REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI

Questa sezione stabilisce i criteri che devono essere seguiti dagli Utenti per utilizzare gli strumenti informatici:

- nel rispetto delle leggi e norme vigenti ed in particolare delle leggi in materia di sicurezza, privacy, copyright, accesso e uso dei sistemi informatici e telematici;
- nel rispetto delle norme e procedure lavorative generali definite dal Settore Informatico dell'Azienda;
- nel rispetto delle norme e procedure specifiche definite dal Settore Informatico dell'Azienda.

Gli strumenti informatici oggetto delle presenti istruzioni sono i servizi e gli apparati di proprietà (o affidati in uso) dell'Ente messi a disposizione degli Utenti per svolgere quotidianamente il proprio lavoro: il PC e gli apparati removibili, i sistemi di identificazione e autenticazione informatica, Internet e gli strumenti di scambio di comunicazioni e file, la posta elettronica.

Attenersi alle regole elencate in questo documento è un preciso obbligo dell'Utente che utilizza gli strumenti informatici che gli sono stati assegnati.

1 Linee guida generali

I responsabili degli uffici e dei settori devono verificare la corretta e puntuale messa in pratica di tali regole al fine di garantire:

- la riservatezza dei dati
- l'integrità dei dati

- la disponibilità dei dati

sui sistemi informativi dell'Azienda.

La precisa applicazione del presente regolamento è adeguata alle misure minime di sicurezza previste dal Codice sulla Privacy (D.lgs 196/2003) e permette perciò all'Azienda di garantire un uso dello strumento informatico a norma di legge.

Condotte non conformi al presente regolamento saranno valutate dalla Direzione competente di appartenenza e dalla Direzione del Personale.

Per l'uso dei sistemi informativi dell'Azienda sono assegnati a ciascun Utente specifiche credenziali di accesso (login e password, smart card).

L'uso di tali credenziali è individuale e non deve essere condiviso con altre persone.

L'assegnazione delle credenziali avviene sulla base di specifica richiesta formulata dal direttore responsabile e inoltrata al Settore Informatico.

L'Utente è responsabile delle credenziali a lui assegnate e della segretezza della propria password.

Gli strumenti informatici sono forniti all'Utente per finalità lavorative.

Non è quindi permesso utilizzare questi strumenti per altre finalità non connesse all'attività lavorativa o in modi che violino le leggi italiane in materia di sicurezza sul luogo di lavoro, ed altre leggi applicabili alla Pubblica Amministrazione quali:

legge sul copyright
legge sul trattamento dei dati personali (D.lgs 196/2003)
codice penale e leggi in materia di reati informatici
codice civile
leggi di tutela del patrimonio della Pubblica Amministrazione
leggi in materia di sicurezza sul luogo di lavoro

Tutti gli Utenti sono direttamente responsabili del fatto che i servizi e i sistemi informativi vengano utilizzati in modo efficace, efficiente ed anche eticamente corretto.

Si ricorda inoltre che un uso inappropriato del proprio PC, ad esempio la produzione e duplicazione di materiale pornografico o avente contenuto di natura pedofila, può

portare a severe violazioni penali di legge e ad un attacco legale nei confronti della persona che compie questa attività.

Eventuali violazioni delle procedure di accesso e sicurezza dei sistemi informativi di cui un Utente venga a conoscenza devono essere immediatamente riportate al Settore Informatico dell'Azienda.

2 Utilizzo del Personal Computer

Il Personale Computer ed i relativi programmi e/o applicazioni affidati al dipendente sono **strumenti di lavoro**, pertanto ciascun dipendente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.

Gli Utenti sono tenuti all'applicazione delle disposizioni e delle procedure di lavoro dell'Azienda relative alla sicurezza per proteggere le apparecchiature informatiche loro assegnate da furti e dall'uso da parte di persone non autorizzate.

Ogni Utente è inoltre responsabile dell'adozione di precauzioni adeguate per la sicurezza e la tutela delle apparecchiature informatiche dell'Azienda non sorvegliate. Tali disposizioni sono volte anche ad evitare accessi non autorizzati alle predette apparecchiature.

Gli Utenti inoltre sono tenuti a rispettare le disposizioni relative alla sicurezza dei locali previste dalla normativa vigente (D.lgs 626/94 e successive modificazioni) e le indicazioni specifiche fornite dagli organi dell'Azienda competenti in materia.

Il PC deve essere utilizzato con la dovuta cura, in particolare l'Utente deve:

- Assicurarsi che il proprio PC abbia attivata una procedura di autenticazione all'accensione;

- Non lasciare il proprio PC accesso e incustodito quando il proprio Utente è connesso e quindi l'accesso ai dati e alle applicazioni è garantito;

- Assicurarsi che sia attivato lo screensaver fornito dal sistema operativo che richiede una password per essere disattivato;

- Eseguire il processo di *log off* quando si finisce una sessione di lavoro;

- Per il salvataggio dei dati utilizzare il proprio spazio dedicato sul server "**cognomenome (NASPR:)**" oppure lo spazio dedicato ai vari uffici e condiviso da più utenti "**nomeufficio (NASPR:)**, i quali possiedono garanzie di riservatezza, protezione e recupero dei dati persi.
  Lo spazio virtuale denominato "**pubblica su (naspr**)", è stato creato e inteso solo quale luogo di interscambio temporaneo dei files; al fine di dissuadere eventuali salvataggi a lungo tempo, si procede alla cancellazione totale dei dati, contenuti nel suddetto spazio, con cadenza periodica breve.

- Eseguire backup manuali dei dati locali (che non sono sotto altre procedure di backup);

- Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione da parte del Sistema Informatico dell'AIPO ;

- Prima di aprire un file presente su un apparecchio removibile (es: floppy disk), assicurarsi che venga verificato da un antivirus aggiornato fornito dall'Azienda;

- Assicurarsi che lo scambio di file di piccole dimensioni avvenga quando possibile tramite posta elettronica, in modo che i messaggi vengano filtrati dai sistemi anti-virus dell'Azienda, e disincentivare l'utilizzo dei floppy, che sono un mezzo di diffusione dei virus;

- Non utilizzare software e programmi differenti da quelli messi a disposizione dall'Azienda;

- Non installare sui PC dell'Azienda software di terze parti, applicazioni o programmi personali, software scaricato da Internet, anche gratuitamente o a scopi di prova (shareware, freeware, software demo, software di prova);

- Non installare software acquistato al di fuori dall'Azienda o software fornito da riviste o software generico di libero mercato;

- Non installare software illegalmente duplicato o di cui non si conosce la provenienza;
- Non utilizzare gli strumenti di archiviazione (masterizzatori, unità floppy, ecc.) per fini personali;
- Non duplicare o diffondere software o file illegali (musica, film, ecc.) o software personale;
- Non duplicare o diffondere il software aziendale senza specifica autorizzazione.

3 Utilizzo di PC portatili

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

Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server)/Accesso Remoto:

- Utilizzare l'accesso in forma esclusivamente personale;
- Utilizzare la password in modo rigoroso;
- Disconnettersi al sistema RAS al termine della sessione di lavoro;

Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

4 Controllo degli accessi

L'accesso alla rete aziendale è protetto da password che ha il compito di prevenire che persone non autorizzate possano accedere ad un sistema informatico e alle relative applicazioni, per cui:

- **è vietato** connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Sistema Informatico Aziendale
- **è vietato** condividere cartelle in rete (global web)
- **è vietato** monitorare ciò che transita in rete
- **è vietato** l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda

Lo scopo è cautelare l'Azienda da ogni tipo di manomissione, furto o distruzione di dati e delle relative conseguenze, sia sul piano operativo che legislativo (penale e civile).

5 Gestione delle Password

La sicurezza di alcuni servizi e procedure informatiche dell'Azienda è basata sull'uso di password.

Pertanto è necessario che ciascun Utente scelga una password "robusta" e che tale password sia mantenuta segreta.

- Per ottenere questo scopo è necessario scegliere la propria password mettendo in pratica le seguenti indicazioni:
  - ✓ Più lunga è la password meglio è: non è possibile scegliere password minori di 8 caratteri.
  - ✓ Scegliere una password che include cifre, lettere e caratteri speciali come: ':;£$(,.ç@&/!

- ✓ Evitare di scegliere il proprio nome o cognome, il soprannome, la data di nascita, il nome di persone familiari, parole comuni, nomi di paesi, animali e così via.
- ✓ Non scegliere parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario. Esistono software in grado di individuarle.
- ✓ Non utilizzare semplici sequenze di tasti, come ad esempio *asdfghjkl*, o ripetizioni del proprio login (ad es., se il proprio login è *rossi*; la password *rossirossi* sarà inopportuna).
- ✓ Le parole con errori ortografici o con sillabe combinate costituite da due parole non correlate tra loro producono password appropriate.

- È necessario cambiare la password con regolarità:

  - ✓ L'obbligo di sostituzione della password ogni 180 gg (90 gg) per procedure di trattamento dati personali (sensibili)

- Si deve tenere riservata la propria password e soprattutto mantenere i seguenti accorgimenti:

  - ✓ Non scrivere la password su pezzi di carta o post-it che si lasciano sulla scrivania o attaccati al monitor;
  - ✓ Non comunicare a nessuno la propria password;
  - ✓ Non condividere con nessuno la propria password;
  - ✓ Quando si digita la propria password, assicurarsi che nessuno stia guardando la tastiera con l'intenzione di memorizzarla;
  - ✓ Non inviare per e-mail la password e se e proprio è necessario comunicarla, farlo a voce, per telefono o a mano in una busta chiusa;
  - ✓ Non utilizzare la stessa password per più scopi o procedure informatiche;

Qualora sia stato affidato all'Utente l'utilizzo di una procedura informatica con una password di default, è necessario che l'Utente provveda a personalizzarla immediatamente al primo uso cambiandola in una password personale.

Qualora le password vengano scritte per fini di backup su file digitali o cartacei al di fuori delle procedure di sicurezza dell'Azienda (es: file personali sul proprio PC), si raccomanda che questi documenti siano ben custoditi e l'accesso sia ristretto.

6 L'uso della Rete Internet

La navigazione su Internet è un servizio che viene messa a disposizione degli Utenti a supporto delle loro attività istituzionali.

Gli Utenti sono tenuti a:

- Navigare per il tempo strettamente necessario e solo per fini di natura lavorativa o professionale;
- Non navigare su siti aventi contenuti pornografici e di dubbia integrità morale, siti di hackers e siti di distribuzione di informazioni relative a software illegale;
- Non fornire dati personali, numeri di carta di credito, l'indirizzo di posta elettronica, dati dell'Azienda, su siti sconosciuti e la cui origine e gestione non sia certa e fidata;
- Non scaricare mai nulla da siti la cui origine e gestione non sia certa e fidata ed in particolare non installare mai sul proprio computer software, giochi o screensaver non connessi con la propria attività lavorativa e scaricati da siti terzi o da fonti che non siano autorizzate o previste dalle procedure dell'Azienda;
- Non utilizzare servizi di scambio di informazioni disponibili su Internet quali P2P, FTP o Telnet a meno che non sia stato autorizzato o previsto dalle procedure dell'Azienda;

Un uso improprio della navigazione su Internet può avere varie conseguenze dannose sia per l'Utente che per l'Azienda.

Può condurre a una seria violazione delle procedure di sicurezza dell'Azienda che può risultare in furti o distruzione di dati e più gravi danni patrimoniali.

In particolare:

- Un uso eccessivo della navigazione su Internet per fini personali o non connessi all'attività lavorativa porta a grandi perdite di tempo, a minore produttività sul lavoro e a un considerevole impegno delle risorse di rete messe a disposizione dall'Azienda;

- Un uso inappropriato della navigazione su Internet, ad esempio la visione di siti pornografici o aventi contenuti di natura pedofila, può portare a pesanti violazioni di legge;

- Il download di software *non autorizzato* può portare instabilità e inaffidabilità del proprio PC con conseguente riduzione delle prestazioni e violazione delle procedure di sicurezza;

- Il download di software *illegalmente duplicato* comporta per l'Utente l'assunzione tutte le responsabilità conseguenti alla violazione della normativa sul copyright;

- Il download di software *sconosciuto* sul computer dell'Utente può portare all'introduzione:

  - ✓ di software spia (*spyware*) che tracciano la nostra attività e la comunicano a nostra insaputa all'esterno;

  - ✓ di *virus* che ne compromettono l'integrità e le funzionalità e che possono portare alla perdita e/o distruzione di dati critici;

  - ✓ l'installazione di software (*virus troiani*) che permettono il controllo remoto del nostro dispositivo e il furto di dati;

- La connessione a Internet mediante modem – o altri mezzi di connessione – non autorizzati è vietata in quanto porta a gravi violazioni delle procedure di sicurezza dell'Azienda e a gravissimi rischi di introduzione di virus e a perdita e/o distruzioni di dati.

7 *Peer to Peer e software di file sharing*

Non è consentito agli Utenti di fare uso di software di software peer to peer (P2P) o di file sharing.

A tal fine è necessario seguire le seguenti regole:

- Non installare sul proprio PC software di file sharing di nessun genere (es. Kazaa, etc, software generico di ftp), a meno che non sia stato fornito dall'Azienda;
- Non creare librerie sul proprio PC di file musicali o video o che nulla hanno a che vedere con l'attività lavorativa;
- Non utilizzare software di file sharing eventualmente fornito dall'Azienda per condividere con Utenti esterni risorse e file del proprio PC;

- Non utilizzare software di file sharing eventualmente fornito dall'Azienda per condividere dati che nulla hanno a che vedere con l'attività lavorativa.

8 *Instant messaging e chat*

Non è consentito agli Utenti di fare uso di software di instant messaging e chat per finalità non stabilite dalle Direzioni dell'Azienda.

A tal fine è necessario seguire le seguenti regole:

- Non installare sul proprio PC applicazioni di instant messaging di nessun genere a meno che non sia stato fornito dall'Azienda;
- Non installare e non utilizzare software di chat di alcun genere;
- Non utilizzare applicazioni di instant messaging eventualmente forniti dall'Azienda per fini personali o con Utenti che non fanno parte del personale dell'Azienda;
- Non aprire eventuali allegati ai messaggi istantanei la cui provenienza non sia certa e non installare mai sul proprio PC software ricevuto in allegati di messaggi istantanei.

9 *La posta elettronica*

La posta elettronica è uno strumento che viene messo a disposizione degli Utenti per favorire lo scambio di informazioni e per migliorare la produttività del lavoro, ma non deve essere abusato e qualora utilizzato, deve essere utilizzato in modo consapevole, corretto e sicuro e nel rispetto delle procedure stabilite dall'Azienda e delle leggi vigenti.

Si raccomanda agli Utenti di adottare cura e attenzione quando si utilizza la posta elettronica.

A tal fine è necessario seguire le seguenti regole:

- Non utilizzare la casella di posta elettronica fornita dall'Azienda per fini personali;
- Non inviare o promuovere la ricezione e la diffusione, tramite la posta elettronica, nel corpo o come allegato di un messaggio, di materiale pornografico, illegale,

commerciale non connesso alle attività dell'Azienda, spam o comunque non legato all'attività lavorativa e professionale;

- Non inviare all'esterno dell'Azienda, nel corpo o come allegato di un messaggio di posta elettronica, materiale e/o documenti di proprietà dell'Azienda senza l'autorizzazione di un dirigente o a meno che non sia previsto dalle procedure dell'Azienda;

- Inviare i messaggi di posta elettronica solamente ai destinatari indispensabili, evitando di coinvolgere nella lettura delle e-mail Utenti non necessari, ed utilizzare in modo discreto e responsabile la rubrica degli indirizzi e-mail di tutti gli Utenti;

- Sul PC fornito dall'Azienda utilizzare sempre e solo la casella di posta elettronica fornita dall'Azienda e conseguentemente:

  ✓ Non installare/configurare, sul PC fornito dall'Azienda, account di posta elettronica personali.

- Qualora si ricevano messaggi che hanno provenienza ignota, dubbia o che hanno titoli ambigui:

  ✓ Non aprire messaggi la cui provenienza non sia certa;

  ✓ Non aprire mai allegati di messaggi di posta la cui natura non sia certa;

  ✓ Non aprire messaggi il cui oggetto/titolo è dubbio, anche se appaiono ricevuti da un mittente noto;

  ✓ Se possibile visualizzare i messaggi di posta elettronica sempre in formato "testo";

  ✓ In caso di necessità, mantenere disattivata l'anteprima nel programma di posta elettronica. Una mail visualizzata in formato HTML potrebbe contenere del codice in grado di inviare il vostro indirizzo e-mail al mittente. Mantenere disattiva l'anteprima del messaggio permetterà di poter eliminare il messaggio senza aprirlo.

- Qualora si ricevano messaggi che nulla hanno a che vedere con l'attività lavorativa e che si ritiene abbiano fini pubblicitari (SPAM);

  ✓ Non rispondere a messaggi di dubbia provenienza e che nulla hanno a che vedere con l'attività dell'Azienda (SPAM);

  ✓ Non cliccare su link che si trovano all'interno di mail pubblicitarie;

  ✓ Non rispondere mai alle mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla loro lista;

  ✓ Evitare di farsi coinvolgere nelle cosiddette "Catene di S. Antonio";

- Segnalare al Settore Informatico qualunque abuso del servizio di posta elettronica venuto a conoscenza dell'Utente (spam commerciali, virus, etc,…).

10 Accesso ai dati

Tutti i dati e le informazioni trattate dalle procedure informatiche sono di proprietà dell'Azienda.
Pertanto qualsiasi diffusione della loro conoscenza e del loro utilizzo al di fuori delle procedure definite all'interno dell'Azienda deve essere esplicitamente avallato dalle Direzioni competenti.

Si raccomanda agli Utenti di adottare cura e attenzione quando si scambiano i file attraverso la rete LAN dell'Azienda.

A tal fine è necessario seguire le seguenti regole:

- Non utilizzare la rete dell'Azienda per scambiare e/o condividere dati che nulla hanno a che vedere con l'attività lavorativa e non salvare sui server dell'Azienda dati o file che nulla a che vedere con l'attività lavorativa;

- Non visualizzare né copiare senza averne l'autorizzazione file che si trovano sui PC di altri Utenti o sui server dell'Azienda;

- Seguire le procedure di archiviazione standard dell'Azienda per eseguire il salvataggio dei dati presenti sul PC assegnato;

- Quando si accede a risorse condivise sulla LAN utilizzare sempre le credenziali di autenticazione che sono state assegnate individualmente all'Utente.

11 Virus

I virus sono una delle principali cause di danni e inefficienze dei sistemi informativi.

Al fine di minimizzare il rischio di infezione e di diffusione dei virus è necessario seguire le seguenti regole:

- Non disinstallare o disabilitare il software antivirus, che deve sempre essere presente, attivo e aggiornato sul proprio PC;

- Non installare sul proprio PC software di nessun genere meno che non sia stato fornito dall'Azienda;

- Non inserire sul proprio PC floppy, CD o altri apparecchi removibili di scambio dei dati la cui fonte non sia certa e sui quali vi sia la possibilità che contengano virus o file infettati.;

- Non aprire messaggi di posta elettronica la cui provenienza non sia certa.