PREMESSA

Questo documento fornisce a tutti gli utenti del sistema informativo una panoramica sulle responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione.
Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;

Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

TERMINOLOGIA

Con il termine di **Sistema Informativo** si intende tutto l'insieme dei documenti <DELLASCRIVENTE> siano essi memorizzati in forma elettronica sui dischi fissi dei calcolatori o sulle memorie interne delle fotocopiatrici, che tutti i documenti di qualsiasi altra natura come originali cartacei, corrispondenza ricevuta, elenchi, disegni, schemi, microfilm ed audiovisivi.

Con il temine **Dati Personali** si intende qualunque dato atto ad identificare univocamente una persona e/o società. A seconda del tipo di dati si parla poi di **dati personali sensibili** o di **dati personali comuni**.

STRUMENTI ELETTRONICI

La progressiva diffusione delle nuove tecnologie informatiche e telematiche, ed in particolare l'accesso alle reti Intranet ed Internet dai Personal Computer, espone <LASCRIVENTE> ai rischi di un coinvolgimento sia patrimoniale sia penale, qualora si verifichino utilizzi illegali degli accessi ad internet o telematici in genere (fax, telefoni aziendali ecc.) <DELLASCRIVENTE>.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche <DELLASCRIVENTE> deve sempre ispirarsi al principio della diligenza, e correttezza e sicurezza, comportamenti che normalmente si usano nell'ambito di un rapporto di lavoro, .

<LASCRIVENTE> ha quindi adottato un regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione della legge n. 675/1996 sulla privacy e del dpr n. 318/1999 sulle misure di sicurezza obbligatorie.

Nei punti sotto indicati del presente regolamento si intende per Amministratore del Sistema la persona designata a svolgere mansioni di amministrazione del sistema informatico aziendale.

Osservanza delle disposizioni in materia di privacy

Si richiamano tutti gli utenti del sistema informativo <DELLASCRIVENTE>, siano essi dipendenti o collaboratori, che è obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza ai sensi del dlg 196/2003.

Non osservanza della normativa

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce inosservanza delle disposizioni al personale e può essere quindi oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale, nonché nei casi più gravi di azioni civili e/o penali – ove consentite – nei confronti dei trasgressori.

Affissione

Il presente Regolamento è consegnato a tutti i dipendenti e collaboratori e disponibile via Intranet sui server <DELLASCRIVENTE>.

Amministratore di Sistema

L'Amministratore del Sistema esclusivamente per l'espletamento delle sue funzioni (backup, restore, ecc) ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna, e di revocare la password dell'utente previa comunicazione.

E' fatto divieto all'Amministratore di Sistema di accedere a dati o documenti di altri utenti

Utilizzo del Personal Computer

L'utente è responsabile del Personal Computer assegnatogli e deve custodirlo con diligenza.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici ed ogni qual volta ci sia la necessità di allontanarsi dal posto di lavoro per più di un ora. Si ricorda che lasciare inutilmente acceso un Calcolatore, oltre a costituire un potenziale rischio di incendio se viene lasciato incustodito, rappresenta

anche un'inutile spreco di risorse energetiche con conseguente aggravio di costi ed inutile danno all'ambiente.

I Personal Computer sono strumenti di lavoro**: è vietato ogni utilizzo non inerente l'attività lavorativa**.

I Personal Computer sono protetti da apposito programma anti virus. **E' vietato disinstallare o disattivare anche solo temporaneamente il programma anti virus**. Eventuali violazioni a questa norma possono essere causa di seri danni alla rete.

Ogni utente deve prestare la massima attenzione ai documenti informatici ricevuti dall'esterno, avvertendo immediatamente l'Amministratore del Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dalle procedure di protezione anti virus.

I singoli Personal Computer vengono protetti dagli accessi indesiderati mediante l'attivazione delle password del sistema operativo che **devono essere mantenute personali e segrete**. Non è consentita l'attivazione della password all'accensione del Personal Computer (BIOS) senza preventiva autorizzazione da parte dell'Amministratore del Sistema: i singoli Personal Computer devono essere sempre disponibili per eventuali interventi di manutenzione.

L'accesso ai dati memorizzati sui server di rete all'elaboratore connesso in rete è effettuato con il proprio **username e password** che **è strettamente personale e non deve essere divulgata.**

In caso di assenze prolungate dall'ufficio è obbligatorio bloccare la postazione attivando lo screen saver con richiesta di password per sbloccare la stazione. **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**.

La connessione ad Internet avviene mediante un router. Dalle macchine connesse alla rete è vietata qualsiasi altra modalità di connessione ad internet.

Non è consentito all'utente effettuare modifiche sia hardware che software al proprio Personal Computer salvo previa autorizzazione scritta da parte dell'Amministratore di Sistema.

Sui server, e più in generale sui dischi dei calcolatori in uso agli utenti, è vietato memorizzare files non inerenti l'attività lavorativa. In particolare modo è vietato memorizzare brani musicali o filmati (nei vari formati di compressione MP3, MP4, AVI, MPEG, DIVX, XVID, ecc.) ed eventuali altri tipi di files soggetti alla normativa sul diritto di autore.

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

E' vietato, salvo esplicite deroghe, salvare i documenti in forma crittografata.

UTILIZZO DI PC PORTATILI

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.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete.

I PC portatili utilizzati all'esterno, quando non vengono utilizzati, devono essere custoditi in un luogo protetto.

Nel caso dei PC portatili, data la facilità con cui possono essere smarriti, è obbligatorio utilizzare la password di accensione (BIOS) per prevenire l'utilizzo non autorizzato ed attivare tutti i meccanismi di protezione del sistema operativo.

Si ricorda che l'utilizzo di sistemi operativi di vecchia generazione (Windows 95, Windows 98, Windows ME) sui portatili non garantisce la segretezza dei dati in essi contenuti a causa del debole sistema di validazione delle password.

Qualora sia necessario memorizzare sui portatili dati considerati sensibili dalla Legge, è obbligatorio l'utilizzo di sistemi operativi con password più sicure o in alternativa l'utilizzo di tecniche di crittografia.

Il problema del Furto di identità

Un errore comune, soprattutto da parte di utenti di PC portatili o dei famigerati PC Palmari, consiste nel non dare importanza alle informazioni memorizzate nel portatile o nel palmare. In genere si pensa che in fondo sul portatile non ci sono memorizzati dati importanti e, in caso di furto si pensa solo al danno economico della perdita della macchina. Raramente si pensa alla perdita dell'identità.

Sul portatile ci possono essere difatti memorizzate troppe password. A parte quelle eventualmente salvate dell'utente nel fantasiosissimo file di word o excel PASSWORD.TXT, PASSWORD.DOC e PASSWORD.XLS e chi più ne ha ne metta.

Sul portatile è configurato l'accesso remoto per le connessioni ad internet via modem, l'accesso alla posta elettronica magari con il salvataggio automatico della password, c'è il certificato per l'accesso all'home bank ecc.

Nel caso di furto, il malintenzionato si trova in mano un oggetto con cui può connettersi ad internet con un'identità rubata, svolgere attività illegali su internet, inviare mail oltraggiose il tutto sfruttando l'identità dell'utente a cui è stato rubato il portatile.

Il problema quindi esula dal semplice danno economico e dalla semplice perdita di qualche file ma è la perdita delle identità che deve destare le maggiori preoccupazioni. Si deve quindi essere metodici e salvare sempre in modo ordinato e ben organizzato, tutti i servizi a cui ci si è abbonati in modo di potere sempre in qualsiasi momento ricollegarsi e cambiare tutte le password. Ovviamente anche queste informazioni non devono essere inserite nel famoso PASSWORD.TXT di cui sopra.

Se non fosse chiaro, il file PASSWORD.* non deve assolutamente essere mantenuto sul portatile, è troppo facile perderlo! Oltre tutto gli utenti tendono ad aggiungerci anche un sacco di altre cose tipo codice del bancomat, codice dell'impianto di allarme ecc. Insomma questo files (che c'e' quasi sempre purtroppo) è una vera minaccia.

Gestione delle Password

Le password sono strettamente personali, è vietato utilizzare la User-ID / password di un altro utente in sua assenza o per qualsiasi altro motivo. Login e password sono strettamente personali e non si ammettono deroghe.

A tutti gli utenti del sistema Informatico viene fornita un identificativo personale di login (User-ID) al quale l'utente deve obbligatoriamente associare una password (vedi comandi dei vari sistemi operativi)

Per ogni chiarimento e disposizione in merito alle regole di creazione e utilizzo delle password si rimanda al sito Intranet aziendale.

Protezione anti virus

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

Su tutti i Personal Computer è installato un apposito programma anti virus; è vietato alterare, disabilitare o modificare il programma anti virus. Ogni calcolatore connesso per qualsiasi motivo, anche solo temporaneamente, alla rete deve essere dotato di software anti virus aggiornato alle ultime definizioni dei Virus disponibili.

Nel caso in cui il software anti virus rilevi la presenza di un virus, l'utente dovrà immediatamente segnalare il problema all'Amministratore del sistema.

Se l'anti virus non è in grado di ripulire il documento infetto si deve inoltre:

- 1) sospendere ogni elaborazione in corso senza spegnere il computer
- 2) se è in grado di farlo, staccare il cavo di rete per isolare la macchina dalla rete aziendale.

Software Installato

Il software per elaboratori e' considerato opera di ingegno e come tale è tutelato dalle Leggi sul diritto di autore. L'utilizzo del software è regolamentato da licenze d'uso che devono essere assolutamente rispettate da tutti. (DLG. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente <DELLASCRIVENTE> perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore e perché sono i programmi per i quali <LASCRIVENTE> possiede la regolare licenza d'uso.

E' vietato provare ad installare il software contenuto nei vari CD ROM distribuiti con le riviste, con i libri e con i quotidiano anche se si tratta di software allegato a riviste del settore. Prima di installare questi CD è necessario il benestare dell'amministratore di sistema.

Non è ammesso l'uso di strumenti atti a catturare o rivelare le password (password crack, keylogger, ecc.) per accedere in modo non autorizzato a dati o sistemi.

E' assolutamente vietato installare, anche solo temporaneamente, programmi ottenuti o sbloccati illegalmente (programmi crackati, codici di sblocco ottenuti da internet, ecc.).

Un programma crackato, oltre a costituire una violazione alle norme che regolano il Diritto d Autore, costituisce anche un'autentica minaccia alla sicurezza della rete ed all'affidabilità del calcolatore su cui viene installato. Lo sblocco del programma (crack) viene infatti effettuato modificando i codici originali del programma per aggirare le protezioni. Questo implica sostituire pezzi del programma originale con parti modificate e queste nuove aggiunte, oltre ad aggirare le protezioni, possono anche introdurre codice dannoso.

Connessione alla Rete

La rete <DELLASCRIVENTE> si basa sul protocollo TCP/IP. Tutte le apparecchiature connesse alla Rete <DELLASCRIVENTE> sono configurate per ricevere l'indirizzo IP dinamicamente dal server DHCP oppure con un IP assegnato staticamente a seconda della tipologia di apparecchiatura.

E' assolutamente vietato connettere alla rete delle macchine configurate con indirizzo IP statico, assegnato direttamente dall'utente, senza una preventiva autorizzazione dall'Amministratore di sistema. Introdurre una macchina con un IP duplicato potrebbe causare un conflitto con l'indirizzo di un server oppure di un altro dispositivo della rete stessa e causare gravi malfunzionamenti alla rete.

In caso di dubbio prima di collegare alla rete aziendale un portatile di terze persone chiedete all'Amministratore di sistema se è possibile connetterlo.

Non è ammessa la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, ecc.)

E' fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, accesso remoto, proxy server.

E' fatto assoluto divieto di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware.

Memorizzazione Dati sui Server

Tutti i dati di interesse aziendale devono essere memorizzati sui server di rete al fine di garantire la corretta gestione dei salvataggi.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte delle persone autorizzate.

E' espressamente vietato memorizzare sui dischi dei server o dei calcolatori in uso agli utenti, di materiale protetto da diritti di autore per il quale non si dispongano i diritti. E' quindi tassativamente vietato il salvataggio di archivi nei classici formati AVI, MPEG, DIVX, XVID, MP3 ecc che contengano copie di film o brani musicali.

Non sono ammesse condivisioni di risorse locali tra i singoli Personal Computer.

L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui Personal Computer degli utenti sia sulle unità di rete, informando l'utente.

Costituisce buona regola la pulizia periodica degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

Servizi Peer to Peer e IRC

Come più volte richiamato in questo documento, la rete <DELLASCRIVENTE> è utilizzabile solo per attività inerenti le mansioni lavorative. E' proibito l'utilizzo delle attrezzature aziendali per attività non inerenti le proprie mansioni.

In particolare modo è tassativamente proibito utilizzare i calcolatori e l'infrastruttura di rete <DELLASCRIVENTE> allo scopo di connettersi ad internet nei circuiti Peer2Peer (i cosiddetti Napster o winmx). Tali circuiti sono prevalentemente utilizzati dagli utenti per lo scambio abusivo di materiali protetti dal diritto di autore ovvero per scaricare e/o condividere filmati, canzoni e programmi.

Questo tipo di attività è in aperta violazione delle norme a tutela del diritto di autore e come tale è tassativamente proibita sulla rete <DELLASCRIVENTE>.

A scanso di equivoci, come già precedentemente detto, **è altresì vietato memorizzare sul server o sui dischi fissi dei calcolatori dati in uso agli utenti, materiale protetto da diritto d'autore per il quale non si posseggano pieni diritti per l'utilizzo**. E' quindi vietato salvare sui dischi fissi files con estensione *.avi, *.mpg, *.ram, *.mp4 ecc. Fatto salvo i casi autorizzati esplicitamente e cioè qualora questo materiale risulti auto prodotto (esempio corso interattivo) e di cui si sia in grado di dimostrare

l'effettiva titolarità dei diritti.

Analogamente anche il traffico di messaggistica istantanea su IRC (Messanger ecc) è vietato.

Essendo inibito l'utilizzo delle reti P2P ed IRC di conseguenza è anche vietata la semplice installazione del software. E' vero che la semplice installazione del software P2P non costituisce di per se un reato ma, essendone esplicitamente vietato l'uso nella rete è automaticamente vietato installare tali programmi.

Qualora su un calcolatore in uso agli utenti venga trovata, a cura dell'Amministratore di sistema o di altri responsabili della sicurezza, un programma per la connessione a reti P2P (Napster, winMx ecc.) o un programma di Messaggistica istantanea (Messanger, ICQ ecc.) il fatto costituisce grave violazione delle regole aziendali.

Oltre ai programmi per scaricare contenuti multimediali dalle reti P2P, è anche vietata l'installazione dei programmi per la gestione in locale (quindi vari Divx player e vari codec). E' ammessa l'installazione solo di un programma standard (tipo Windows media player senza codec particolari tipo XVID e DIVX) nei casi in cui sia necessario, per lo svolgimento della normale attività lavorativa, accedere a contenuti Multimediali (Corsi interattivi ecc.).

Stampanti e supporti Magnetici/ottici

Le stampe dimenticate o i dati memorizzati su supporti rimovibili possono spesso costituire involontaria fuga di notizie. Si raccomanda quindi la massima attenzione nell’utilizzo di stampe e dischetti o diversi dispositivi di memorizzazione con particolare riferimento alla corretta distruzione di documenti e o supporti che non servono più.

E’ cura dell’utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

E’ vietato portare fuori dall’azienda tabulati, stampe, supporti di memorizzazione sia magnetici che ottici salvo esplicita autorizzazione.

Qualsiasi CD, DVD o Floppy disk prodotto all’interno dell’azienda deve obbligatoriamente essere realizzato mediante i supporti ufficiali <DELLASCRIVENTE> Non è assolutamente ammesso l’utilizzo di supporti (CD-R o CD-RW) diversi dai supporti ufficiali.

Tutti i supporti magnetici e/o ottici (dischetti, cassette, CD-R, CD-RW, DVD-R, DVD-RD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato o cadere in mano a terzi non autorizzati (art. 7 del DPR 318/99). La semplice cancellazione dei supporti non garantisce l’eliminazione dei dati in essi memorizzati; una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

Supporti magnetici o tabulati, contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave come prescritto dalla Legge sulla tutela dei dati personali.

Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro e come tale non deve essere usato a fini diversi rispetto alla normale attività lavorativa.

E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga saturano lo spazio disponibile sui dischi del server.

E' vietato utilizzare l'indirizzo e caselle di posta elettronica aziendale, nel formato previsto nome.cognome@dominio.it, per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

E' importante comprendere che un messaggio di email inviato con un indirizzo di posta aziendale è in qualche modo assimilabile ad una lettera su carta intestata. Il Dominio infatti identifica in modo univoco la fonte. La partecipazione ad un forum su internet con un indirizzo aziendale potrebbe trarre in inganno gli altri utenti che, vedendo il nome del dominio, potrebbero supporre che questo sia un parere ufficiale e non un semplice messaggio di un utente. Questo potrebbe avere anche conseguenze in termini di immagine per <LASCRIVENTE>.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali <PERLASCRIVENTE>, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dalla Direzione.

E' vietato utilizzare la login / password di un altro utente per accedere in sua assenza alla sua posta elettronica.

Non è possibile ottenere per via informatica, nelle comunicazioni esterne all'azienda, la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Pertanto, di norma, per la comunicazione per avere una garanzia di avvenuta ricezione è conveniente chiedere al destinatario di confermare esplicitamente.

Si ricorda che l'utilizzo della posta elettronica deve seguire le stesse regole in uso per la tradizionale posta cartacea quindi, stampa messaggio, protocollo se previsto ed archiviazione.

Per le altre regole sull'utilizzo della posta elettronica si rinvia al documento controfirmato dai singoli utenti per l'abilitazione del servizio.

Uso della rete Internet e dei relativi servizi

La connessione ad Internet è fornita agli utenti abilitati esclusivamente come uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

E' fatto divieto all'utente lo scarico di software da siti Internet, se non espressamente autorizzato dall'Amministratore del Sistema.

E' tassativamente vietato l'utilizzo di Internet per 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 e con il rispetto delle normali procedure di acquisto.

E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, la partecipazione a Forum non professionali, l'utilizzo di chat-line e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Si ricorda che la navigazione in internet non è assolutamente anonima. La semplice visualizzazione di una pagina web comporta l'inserimento automatico in una certa serie di LOG mantenuti dalle varie macchine tra cui l'eventuale LOG del proxy server della rete <DELLASCRIVENTE> da cui viene effettuata la connessione, dal LOG del provider internet che fornisce la connessione ad internet ed infine dal LOG del sito internet consultato. La navigazione viene quindi tracciata da parecchie macchine. Sono tutti LOG automatici raccolti solo per eventuali problemi di ordine giudiziario: in caso di attività illegali svolte su internet la Polizia Postale può richiedere l'accesso ai LOG dei vari provider e verificare da quale connessione internet risulta essere stato generato il traffico.

<LASCRIVENTE>, ai soli fini di raccolta per evitare problemi futuri, si riserva di attivare in qualsiasi momento e senza ulteriori comunicazioni agli utenti, un servizio di memorizzazione dei LOG del proxy server al solo fine di avere la possibilità di risalire all'utente che ha effettuato eventuali attività illecite su internet, in caso di indagini svolte dalla magistratura a carico <DELLASCRIVENTE>.

Per le altre regole sull'utilizzo della posta elettronica si rinvia al documento controfirmato dai singoli utenti per l'abilitazione del servizio.

IL PRESIDENTE	L'AMMINISTRATORE DI SITEMA	FIRMA PER PRESA VISIONE
_____	_____	_____

Lettera Autorizzazione

Circolare a tutti i dipendenti e collaboratori <DELLASCRIVENTE>

_____ li; _____

Posta elettronica

La rete <DELLASCRIVENTE> prevede una connessione ad Internet mediante rete <Internet> ed un servizio di posta elettronica.

Si rammenta che la posta elettronica trasmessa e/o ricevuta tramite Internet è considerata, per motivi organizzativi, una componente del circuito di comunicazione aziendale e quindi viene trattata con le stesse regole di un qualsiasi documento aziendale.

A breve sarà attivato un servizio automatico di archiviazione di tutta la posta in arrivo all'indirizzo nome.cognome@dominio ed appena possibile lo stesso servizio verrà attivato anche per tutta la posta in uscita per l'account nome.cognome@dominio

Si prega quindi gli utenti di non utilizzare per messaggi personali gli account di posta aziendali ovvero gli account del dominio <DELLASCRIVENTE>

Firma per presa visione e consenso

_____

Fax

Analogamente alla posta elettronica si rammenta agli utenti che anche il servizio Fax è considerato, per motivi organizzativi, una componente del circuito di comunicazione aziendale e quindi viene trattata con le stesse regole di un qualsiasi documento aziendale.

Si prega quindi gli utenti di non utilizzare il Fax aziendale per messaggi personali.

Firma per presa visione e consenso

_____

Navigazione Internet

Il servizo di navigazione su Internet viene messo a disposizione degli utenti esclusivamente come strumento di lavoro. **L'utilizzo della Navigazione su Internet a fini personali è vietato.**

L'accesso ad Internet attraverso la rete aziendale deve essere effettuato solo mediante il servizio aziendale di proxy server.

L'utilizzo di metodi alternativi per accedere ad Internet dalla sede, ad esempio mediante modem, wireless e cellulari, e' tassativamente vietato per seri problemi di sicurezza.

Si ricorda a tutti gli utenti che l'utilizzo di internet, pur essendo collegati alla rete solo mediante una

connessione dati, non è assolutamente anonimo. Ad ogni click del mouse ci sono varie macchine che registrano l'attività svolta. Queste macchine sono, i server del provider che offre la connessione, i server delle pagine web che si stanno visitando, i server di posta che si stanno utilizzando ecc.

Il fatto che Internet non abbia un padrone non vuole quindi dire che è anonima e non ha un controllo.

Il provider è obbligato a mantenere il Log delle connessioni degli utenti; per ogni pagina consultata vengono salvate le informazioni relative all'IP, alla data e all'ora di connessione. Il Log del provider comunque è generale per tutte le connessioni <DELLASCRIVENTE> e non fa alcuna distinzione tra gli utenti. Un eventuale indagine della Magistratura, mediante Log del provider, porterebbe ad identificare <LASCRIVENTE> come unico responsabile di eventuali illeciti.

Con l'unico scopo di difesa nel caso di comportamenti illeciti da parte di qualche utente, la connessione ab internet dalla della rete <DELLASCRIVENTE> viene effettuata mediante un servizio di proxy server che tiene traccia di tutte le connessioni degli utenti.

Il proxy server, in fase di connessione ad internet, richiede di specificare la propria User-ID e la propria password (che devono essere personali e segrete).

Il servizio di proxy aziendale è configurato per tenere un Log delle connessioni internet memorizzando elenco siti visitati, data ed utente.

Questo log viene raccolto esclusivamente per tutelare <LASCRIVENTE> qualora ci siano contestazioni da parte della Magistratura o della Polizia Postale, in merito all'attività svolta su internet a partire dalla connessione <DELLASCRIVENTE>.

Non ci sono altre finalità nella raccolta di questi Log e non sono previsti strumenti per visualizzazione ed analisi di detti Log.

I Log archiviati con periodicità mensile e verranno conservati per un periodo di 2 anni su CD-R trascorso il quale saranno distrutti.

Firma per presa visione e consenso

_____

LA SICUREZZA IN 13 PUNTI

1. **UTILIZZATE LE CHIAVI!**
   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. **CONSERVATE I DISCHETTI IN UN LUOGO SICURO**
   Per i dischetti si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato.Riponeteli sotto chiave non appena avete finito di usarli.

3. **UTILIZZATE LE PASSWORD**
   Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
   La password di accesso al computer (BIOS) impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
   La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato ai Vostri dati sui server.
   La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.
   Imparate a utilizzare questi tre tipi fondamentali di password. Scegliete una password facile da ricordare na difficile da indovinare!

4. **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**
   Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete le stampe quando non servono più.

5. **NON LASCIATE TRACCIA DEI DATI RISERVATI**
   Quando riutilizzate un dischetto, prima riformattatelo sempre. Per evitare problemi non riutilizzate mai i CD-R non completamente scritti.. Nel dubbio, è sempre meglio usare un supporto nuovo.

6. **PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI**
   I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, utilizzate una procedura di backup periodico e proteggete il portatile con le password di accensione.

7. **NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD**
   Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

8. **CUSTODITE LE PASSWORD IN UN LUOGO SICURO**
   Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

9. **NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ**
   Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

10. **NON UTILIZZATE APPARECCHI NON AUTORIZZATI**
    L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con l'Amministratore di rete.

11. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
    Utilizzate solo i programmi autorizzati dall'Amministratore di rete. Non fidatevi assolutamente dei programmi trovati su CD o scaricati da Internet.

12. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
    La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

13. **CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP**
    Verificate personalmente che i Vostri dati siano regolarmente salvati dal Responsabile dei Backup.