore di Sistema.

10.4 L'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota comporta un elevato rischio di introduzione di virus informatici. Tale utilizzo deve quindi essere evitato, oppure, qualora assolutamente necessario, attuato con estrema attenzione.

10.5 Ogni dispositivo magnetico di provenienza esterna all'Amministrazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di Sistema.

11. Osservanza delle disposizioni in materia di Privacy

11.1 E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nel documento programmatico sulla sicurezza predisposto dal proprio Servizio. L'Amministrazione si riserva di mettere in atto tutto ciò che serve a controllare l'osservanza di queste disposizioni.

12. Non osservanza della presente normativa aziendale

12.1 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 a tutela dell'immagine e dei diritti della Provincia di Arezzo.

13. Aggiornamento e revisione

13.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente regolamento. Le proposte verranno esaminate dall'Amministratore di Sistema e, se opportune, saranno presentate alla Giunta provinciale per la necessaria adozione.

13.2 Il presente regolamento è soggetto a revisione e l'adozione di nuove revisioni sarà segnalata nella Intranet aziendale.

Software standard da installare su ogni macchina nuova:
Antivirus
Winzip
AcrobatReader
OpenOffice
SuS1.exe

Regole per la creazione posta elettronica
Naming convention delle caselle
Richiesta scritta da Uff.Pers. per personale tempo indeterminato, da dirigente (il quale si impegna a comunicare la data di licenziamento) per personale a tempo determinato. Per personale a convenzione o a progetto non si crea.
Caselle a nome ufficio o progetto o per manifestazioni (es.ced oppure progettoscuola oppure lupo, ecc): richiesta fatta da dirigente servizio per scritto; nella richiesta specificare data di inizio e di fine oltre la quale si elimina.