Azienda pubblica di servizi alla persona

"OPERA PIA COIANIZ" – TARCENTO

REGOLAMENTO PER L'UTILIZZO DELLA RETE INFORMATICA

determinazione del Direttore Generale n. 79 del 25 giugno 2012

Art. 1 - Oggetto

1. Questo regolamento, ispirato alle Linee guida del Garante della protezione dei dati personali (deliberazione n. 13 del 1.03.2007) ed alla Direttiva del Dipartimento della Funzione Pubblica n. 2 del 26.05.2009, intende fornire in modo trasparente ed esauriente un'informativa sull'uso degli strumenti informatici, di Internet e della posta elettronica, affinché il personale aziendale sia sensibilizzato ad un uso corretto di questi servizi, nonchè sia informato sulle politiche di sicurezza adottate dall'Azienda, per evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
2. Le prescrizioni qui contenute si aggiungono ed integrano le specifiche istruzioni già riportate nella "*Lettera di conferimento alla Sua persona di un incarico, nell'ambito del trattamento dei dati personali, ai sensi dell'articolo 30 D. Lgs. 196/2003*", consegnata a suo tempo agli incaricati di ruolo amministrativo.
3. La *Rete Informatica* dell'Opera Pia Coianiz è costituita dalle Risorse informatiche strutturali e dal Patrimonio informativo digitale:
   - le *risorse informatiche* sono le componenti hardware/software e gli apparati elettronici collegati alla Rete Informatica aziendale e componenti il sistema di trasmissione, ricezione ed elaborazione digitale del patrimonio informativo;
   - il *patrimonio informativo* è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Art. 2 - Principi generali - Diritti e responsabilità

1. L'utilizzo della rete informatica dell'Azienda pubblica di servizi alla persona "OPERA PIA COIANIZ" deve sempre ispirarsi al principio della diligenza e correttezza ed è consentito solo al personale autorizzato e per l'esclusivo svolgimento delle proprie mansioni.
2. Esiste in capo ai dipendenti l'obbligo, sancito da norme di legge e di C.C.N.L., di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono tutte le tecnologie informatiche ed i sistemi informativi messi a disposizione dall'Amministrazione.
3. Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. A tal fine, riceverà copia del presente Regolamento e potrà richiedere all'Amministratore del Sistema Informativo eventuali maggiori informazioni e/o delucidazioni.
4. In particolare, l'accesso ai servizi informatici deve avvenire solo utilizzando le stazioni di lavoro (Personal Computer) e gli strumenti software messi a disposizione dall'Azienda al personale autorizzato e per l'esclusivo svolgimento delle proprie mansioni, e solo con le proprie credenziali personali di autenticazione (userID e password).

5. Per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati, il dipendente ha, pertanto, anche l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica.
6. L'Azienda può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, rispetterà la libertà e la dignità dei lavoratori.
7. Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione in appositi file e riconducibili ad un account utente e pc client. Detti files possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D. Lgs. n. 196/2003.

Art. 3 - L'Amministratore del Sistema Informativo

1. L'Amministratore del Sistema Informativo – nominato con atto del Titolare del trattamento dei dati ai fini dl D. Lgs. 196/2003, con il quale collabora - ha il compito di sovrintendere alle risorse dei sistemi operativi e dei sistemi di base dati, a tutti gli elaboratori in uso presso l'Azienda e consentirne l'utilizzazione a specifici utenti in base alle richieste presentate dalla Direzione.
2. L'attività dell'Amministratore si esplica in due contesti complementari:
   a) attività di ordinaria amministrazione, volta a garantire il normale funzionamento e lo sviluppo della rete informatica;
   b) gestione delle emergenze, quando si rilevino condizioni che pongano a rischio immediato la corretta funzionalità della rete o la sicurezza dei dati e delle risorse informatiche. In questa caso l'Amministratore può operare anche mediante il supporto delle ditte esterne alle quale viene affidato l'incarico di manutenzione dei sistemi installati presso l'Azienda.
3. L'Amministratore assegna ad ogni utente una credenziale di identificazione pubblica (user ID), una credenziale riservata di autenticazione (password) ed profilo di autorizzazione per l'utilizzo della Rete Informatica aziendale e/o per l'uso della posta elettronica e/o di internet e/o per l'uso di servizi/programmi specifici.
4. L'Amministratore è autorizzato a svolgere regolari attività di controllo, amministrazione e backup sui dischi locali dei PC degli utenti e sulle unità di rete.
5. L'Amministratore può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

Art. 4 - Utilizzo del personal computer

1. Per essere autorizzati all'uso delle risorse informatiche è necessario che venga presentata all'Amministratore da parte del Direttore d'Area cui è assegnato il dipendente apposita richiesta scritta per la creazione di un nuovo account (userID e password), con indicazione del profilo di autorizzazione per ogni applicativo richiesto (modello allegato A).
2. Il personal computer affidato al dipendente e le unità di rete a sua disposizione sono strumenti di lavoro ed aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
3. **Ogni dipendente** – essendo personalmente responsabile della macchina a lui consegnata – **deve utilizzare unicamente il pc e le credenziali ad egli assegnato** ed ha diritto ad accedere alle risorse informatiche aziendali per le quali è stato espressamente autorizzato e ad utilizzarle esclusivamente per gli scopi inerenti le mansioni svolte. Tali autorizzazioni sono strettamente personali e non cedibili.
4. Gli accessi alle banche dati informatizzate e/o ai dati personali oggetto di trattamento

dovrà avvenire tramite l'elaboratore/gli elaboratori assegnati, anche temporaneamente, di cui l'Utente è personalmente responsabile durante il periodo in cui svolge la prestazione lavorativa. A tal fine, dovrà evitare di divulgare ad altri la propria user-id e password e mettere in atto tutti gli strumenti e le precauzioni necessarie al fine di evitare l'accesso alla risorsa da parte di soggetti non autorizzati, ogniqualvolta ci si allontana dal personal computer (ad es. procedere al blocco del computer oppure all'attivazione automatica dello screen saver protetto da password).

5. Al fine di consentire correttamente lo svolgimento delle attività legate alle protocollazione della corrispondenza dell'Azienda, è consentito a tutti i ruoli dell'Ufficio di Coordinamento dell'Area delle Funzioni Contabili e Alberghiere l'uso della postazione denominata "Protocollo Informatico".
6. L'Amministratore, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, in relazione agli scopi di volta in volta identificati.
7. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcuni Servizi, deve essere presentata richiesta per iscritto all'Amministratore, il quale valuterà l'istanza meramente al fine di evitare il pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.
8. Il personal computer deve essere spento prima di lasciare gli uffici al termine dell'orario di lavoro o in caso di assenze prolungate dall'ufficio. 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. In ogni caso deve essere attivato lo screen saver con relativa password.
9. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 12 del presente Regolamento relativo alle procedure di protezione antivirus.
10. Al fine di assicurare il corretto funzionamento di tutta la rete informatica (PC), nonché di garantire la corretta gestione delle politiche di sicurezza delle informazioni e di evitare il grave pericolo di introdurre virus informatici all'interno della rete dell'Azienda, l'Utente non deve assolutamente:
    - permettete ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le sue credenziali; diversamente si risulterà autore di qualunque azione;
    - modificare, le caratteristiche impostate sul PC assegnato, gli indirizzi IP, i punti rete di accesso e le configurazioni delle reti LAN/WAN configurate;
    - attivare la password di accensione (bios) sul proprio PC;
    - rimuovere o modificare, senza preventiva autorizzazione, alcun dato o apparecchiatura aziendale;
    - dislocare, nemmeno per brevi periodi, in queste unità, qualunque files che non sia legato all'attività lavorativa;
    - effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
    - replicare sul disco locale del proprio PC dati aziendali, banche dati e documenti sensibili senza la preventiva autorizzazione dell'Amministratore;
    - installare sul proprio PC e/o non colleghi sulla rete LAN alcun dispositivo di memorizzazione, comunicazione od altre periferiche o componenti hardware (come ad esempio masterizzatori, modem, pc portatili ed apparati in genere ...) non acquistati dall'Azienda e non di proprietà della stessa e non autorizzati;
    - installare autonomamente ed utilizzare software diversi da quelli distribuiti ufficialmente e comunque non di proprietà dell'Azienda e/o non autorizzati in quanto non compatibili con l'attività istituzionale (D. Lgs. 518/1992 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore);
    - cancellare, copiare o asportare programmi software per scopi personali;
    - rimuovere, danneggiare o asportare componenti hardware;
    - installare, eseguire o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (ad es. virus, spamming della posta elettronica);

- realizzare copie di software di proprietà o utilizzati dall'Azienda da cedere, a qualsiasi titolo, a terzi, anche se ricevuto in uso al di fuori delle finalità lavorative;
- distribuire (anche via e-mail) ed utilizzi software che possa danneggiare le risorse informatiche;
- gettare integre eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDRom, …), prima di aver reso irrecuperabili i dati in essi contenuti;
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;
- memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Art. 5 - Gestione della password

1. L'accesso all'elaboratore, a qualsiasi applicazione che lo preveda, alle banche dati informatiche e lo screen saver sono protetti da una o più credenziali di autenticazione consistenti in uno o più user-id (identificativo utente) e da una o più password univoche (associate esclusivamente a ciascun utente) e devono essere custodite dall'utente con la massima diligenza e non divulgate: **le password sono strettamente personali e devono rimanere segrete;** la loro tutela è a carico dell'incaricato e non vanno comunicate o essere rese disponibili ad alcuno.
2. L'Amministratore provvede ad assegnare ad ogni utente un account di rete e un account per ogni servizio/programma autorizzato.
3. A ciascun utente sono attribuiti, pertanto, un "nome utente" ed una password di accesso ai sistemi informatici dell'Azienda. Saranno inoltre assegnate ulteriori user-id e password per l'accesso ad applicativi o a parte di essi a cui ciascun Utente è autorizzato ad accedere secondo i profili di autorizzazione riconosciuti.
4. Le password verranno forniti per la prima volta dall'Amministratore e, al primo utilizzo della password inizialmente comunicata, l'Utente è tenuto a modificarla.
5. La password deve essere lunga almeno 8 caratteri, deve essere alfanumerica e non deve avere riferimenti diretti con dati personali dell'utente (data di nascita, nome, cognome, nome dei figli, ecc.) o ad esso facilmente riconducibili.
6. E' assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dal proprio o da quello individuato dall'Amministratore del sistema.
7. Ai fini dell'assistenza sistemistica, la password di accesso può venire comunicata agli operatori tecnici chiamati ad intervenire i quali ne assicurano la riservatezza e la tutela.
8. Le password utilizzate hanno una durata massima di tre mesi, trascorsi i quali le password devono essere sostituite.
9. La password deve essere immediatamente sostituita, dandone comunicazione all'Amministratore del sistema, nel caso si sospetti che la stessa abbia perso la segretezza.
10. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore del sistema.
11. E' dato incarico ai Direttori d'Area di comunicare per iscritto all'Amministratore di Sistema tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

Art. 6 - Salvataggio dei documenti

1. Ad ogni dipendente viene creata ed assegnata una **cartella sul server** (denominata con il "nome utente" dello stesso) per il **salvataggio dei propri documenti di lavoro**, sulla quale è garantita la creazione di copie di sicurezza (backup). Tale

cartella – di norma – è disponibile agli altri utenti in modalità "sola lettura", ovvero in modalità "lettura e scrittura" se contenente informazioni gestite da più utenti.

2. Si consiglia di **non salvare su disco locale (C:\) e sul desktop** documenti riguardanti procedimenti ufficiali: in caso di rottura o danneggiamento del PC infatti non sarà possibile recuperare i file in esso contenuti. Si ricorda che – in caso di file riservati – è possibile utilizzare – in sede di salvataggio del documento - una password per evitare l'apertura o la modifica di documenti da parte di persone non autorizzate.
3. Queste le regole da seguire per la memorizzazione di files, al fine di non creare eccessivi appesantimenti sui dischi fissi del server:
   - non salvare permanentemente documenti PDF che sono stati o che verranno protocollati o che comunque vengono registrati, ad esempio: preventivi, richieste di preventivi e simili; domande di accoglimento ed allegati; scansioni di atti ufficiali (delibere, determine, capitolati di gara e simili); fatture, ordinativi di acquisto;
   - evitare assolutamente la duplicazione di dati ed archiviazioni ridondanti: non creare sommariamente copie di cartelle per l'istruzione di procedimenti analoghi, ma copiare solamente i file utili, avendo cura di rinominarli correttamente;
   - eliminare copie obsolete e versioni non ufficiali di file (ad es. "prova", "bozza", "vecchia" "1", "2"…): costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili;
   - evitare di creare copie di file, copie di copie, … senza rinominarli correttamente;
4. Si invita inoltre:
   - ad utilizzare nomi di salvataggio il più possibile chiari e che permettano la comprensione del contenuto;
   - per il medesimo tipo di documento, a salvare solo un documento "tipo" da utilizzare in tutti i casi di necessità di emissione di successivi atti analoghi, esempi: richiesta di preventivo, conferma preventivo, ordine di acquisto; comunicazioni derivanti da presentazione domande di accoglimento; contratto individuale di lavoro, lettera assunzione/ fine prova; dichiarazioni varie di contenuto analogo;
   - il Servizio Protocollo - in sede di inserimento del protocollo con la procedura "Protocollo informatico" - a scansionare tutta la documentazione relativa alla registrazione – e non esclusa dalla riproduzione in formato immagine, secondo elenco fornito - con scanner da tavolo o scanner/fotocopiatore.
5. Non è consentito salvare documenti personali su nessuna risorsa hardware: **il pc è uno strumento di lavoro**! Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del sistema.

Art. 7 - Utilizzo dei supporti magnetici

1. Tutti i supporti magnetici riutilizzabili (floppy-disk, cd-rom, dvd, cassette, chiavette e hard-disk usb, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
2. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
3. Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
4. Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo da parte dell'Amministratore del sistema.

Art. 8 - Utilizzo di pc portatili

1. Per particolari esigenze è possibile richiedere l'utilizzo di pc portatile aziendale al di fuori della Struttura (convegni, corsi etc.). 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.
2. Al PC portatile si applica le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Art. 9 - Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come cd-rom e dvd) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
2. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
3. E' buona regola evitare in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Art. 10 - Utilizzo della posta elettronica

1. L'Azienda è titolare di tutti i dati memorizzati con l'aiuto di strumenti informatici utilizzati in ambito aziendale, inclusa la posta elettronica. La posta elettronica aziendale è un servizio che appartiene all'Azienda e deve di conseguenza essere usata esclusivamente per gli scopi legittimi di lavoro.
2. 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.
3. Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomandano gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.
4. La casella di posta elettronica deve essere mantenuta in ordine, cancellando dalla "posta eliminata" documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.
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 della casella di posta elettronica certificata operapiacoianiz@pec.it.
6. Per la trasmissione di file all'interno dell'Azienda è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le cartelle presenti sul server, notificando a mezzo e-mail al destinatario la disponibilità del file stesso.
7. E' obbligatorio controllare con il software antivirus i files allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
8. In caso di assenza programmata del lavoratore, il medesimo potrà attivare un messaggio automatico di risposta alle e-mail ricevute che indichi a quale altro soggetto o struttura inviare messaggi.
9. Nel precisare che la Posta Elettronica è uno strumento di lavoro, si ritiene utile segnalare che l'Utente deve evitare di:
   - utilizzare l'indirizzo di posta elettronica aziendale (.....@operapiacoianiz.it) per l'invio di messaggi a carattere personale/extra-lavorativo e per la partecipazione a dibattiti, forum o mailing-list non direttamente attinenti l'attività lavorative e le

proprie mansioni, salvo diversa ed esplicita autorizzazione;
- effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;
- utilizzare la posta elettronica privata (p.es. hotmail, libero, tiscali, ecc.) per attività di servizio. Queste caselle di posta elettronica non possono infatti garantire i criteri di sicurezza che l'Azienda si è data;
- far uso della funzionalità di ridirezione della propria posta elettronica aziendale ad una casella di posta elettronica privata esterna. Nello stesso modo, per proteggere la rete dell'Azienda, non è consentito attivare la funzionalità di ridirezione da una propria casella di posta privata a quella aziendale;
- prestare la massima attenzione nell'aprire allegati di posta elettronica "ambigui" (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati aziendali).

Art. 11 - Utilizzo della rete internet e dei relativi servizi

1. Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. L'Utente deve evitare:
   - di effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;
   - di navigare in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa;
   - di scaricare e diffondere software gratuito (freeware), giochi, immagini e shareware prelevati da siti Internet, e non attinenti l'attività di servizio;
   - di scaricare file multimediali per finalità non direttamente afferenti l'attività lavorativa, comunque sempre con esplicita autorizzazione del proprio Responsabile;
   - di accedere a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
   - di accedere a flussi in streaming video da Internet per scopi non istituzionali (ad esempio guardare video o filmati utilizzando le risorse Internet);
   - di scaricare documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza sindacale o politica;
   - di effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione Generale;
   - di procedere ad ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
   - di partecipare a forum non professionali, di utilizzare chat line (esclusi gli strumenti autorizzati), bacheche elettroniche e registrazioni in guest books e social networks anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.
2. L'Amministratore si riserva di applicare per singoli e/o gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

Art. 12 - Protezione antivirus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
2. Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato.
3. 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 e segnalare l'accaduto all'Amministratore del sistema.

4. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, dvd, nastri magnetici di provenienza ignota.
5. 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 consegnato all'Amministratore di sistema.

Art. 13 - Non osservanza della normativa aziendale

1. La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni disciplinari previste dalla normativa vigente in materia che possono essere comminate e ulteriori conseguenze di natura penale, civile e amministrativa.

Allegato A

All'Amministratore del Sistema Informativo

Il sottoscritto, ……..
Direttore .....……

RICHIEDE

la creazione di un ACCOUNT PERSONALE per il dipendente:
Nome e Cognome……...……...
in servizio dal …… presso …….

Inoltre si richiede l'attivazione dei seguenti servizi/programmi:

- ❒ software/applicativi (indicare quali):
  …….
  …….
  …….
  …….
  …….
- ❒ posta elettronica
- ❒ internet
- ❒ altro: …….

Firma: ……

Data: …….