ISTRUZIONI OPERATIVE E NORME COMPORTAMENTALI

Interactive 3G s.r.l.

INTRODUZIONE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'azienda e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda adotta un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza informatica e al trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati ed i responsabili del trattamento dei dati in attuazione del d.lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

DEFINIZIONI

Ai fini delle seguenti istruzioni operative e norme di comportamento dettate per l'utilizzo delle risorse informatiche e telematiche, per "**Incaricato**" (di seguito anche utente) deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, volontario, tirocinante ecc.) in possesso di specifiche credenziali di autenticazione ed autorizzato a compiere operazioni di trattamento dei dati personali,sensibili e giudiziari presenti in azienda.

CAMPO DI APPLICAZIONE DELLE ISTRUZINI OPERATIVE E NORME DI COMPORTAMENTO

Dette norme si applicano a tutti i componenti dell'organigramma aziendale, nonché gli "esterni" all'Azienda, nei casi relativi a collaborazione di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, ecc.) e verranno diffuse in modo capillare.

UTILIZZO DEL PERSONAL COMPUTER

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.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete aziendale (intranet) solo attraverso specifiche credenziali di autenticazione come meglio descritto nei successivi articoli del presente Regolamento.

L'Azienda rende noto che il personale incaricato che opera presso il servizio *Information Tecnology* (IT) della stessa Azienda 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.).

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del IT per conto dell'Azienda 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 l'Azienda 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.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del IT nel caso in cui siano rilevati virus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un 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 *.

* *Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare lo screen-saver a tempo con obbligo di reintrodurre la password per l'accesso.*

I SISTEMI INFORMATICI AZIENDALI – NORME GENERALI.

Tutte le Apparecchiature Informatiche nonché i Personal Computer, fissi o mobili, i PDA – *Smartphone,* i relativi programmi e/o le applicazioni, affidate agli "utenti aziendali" sono, com'è noto, strumenti di lavoro, pertanto:

- Tali strumenti vanno custoditi in modo appropriato.
- Tali strumenti possono essere utilizzati solo per fini professionali (ovviamente in relazione alle mansioni assegnate) e non anche per scopi personali, tantomeno per scopi illeciti.
- Non è consentito prestare o cedere a terzi qualsiasi Apparecchiatura Informatica, quali ad esempio PC, PDA – *Smartphone,* Proiettori, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi.
- Non è consentito rimuovere i contrassegni identificativi se presenti sulle Apparecchiature Informatiche.
- Debbono essere prontamente segnalati alla Direzione il Danneggiamento o lo Smarrimento di tali strumenti. Inoltre, qualora si verifichi un furto o si smarrisca un'Apparecchiatura Informatica di qualsiasi tipo,

l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla Direzione l'originale della denuncia all'Autorità di Pubblica Sicurezza.

- È fatto assoluto divieto di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso. Resta inteso che, in caso di violazione, troveranno applicazione la personale responsabilità civile e penale del dipendente, nonché le sanzioni disciplinari da parte dell'azienda.

- È fatto assoluto divieto di trasferire all'esterno dell'Azienda e/o trasmettere *files,* documenti, disegni, progetti o qualsiasi altra documentazione riservata di proprietà Azienda, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile.

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

- Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Responsabile dei Sistemi Informativi.

- Non è consentito l'uso di programmi non autorizzati dal Responsabile dei Sistemi Informativi che valuterà il rispetto degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla legge 18 agosto 2000 n. 248, contenente nuove norme di tutela del diritto d'autore

- Non è consentito modificare le configurazioni impostate sulle Apparecchiature Informatiche (PC, Workstation, PDA – *Smartphone,* ecc…).

- Non è consentita l'installazione e/o il collegamento alle Apparecchiature Informatiche (PC, Workstation, PDA – *Smartphone,* ecc…) di periferiche aggiuntive non autorizzate dal Responsabile dei Sistemi Informativi.

- Sui PC dotati di scheda audio e/o lettori CD/DVD non è consentito l'ascolto di Files audio o musicali, né la visualizzazione di video e *films* se non a fini prettamente lavorativi.

- Non è consentito lasciare incustodito e/o accessibile ad altri il proprio PC. Durante le assenze prolungate deve essere attivata la funzione di Blocco Computer.

- Non è consentito lasciare incustodito e/o accessibile ad altri qualsiasi apparecchiatura Informatica mobile (PC portatili, PDA – *Smartphone,* Videoproiettori, ecc…) durante l'assenza dall'Azienda (ferie, fine settimana, notte).

GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione per l'accesso al PC vengono assegnate al dipendente dal personale del servizio IT.

Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione aziendale (ovvero dal Responsabile dell'ufficio con il quale il collaboratore si coordina nell'espletamento del proprio incarico).

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente *(user-id),* assegnato dal Servizio IT associato ad una parola chiave *(password)* riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

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.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del servizio IT.

Le *passwords* che consentono l'accesso alla Rete Societaria devono essere, con riferimento alle Misure di Sicurezza imposte dal Decreto Legislativo 196 del 30 giugno 2003, riservate; ognuno ha pertanto il dovere di tutelare la loro segretezza.

Le *passwords* non devono essere comunicate ad altri, né devono essere esposti sul PC etichette e/o adesivi riportanti userid e/o *passwords.*

Le *passwords* devono essere lunghe almeno 8 caratteri, non devono contenere riferimenti agevolmente riconducibili all'utente, devono essere modificate al primo accesso e cambiate almeno ogni 3 mesi.

Non è in alcun modo consentito l'utilizzo di *passwords* di altri "utenti aziendali", neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi.

Il personale del servizio IT 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.

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.

UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente potrà contattare il personale del servizio IT e seguire le istruzioni da questo impartite.

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

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

UTILIZZO DI PC PORTATILI

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

Ai PC portatili si applicano le regole di utilizzo previste dalle presenti norme, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

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.

GESTIONE DEL SERVIZIO

Della gestione delle risorse informatiche così come dell'abilitazione per la connessione ad internet e del servizio di posta elettronica è responsabile il servizio IT.

Il servizio IT è tenuto a:

- adottare le misure più idonee a garantire continuità, disponibilità e sicurezza del servizio
- gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali Informare tempestivamente gli utenti con anticipo di eventuali fermi o interruzioni di servizio che si rendessero necessari per manutenzione o per cause di forza maggiore;
- monitorare i livelli di servizio al fine di garantire la massima efficienza.

Garantire la funzionalità tecnica In particolare cura:

- l'attribuzione e la revoca di account e di password e la gestione dei livelli di accesso;
- l'individuazione delle risorse informatiche e software relativamente agli acquisti ed il collaudo di tutte le attrezzature informatiche, telematiche e software;
- l'assegnazione – come richiesto ed autorizzato dal responsabile della Struttura presso la quale il dipendente è in servizio - del numero degli accessi ad internet sulla base delle effettive necessità e compatibilmente con la banda minima da garantire per le normali attività dell'azienda;
- la configurazione e l'amministrazione delle risorse informatiche e reti.

Per risorse informatiche si intendono:

- macchine del Settore IT (installate presso il settore e/o presso la sala Server);
- workstation, personal computer, notebook , stampanti utilizzati da dipendenti,
- amministratori, personale con incarichi professionali, stagisti, tirocinanti ed eventuali
- ospiti;

- tutte le macchine facenti comunque parte della rete;
- apparati di rete; tutto il software e i dati acquistati o prodotti per l'amministrazione dei sistemi, per l'utilizzo da parte degli utenti o di terzi autorizzati.

- La revoca dell'accesso temporaneo alla risorsa Informatica e di rete, sentito il Responsabile preposto, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti; potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
- L'attivazione/disattivazione della casella di Posta Elettronica personale del Responsabile/i incaricati al trattamento dei dati.
- L'attivazione/disattivazione di una casella di posta elettronica nominale per il dipendente, autorizzato dal Responsabile di riferimento.
- L'attivazione/disattivazione della casella di Posta Elettronica per i collaboratori, previa richiesta del Responsabile di riferimento;
- L'attivazione/disattivazione della casella di Posta Elettronica di servizio/struttura a seguito di modifica organizzativa dell'Azienda per variazione organizzativa come da atto aziendale. Al fine degli adempimenti di cui sopra la Direzione provvede a comunicare al servizio IT l'elenco del personale assunto/cessato;
- Il servizio IT può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell' Azienda sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.
- Il servizio IT non effettua alcuna misura, controllo, censura, modifica, cancellazione di messaggi sui server di posta elettronica tranne quando ciò è legato a:
  - esigenze tecniche o di sicurezza del tutto particolari;
  - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
  - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

- Vige l'assoluto divieto di effettuare controlli con le seguenti modalità:
  - la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail;*
  - la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
  - la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
  - l'analisi occulta di computer portatili affidati in uso.

ACCESSO A INTERNET E USO DI RETE AZIENDALE

La navigazione in internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione.

L’uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e le attività svolte mediante la navigazione in internet o il sistema di posta elettronica sono destinati al conseguimento dei fini istituzionali dell’Azienda.

I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà dell’Azienda.

La banda Internet ed il sistema di posta elettronica sono operanti con continuità, 24 ore al giorno per 365 giorni all’anno.

Per l’accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione (ID utente) e una parola chiave segreta (password).

È assolutamente proibito entrare nella rete e nei programmi con un codice d’identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Superato il sistema di autenticazione l’utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.

Tutti gli utenti cui è assegnata una postazione di lavoro possono utilizzare internet, compatibilmente con le bande a disposizione

Data la vasta gamma di attività aziendali, non è definito a priori un elenco di siti aziendali autorizzati

L’utente si impegna a:

- non cedere, una volta superata la fase di autenticazione, l’uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l’accesso a intranet e ai servizi di posta elettronica;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (ID utente e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l’utente assegnatario del codice.

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.

USO DELLA POSTA ELETTRONICA

L’Azienda fornisce, limitatamente agli “utenti aziendali” che ne hanno necessità, una Casella di Posta Elettronica nominale ed univocamente assegnata. Anche la Posta Elettronica è uno strumento di lavoro messo a disposizione per svolgere le attività legate alle mansioni assegnate, pertanto l’indirizzo attribuito agli “utenti aziendali” è personale ma non privato. Ognuno è direttamente responsabile, disciplinarmente e giuridicamente, del contenuto della propria Casella di Posta e dei messaggi inviati.

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.

La casella di posta deve essere mantenuta in ordine, cancellando periodicamente i messaggi in SPAM e svuotando il cestino

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

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 Direttori di Struttura, a seconda del loro contenuto e dei destinatari delle stesse.

È obbligatorio porre la massima attenzione nell'aprire i file *attachments* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

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.

In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio *web-mail* entro cinque giorni - verrà attivata a cura dell'Azienda.

Sarà comunque consentito al superiore gerarchico dell'utente o all'incaricato della custodia della copia delle credenziali, individuato dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

L'accesso alla posta elettronica è personale e vi si passa tramite nome utente e password di identificazione.

L'accesso non può essere condiviso o ceduto.

Si ritiene inoltre utile segnalare che:

- non è consentito utilizzare la Posta Elettronica, interna ed esterna, per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi, interni ed esterni, di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito l'utilizzo della Posta Elettronica di altri "utenti aziendali" per l'invio di comunicazioni a proprio nome o in nome di questi, salvo espressa autorizzazione dei medesimi; In caso di assenza programmata del lavoratore, è fortemente raccomandata agli utenti aziendali la condivisione della propria casella di posta, attivando una risposta automatica di fuori sede con l'eventuale indicazione dei soggetti terzi autorizzati a ricevere e leggere la posta dell'assente.
- non è consentito creare, consultare, utilizzare caselle di Posta Elettronica private;
- l'Azienda potrebbe rendere disponibili alcuni indirizzi condivisi da più "utenti aziendali" rendendo chiara la natura non privata della corrispondenza. Tali indirizzi corrispondono generalmente a caselle di segreteria o caselle di funzione e, nella rubrica interna, sono preceduti dai caratteri * o **. Tutte le comunicazioni esterne, inviate o ricevute con questi indirizzi potranno essere archiviate.

PROTEZIONE ANTIVIRUS

Il sistema informatico dell'azienda 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.

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 IT. 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 IT.

Ai fini sopra esposti, sono quindi da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli di seguito richiamati a titolo indicativo:

- onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Responsabile dei Sistemi Informativi;
- non è consentito l'uso di programmi non autorizzati dal Responsabile dei Sistemi Informativi che valuterà il rispetto degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla legge 18 agosto 2000 n. 248, contenente nuove norme di tutela del diritto d'autore;
- non è consentito modificare le configurazioni impostate sulle Apparecchiature Informatiche (PC, Workstation, PDA – Smart Phone, ecc…);
- non è consentita l'installazione e/o il collegamento alle Apparecchiature Informatiche (PC, Workstation, PDA – *Smartphone,* ecc…) di periferiche aggiuntive non autorizzate dal Responsabile dei Sistemi Informativi;
- sui PC dotati di scheda audio e/o lettori CD/DVD non è consentito l'ascolto di Files audio o musicali, né la visualizzazione di video e *films* se non a fini prettamente lavorativi;
- non è consentito lasciare incustodito e/o accessibile ad altri il proprio PC. Durante le assenze prolungate deve essere attivata la funzione di Blocco Computer;
- non è consentito lasciare incustodito e/o accessibile ad altri qualsiasi apparecchiatura Informatica mobile (PC portatili, PDA – Smart Phone, Videoproiettori, ecc…) durante l'assenza dall'Azienda (ferie, fine settimana, notte).

COMPITI E RESPONSABILITÀ

L'utente è responsabile della propria postazione informatica e della sua casella di Posta Elettronica Personale.

Il Titolare o il Responsabile può delegare un dipendente alla gestione della casella di Posta Elettronica di struttura. La delega va attribuita per iscritto.

L'utente è responsabile della segretezza del proprio *user-id* e relativa password. È anche responsabile del contenuto dei messaggi inviati dalla propria casella elettronica. E' responsabile di effettuare un back up della posta elettronica su server messo a disposizione dall'azienda una volta a settimana. Il back up settimanale va a sostituire il precedente memorizzato.

L'utente si impegna a comunicare alla Direzione IT, non appena ne venisse a conoscenza, qualsiasi uso non autorizzato da parte di terze persone del proprio *user-id* così come sono obbligati a segnalare immediatamente al IT ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, *files* e servizi non espressamente e preventivamente autorizzati dalla Azienda.

I dati personali, sensibili o giudiziari che sono affidati all'Incaricato per lo svolgimento dei suoi compiti, devono essere costantemente controllati e custoditi fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive del Servizio IT aziendale divulgate tramite e-mail o circolare.

I responsabili dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche messe a disposizione della loro struttura, esercitando una funzione di istruzione, indirizzo e controllo sugli utenti incaricati ed individuando con precisione le responsabilità per la gestione dei dati, dei salvataggi e delle risorse stesse.

In caso di cessazione del rapporto di lavoro, trasferimento ad altro servizio, o comunque di non necessità di utilizzo da parte di utenti già autorizzati, sarà data tempestiva comunicazione scritta, per gli applicativi da esso gestiti, al servizio IT che provvederà alla disattivazione delle credenziali di autenticazione ovvero alla loro modifica per ogni diversa esigenza.

Il servizio IT è responsabile della sicurezza, della funzionalità e del corretto impiego delle risorse informatiche centralizzate e della rete aziendale. Non rientrano nelle proprie competenze la gestione e l'assistenza tecnica delle apparecchiature personali e dei sistemi informatici di proprietà esterna all'azienda.

La gestione e responsabilità di questi ultimi è demandata ai singoli Responsabili che provvedono alla verifica ed alla corretta applicazione delle misure minime di sicurezza.

Per le postazioni personal computer "stand alone", ossia non collegate in rete, la responsabilità nell'applicazione delle misure minime di sicurezza è demandata all'utente finale ed al Responsabile che le ha in dotazione.

ISTRUZIONI OPERATIVE PER GLI "INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI" SENZA L'AUSILIO DI STRUMENTI INFORMATICI

L'Incaricato del trattamento dei dati personali è la persona fisica autorizzata dal Titolare/Responsabile del trattamento a compiere operazioni sui dati personali.

All'interno della struttura il titolare e/o i responsabili, se nominati, definiscono un elenco degli incaricati autorizzati al trattamento dei dati personali impartendo agli stessi precise e chiare istruzioni necessarie per garantire un costante controllo e accesso agli archivi.

Ciascun Incaricato è informato che tutti gli atti e i documenti "trattati" devono essere dagli stessi conservati e restituiti al termine delle operazioni.

Nel caso si tratti di dati sensibili o giudiziari gli incaricati, al termine del trattamento, dovranno riporli nell'armadio chiuso a chiave e restituire la chiave.

Salvo diverse indicazioni nonché previa identificazione e registrazione dei soggetti l'accesso agli archivi ove sono presenti dati sensibili/giudiziari non è consentito dopo l'orario di chiusura.

È fatto divieto a chiunque di effettuare copie su supporti magnetici, fotostatiche o di qualsiasi altra natura se non espressamente autorizzate dal titolare e/o dal responsabile se nominato.

L'Incaricato del trattamento, nello svolgimento delle sue mansioni, deve osservare le seguenti disposizioni:

- controllo e custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- aggiornamento periodico, con cadenza almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione, così come disposto dal d.lgs. 196/2003 (Allegato B) punto 27);
- il titolare ha pieni poteri per garantire un controllo costante nell'accesso degli archivi;
- ciascun incaricato, che tratta atti e documenti contenenti dati personali, deve conservarli e a restituirli solo al termine delle operazioni;
- se i documenti in possesso degli incaricati contengono dati sensibili / giudiziari (art. 4 d.lgs. 196/2003) ciascun Incaricato è tenuto a conservarli fino alla restituzione in contenitori muniti di serratura;
- dopo l'orario di chiusura, l'accesso agli archivi contenenti documenti è consentito (nel caso sono presenti dati sensibili / giudiziari) solo previa identificazione e registrazione dei soggetti/Incaricati;
- se gli atti ed i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate, così come disposto dall'art. 28 "incaricati del trattamento" del d.lsg. 196/2003 (punto 28);
- l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate;
- quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate, così come disposto dall'art. 29 "incaricati del trattamento" del d.lgs. 196/2003 (punto 29).

COMPORTAMENTI NON CONSENTITI NELLA "NAVIGAZIONE" IN INTERNET.

Non è consentito: l'utilizzo di modem personali; utilizzo di qualunque altro dispositivo "internet-Key" con account personali; navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate; l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking,* acquisti *on-line* e simili, salvo casi espressamente autorizzati dalla Titolare; lo scarico di software gratuiti e shareware prelevati da siti internet, salvo casi espressamente autorizzati dalla Titolare; ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa; la partecipazione, per motivi non professionali a Forum, l'utilizzo di *chat-line,* di bacheche elettroniche e le registrazioni in *guestbook* anche utilizzando pseudonimi (nickname); la memorizzazione di documenti

informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica; scaricare/scambiare materiale coperto da diritto d'autore; eseguire o favorire pratiche di Spamming.

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, sulle unità di rete e sulle Apparecchiature Informatiche in generale (PC, Workstation);

l'Azienda si riserva la facoltà di procedere alla rimozione di ogni File o applicazione che riterrà pericolosa per la sicurezza del sistema, ovvero acquisiti e/o installati in violazione del Codice Etico Informatico;

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

non è consentito collegare alla rete aziendale PC non di proprietà Azienda, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi.

COMPORTAMENTI NON CONSENTITI NELL'UTILIZZO DELLA POSTA ELETTRONICA.

Non è consentito:

- utilizzare l'indirizzo di posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni assegnate usare il servizio per scopi illegali, per inviare e ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso; utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum o mailing-list, su internet per motivi non professionali; non è, altresì consentito, aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare verso ulteriori indirizzi @-mail contenuti o documenti oggetto delle cosiddette "catene di s. Antonio"; (se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi).

- effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni di remote Banking, acquisti *on-line* e simili, salvo diversa ed esplicita autorizzazione aziendale; simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi; prendere visione della posta altrui; aprire allegati di posta elettronica ambigui o di incerta provenienza (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati); modificare la configurazione hardware e software della sua macchina; né utilizzare sistemi client di posta elettronica non conformi a quelli accettati dall'azienda; l'utilizzo di critto sistemi o di qualsiasi altro programma di sicurezza e/o crittografia non previsto esplicitamente dal servizio informatico aziendale; l'invio di informazioni o documentazioni ad Istituti, Enti pubblici o privati, Associazioni, Comuni, Regioni senza previa autorizzazione della Direzione Aziendale la trasmissione a mezzo posta elettronica di dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati;

In caso di violazione o inadempimento di quanto riportato ai precedenti art. 8 e 9, il IT procederà al distacco dell'utente dal collegamento ad internet e ne darà comunicazione al GRU per l'eventuale accertamento di responsabilità disciplinari del personale dipendente.

SOLUZIONI PER GARANTIRE LA CONTINUITA' LAVORATIVA

Ciascun operatore può, anche da postazioni esterne all'azienda, utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e funzioni di inoltro automatico dei messaggi ricevuti verso indirizzi di altro personale dipendente.

Nel caso in cui un dipendente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, il Responsabile delle copia credenziali di autentificazione, potrà accedere alla casella di posta al fine di garantire la continuità dell'attività lavorativa.

CONTROLLI

I controlli saranno svolti in conformità alla legge, anche saltuari o occasionali, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema sia per verificare il corretto utilizzo da parte dei propri dipendenti tanto della rete internet che della posta elettronica.

Nell'esercizio del potere di controllo l'Azienda si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo, rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi e informerà preventivamente i lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali. Le informazioni trattate infatti contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili ed in più le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, "può essere tracciata a volte solo con difficoltà". "Il luogo di lavoro è infatti una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali" (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).

I controlli si svolgeranno in forma graduata:

- In via preliminare l'azienda provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree e dunque ad un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.

- In assenza di successive anomalie non si effettueranno controlli su base individuale.

- Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro e in caso di abusi singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati - anche per verifiche sulla funzionalità e sicurezza del sistema - e le relative modalità - inoltrando preventivi avvisi collettivi o individuali).

- In caso in cui la posta elettronica e la rete Internet siano utilizzate indebitamente o di riscontrato e reiterato uso non conforme delle risorse informatiche, il IT, che effettua i controlli, segnalerà il comportamento al responsabile della struttura di appartenenza del dipendente il quale attiverà il procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L. di riferimento.

- Per il personale dirigente il comportamento andrà segnalato alla Direzione Aziendale ed al competente Ufficio per i procedimenti disciplinari per l'adozione degli atti di rispettiva competenza.

- Per il personale non dipendente cui non è applicabile il C.C.N.L. di riferimento il comportamento andrà segnalato alla Direzione Aziendale per l'adozione degli atti di specifica competenza.

L'Azienda si riserva la facoltà di procedere periodicamente, secondo le garanzie previste dalla normativa in materia di tutela della Privacy e di diritto del lavoro, a controlli sull'utilizzo del PC, della rete e dei dispositivi Aziendali assegnati, allo scopo di rilevare la presenza di virus informatici e garantire l'integrità e la sicurezza del sistema.

L'Azienda si riserva la facoltà di disporre, secondo le garanzie previste dalla normativa in materia di tutela della Privacy e di diritto del lavoro, controlli specifici, non sistematici, sull'utilizzo della Posta Elettronica e di Internet, attraverso analisi di dati aggregati, allo scopo di verificare il corretto utilizzo dei Servizi.

I dati analizzati durante tali controlli non vengono automaticamente né sistematicamente associati a "utenti aziendali" identificati, ma per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con altri dati, permettere di identificare gli "utenti aziendali".

I Dati Internet vengono utilizzati al solo fine di ricavare informazioni statistiche sull'uso dei siti nonché per controllarne periodicamente il corretto utilizzo e vengono conservati per un periodo di tempo limitato.

Tutti i dati in questione potrebbero essere utilizzati per l'accertamento di responsabilità in caso di eventuali reati informatici ai danni dell' Azienda.

INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO

Eventuali interruzioni del servizio sono comunicate agli utenti.

Ai sensi del presente regolamento, l'utilizzo del servizio di accesso ad internet e di utilizzo di posta

elettronica cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;

- se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;

- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;

- in caso di diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;

- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;

- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti;
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

In caso di interruzione/cessazione d'ufficio del servizio è espressamente vietato all'utente cancellare la posta aziendale.

Con la cessazione il profilo dell'utente verrà disattivato, ma la posta verrà mantenuta archiviata e consultabile all'occorrenza per fini strettamente aziendali secondo il termine della fine del processo produttivo a cui essa fa riferimento

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L' ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI

Qualora l'utente acceda a Internet tramite la rete dell'Azienda, è tenuto a sottoscrivere la dichiarazione di assunzione di responsabilità e acquisisce lo status di responsabile per la gestione e l'utilizzo della risorsa stessa;

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L' ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI

(Dichiarazione da sottoscrivere e trasmettere alla Direzione)

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente le politiche e le regole della **INTERACTIVE 3G S.r.l.,** anche riguardo l'utilizzo e l'accesso a Internet; il sottoscritto si assume inoltre la piena responsabilità in caso di violazione delle leggi e dei regolamenti riconducibili al suo accesso personale.

Nome e Cognome :

…….

Settore :

…….

Firma :

……..

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

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.

DISPOSIZIONI FINALI

1. Le presenti Istruzioni e norme comportamentali sono state redatte dalla Titolare;
2. Le stesse sono state approvate dal Consiglio di amministrazione;
3. La sua pubblicizzazione avverrà nelle seguenti forme: consegna agli interessati e loro assunzione di responsabilità e affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.
4. E' fatto obbligo a chiunque spetti di osservarlo.
5. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal Presidente della Società. Ogni azione che non sia comunque conforme allo spirito delle presenti norme, verrà considerata una violazione della sicurezza, e come tale comporterà la segnalazione al Presidente
6. Il mancato rispetto delle presenti Istruzioni e norme comportamentali, ovvero del Codice Etico Informatico (se presente), potrà costituire oggetto di valutazione sotto l'aspetto disciplinare con l'applicazione di provvedimenti quali richiami, multe, ammonizioni scritte, sospensione dal lavoro fino a tre giorni e licenziamento, nonché sotto l'aspetto giudiziario;
7. L'Azienda potrà rivalersi sui responsabili degli eventuali danni derivanti da un uso non diligente o non conforme alle norme qui contenute e/o del Codice Etico Informatico.